AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBER THREATS AND SECURITY SOLUTIONS

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

MAY 21, 2013

Serial No. 113–45

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE
82–197 WASHINGTON : 2013

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 ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

RALPH M. HALL, Texas
JOE BARTON, Texas
Chairman Emeritus
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
Vice Chairman
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Missouri
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York

CONTENTS

WITNESSES

CYBER THREATS AND SECURITY SOLUTIONS

TUESDAY, MAY 21, 2013

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
WASHINGTON, DC.

The committee met, pursuant to call, at 10:05 a.m., in room 2123 of the Rayburn House Office Building, Hon. Marsha Blackburn (vice chairman of the committee) presiding.

Present: Representatives Blackburn, Shimkus, Pitts, Walden, Terry, Rogers, Murphy, Burgess, Scalise, Latta, Harper, Lance, Cassidy, Olson, McKinley, Gardner, Pompeo, Kinzinger, Griffith, Bilirakis, Johnson, Long, Ellmers, Dingell, Rush, Eshoo, Green, DeGette, Capps, Doyle, Schakowsky, Matheson, Butterfield, Barrow, Matsui, Castor, McNerney, Braley, Tonko, and Waxman (ex officio).

Staff present: Nick Abraham, Legislative Clerk; Carl Anderson, Counsel, Oversight; Gary Andres, Staff Director; Charlotte Baker, Press Secretary; Ray Baum, Senior Policy Advisor/Director of Coalitions; Mike Bloomquist, General Counsel; Matt Bravo, Professional Staff Member; Patrick Currier, Counsel, Energy and Power; Neil Fried, Chief Counsel, Communications and Technology; Brad Grantz, Policy Coordinator, Oversight and Investigations; Gib Mullan, Chief Counsel, Commerce, Manufacturing, and Trade; Andrew Powaleny, Deputy Press Secretary; David Redl, Counsel, Telecom; Krista Rosenthall, Counsel to Chairman Emeritus; Chris Sarley, Policy Coordinator, Environment and the Economy; Peter Spencer, Professional Staff Member, Oversight; Dan Tyrrell, Counsel, Oversight; Lyn Walker, Coordinator, Admin/Human Resources; Phil Barnett, Democratic Staff Director; Jeff Baron, Democratic Senior Counsel; Shawn Chang, Democratic Senior Counsel; Patrick Donovan, FCC Detailee; Margaret McCarthy, Democratic Staff; Roger Sherman, Democratic Chief Counsel; and Kara van Stralen, Democratic Policy Analyst.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Mrs. BLACKBURN. The subcommittee will come to order. As we open our hearing today, I am certain we all are mindful and remembering and are prayerful for those in Oklahoma, and our former colleague, Governor Mary Fallin, who is addressing that tragedy today with the storms there in Oklahoma. I recognize myself for 5 minutes for an opening statement.

American companies, the U.S. government and private citizens are facing new challenges in the fight to protect our Nation's security, economy, intellectual property and critical infrastructure from cyber attacks.

Today the Energy and Commerce Committee is exploring how the private sector and our government are responding. We will also review the implementation of the President's Cybersecurity Executive Order 13636.

Cyber attacks have grown in scope and sophistication to include nearly every industry and asset that makes America work. That is why this committee is well positioned to lead, oversee and review policies and solutions to these wide-ranging and evolving threats. Last year an al-Qaeda video surfaced calling for a covert cyber jihad against the United States. On Sunday, the New York Times reported that hackers sponsored by China's People's Liberation Army have resumed attacks on U.S. targets. According to the GAO, the number of cyber incidents reported by federal agencies to U.S. Computer Emergency Readiness Teams has increased by 782 percent over 6 years.

As vice chairman of the full committee, I offered a discussion framework, the SECURE IT Act, to provide our government, business community and citizens with the tools and resources needed to protect themselves from those who wish us harm. The five major components that make up the Secure IT Act are, number one, allow the government and the private sector to share cyber threat information in a more transparent fashion; number two, reform how our government protects its own information systems; number three, create new deterrents for cyber criminals; number four, prioritize research and development for cybersecurity initiatives; and number five, streamline consumers' ability to be notified when they are at risk of identity theft and financial harm.

One of the things we know is that cybersecurity is uniquely ill suited for federal regulation. Rapid changes in technology guarantee the failure of static, prescriptive approaches. Our focus should be on developing consensus public policy that puts American businesses in the driver's seat and allows cooperation and collaboration, not top-down and one-size-fits all mandates.

NIST's written testimony on implementing the framework of the Executive order states, "Any efforts to better protect critical infrastructure need to be supported and implemented by the owners and operators of this infrastructure. It also reflects the reality that many in the private sector are already doing the right things to protect their systems and should not be diverted from those efforts through new requirements." Private solutions—not government presumptions—offer the best prospect for our future cyber defenses.

As we explore ways to incentivize the private sector to diminish our exposure to cyber threats, we must ensure the Executive order stays true to a voluntary, cooperative standard. Likewise, Congress and the executive branch should refrain from further exploring legislative regulatory proposals giving DHS authority to impose critical infrastructure requirements as our government is purportedly already in the midst of working with the private sector to draft a voluntary cybersecurity framework.

I look forward to the testimony and appreciate each and every one of our nine witnesses' thoughtful answers to our questions this morning.

[The prepared statement of Mrs. Blackburn follows:]

PREPARED STATEMENT OF HON. MARSHA BLACKBURN

American companies, the U.S. government, and private citizens are facing new challenges in the fight to protect our nation's security, economy, intellectual property, and critical infrastructure from cyber attacks.

Today the Energy and Commerce Committee is exploring how the private sector and our government are responding. We will also review the implementation of the President's Cybersecurity Executive Order 13636.

Cyber attacks have grown in scope and sophistication to include nearly every industry and asset that makes America work. That is why this committee is well-positioned to lead, oversee, and review policies and solutions to these wide-ranging and evolving threats. Last year an al-Qaeda video surfaced calling for a covert cyber jihad against the United States. On Sunday the New York Times reported that hackers sponsored by China's People's Liberation Army have resumed attacks on U.S. targets. According to the GAO, the number of cyber incidents reported by federal agencies to US Computer Emergency Readiness Team has increased by 782 percent over 6 years.

As vice chairman of the full committee, I offered a discussion framework—the SECURE IT Act—to provide our government, business community, and citizens with the tools and resources needed to protect themselves from those who wish us harm. The five major components that make up the Secure IT Act are: 1) allow the government and the private sector to share cyber threat information in a more transparent fashion; 2) reform how our government protects its own information systems; 3) create new deterrents for cyber criminals; 4) prioritize research and development for cybersecurity initiatives; and 5) streamline consumers' ability to be notified when they are at risk of identity theft and financial harm.

One of the things we know is that cybersecurity is uniquely ill-suited for federal regulation. Rapid changes in technology guarantee the failure of static, prescriptive approaches. Our focus should be on developing consensus public policy that puts American businesses in the driver's seat and allows cooperation and collaboration, not top-down and one-size-fits-all mandates.

NIST's written testimony on implementing the framework of the Executive order states, "Any efforts to better protect critical infrastructure need to be supported and implemented by the owners and operators of this infrastructure. It also reflects the reality that many in the private sector are already doing the right things to protect their systems and should not be diverted from those efforts through new requirements." Private solutions—not government presumptions—offer the best prospect for our future cyber defenses.

As we explore ways to incentivize the private sector to diminish our exposure to cyber threats, we must ensure the Executive order stays true to a voluntary, cooperative standard. Likewise, Congress and the executive branch should refrain from further exploring legislative regulatory proposals giving DHS authority to impose critical infrastructure requirements as our government is purportedly already in the midst of working with the private sector to draft a voluntary cybersecurity framework.

I look forward to the testimony and appreciate all nine of our witnesses' thoughtful answers to our questions this morning.

# # #

Mrs. BLACKBURN. At this time, is there any member seeking the remainder of the time? I yield back my time, and Mr. Waxman, you are recognized for 5 minutes.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. WAXMAN. Thank you very much, Madam Chair, for holding this hearing today on cyber threats to the Nation's critical infrastructure.

Cybersecurity is a vital concern for sectors that span the committee's jurisdiction, from the electric grid and natural gas pipelines to telecommunications networks and health care. Our committee should be playing a key role in developing policies to enhance the cybersecurity of the infrastructure we depend on every day for power, drinking water, communications and medical care. All of these sectors are essential to the daily operation of our economy and our government, but I want to focus on one in particular: the electric grid.

The Nation's critical infrastructure and defense installations simply cannot function without electricity. The committee has a special responsibility to ensure that the electric grid is properly defended from cyber and physical attacks. The Executive order we are examining today is a step in the right direction but we also need new legislation.

In January, Representative Ed Markey and I wrote to more than 150 electric utilities to ask about their efforts to protect the electric grid from cyber attacks, physical attacks and geomagnetic storms. We received responses from over 60 percent of those utilities.

Today, we are releasing a report analyzing the responses we received. The findings are sobering. Many utilities reported that the electric grid is a target of daily cyber attacks. Some utilities explained that they are under a "constant state of attack." One utility reported that it was the target of approximately 10,000 attempted cyber attacks each month. The utilities did not report any damage from these attacks to date, but the threat is growing.

An industry organization called the North American Electric Reliability Corporation, or NERC, develops mandatory reliability standards for the electric grid through a protracted consensus-based process. NERC also recommends voluntary actions to utilities. Our report finds that most utilities comply only with the mandatory cyber security standards, which mostly focus on general procedures. They have not implemented the voluntary NERC recommendations, which are targeted at specific threats. For example, only 21 percent of investor-owned utilities reported implementing NERC's recommended actions to protect against the Stuxnet virus.

The failure of utilities to heed the advice of their own industry-controlled reliability organization raises serious questions about whether the grid will be adequately protected by a voluntary approach to cybersecurity. When specific threats arise, prompt action is needed, but utilities are apparently not responding to the alerts from this organization.

We also asked utilities about geomagnetic storms, which can interfere with the operation of the electric grid and damage large electric transformers. Most utilities have not taken concrete steps to reduce the vulnerability of the grid to geomagnetic storms. Only one-third of investor-owned utilities and one-fifth of municipal utilities or rural electric co-ops reported taking specific mitigation

measures, such as hardening their equipment. The Federal Energy Regulatory Commission is aware of this vulnerability to geomagnetic storms. Last week, it directed NERC to address the issue. Yet FERC lacks the authority to make sure that NERC's actions are sufficient.

In 2010, Congressman Fred Upton and Congressman Ed Markey introduced the bipartisan GRID Act to provide FERC with authority to address cyber threats and vulnerabilities. The legislation also provided FERC with the authority to protect the grid against physical attacks, electromagnetic pulses and geomagnetic storms. There was a bipartisan consensus that national security required us to act. That bill was reported out of this committee by a vote of 47 to nothing, and then it passed the full House by voice vote. However, the Senate did not act on the legislation.

Madam Chair, we need to work together in a bipartisan way to protect the electric grid. Nothing in the executive order we are examining today will address the regulatory gaps that prevent FERC from acting decisively to tackle these dangers. I hope that today's hearing will be the first step in rebuilding the bipartisan consensus we had on the need for legislative action. Thank you, Madam Chair.

[The prepared statement of Mr. Waxman follows:]

PREPARED STATEMENT OF HON. HENRY A. WAXMAN

Mr. Chairman, thank you for holding today's hearing on cyber threats to the nation's critical infrastructure. Cyber security is a vital concern for sectors that span the Committee's jurisdiction—from the electric grid and natural gas pipelines to telecommunications networks and health care. Our Committee should be playing a key role in developing policies to enhance the cyber security of the infrastructure we depend on every day for power, drinking water, communications, and medical care.

All of these sectors are essential to the daily operation of our economy and our government, but I want to focus on one in particular: the electric grid. The nation's critical infrastructure and defense installations simply cannot function without electricity.

The Committee has a special responsibility to ensure that the electric grid is properly defended from cyber and physical attacks. The Executive order we are examining today is a step in the right direction. But we also need new legislation.

In January, Ed Markey and I wrote to more than 150 electric utilities to ask about their efforts to protect the electric grid from cyber attacks, physical attacks, and geomagnetic storms. We received responses from over 60% of those utilities.

Today, we are releasing a report analyzing the responses we received. The findings are sobering. Many utilities reported that the electric grid is the target of daily cyber attacks. Some utilities explained that they are under a "constant state of attack." One utility reported that it was the target of approximately 10,000 attempted cyber attacks each month.

The utilities did not report any damage from these attacks to date. But the threat is growing.

An industry organization called the North American Electric Reliability Corporation, or NERC, develops mandatory reliability standards for the electric grid through a protracted, consensus-based process. NERC also recommends voluntary actions to utilities. Our report finds that most utilities comply only with the mandatory cyber security standards, which mostly focus on general procedures. They have not implemented the voluntary NERC recommendations, which are targeted at specific threats. For example, only 21% of investor-owned utilities reported implementing NERC's recommended actions to protect against the Stuxnet virus.

The failure of utilities to heed the advice of their own industry-controlled reliability organization raises serious questions about whether the grid will be adequately protected by a voluntary approach to cyber security. When specific threats arise, prompt action is needed. But utilities are apparently not responding to the alerts from NERC.

We also asked utilities about geomagnetic storms, which can interfere with the operation of the electric grid and damage large electric transformers. Most utilities have not taken concrete steps to reduce the vulnerability of the grid to geomagnetic storms. Only one-third of investor-owned utilities and one-fifth of municipal utilities or rural electric co-ops reported taking specific mitigation measures, such as hardening their equipment.

The Federal Energy Regulatory Commission is aware of this vulnerability to geomagnetic storms. Last week, it directed NERC to address the issue. Yet FERC lacks the authority to make sure that NERC's actions are sufficient.

In 2010, Fred Upton and Ed Markey introduced the bipartisan GRID Act to provide FERC with authority to address cyber threats and vulnerabilities. The legislation also provided FERC with authority to protect the grid against physical attacks, electromagnetic pulses, and geomagnetic storms. There was a bipartisan consensus that national security required us to act. That bill was reported out of this Committee by a vote of 47 to zero. And then it passed the full House by voice vote. However, the Senate did not act on the legislation.

Mr. Chairman, we need to work together in a bipartisan way to protect the electric grid. Nothing in the executive order we are examining today will address the regulatory gaps that prevent FERC from acting decisively to tackle these dangers.

I hope that today's hearing will be the first step in rebuilding the bipartisan consensus we had on the need for legislative action.

Mrs. BLACKBURN. The gentleman yields back, and I would like to welcome and recognize our first witness today. Dr. Gallagher is the Under Secretary of Commerce for Standards and Technology and Director of the National Institute of Standards and Technology, or NIST. And everyone knows, Mr. Waxman had all of his acronyms. There is an app for that. You can get an app and follow all of these acronyms. Dr. Gallagher, we are delighted you are here, and you are recognized for 5 minutes for an opening statement.

Mr. WAXMAN. Madam Chair, can I just ask a question? Is the app able to tell us what a NERC and a FERC is for jerks? Oh, bad joke.

Mrs. BLACKBURN. Dr. Gallagher, you are recognized.

STATEMENT OF DR. PATRICK D. GALLAGHER, UNDER SECRETARY OF COMMERCE FOR STANDARDS AND TECHNOLOGY, AND DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Dr. GALLAGHER. Thank you, Madam Chair and Ranking Member Waxman. I want to thank you and the members of this committee for this opportunity to testify today. My task this morning is to briefly summarize NIST's role and our responsibility specifically to develop a framework to reduce cyber risk to critical infrastructure.

It may be a surprise to some that an agency of the U.S. Department of Commerce has a key role in cybersecurity, but in fact, NIST has a long history in this area. We have provided technical support to cybersecurity for over 50 years working closely with our federal partners. Also because NIST is a technical but non-regulatory agency, we provide a unique interface with industry to support their technical and standards efforts. Today NIST has programs in a wide variety of cybersecurity areas including cryptography, network security, security automation, hardware roots of trust, identify management and cybersecurity education.

As directed in the Executive order, NIST will work with industry to develop a cybersecurity framework. This is in essence a collection of industry-developed standards and best practices to reduce cyber risk to critical infrastructure. The Department of Homeland

Security in coordination with sector-specific agencies will then support the adoption of the cybersecurity framework by owners and operators of critical infrastructure and other interested entities through a voluntary program.

To be successful, two major elements have to be part of this approach. First, it will require an effective partnership across government to ensure that our work with industry for the cybersecurity framework is fully integrated with the mission of a diverse set of agencies. This will enable a more holistic approach to addressing the complex nature of this challenge.

Secondly, the cybersecurity framework must be developed through a process that is industry led and open and transparent to all stakeholders. By having industry develop their own practices that are responsive to the performance goals, this process will ensure a robust technical basis but also one aligned with business interests. This approach has many benefits. It does not dictate a specific solution to industry but it promotes industry offering its own solutions. It provides solutions that are compatible with the market and other business conditions, and by leveraging industry's own capacity, it brings more talent and expertise to the table to develop the solutions.

This is not a new or novel approach for NIST. We have utilized very similar approaches in the recent past to address other pressing national priorities, most notably on the development of a nationwide end-to-end interoperable smart grid, and in the area of cloud computing technologies. We believe we know how to do this.

Since this is industry's framework, the NIST role will be to lend its technical expertise and to support their efforts. We will act as a convener, a contributor, and we will work closely with our federal partners to ensure that the effort is relevant and contributes to their missions to protect the public.

So what is in this framework? In short, whatever is needed to achieve good cybersecurity performance. In practice, we expect that the framework will include standards, methodologies, procedures and processes that can align business, policy and technological approaches to address cyber critical infrastructure.

Let me touch quickly on the topic of standards and their importance to the success of this effort. By "standards," I am using the term as industry does. These are agreed-upon best practices or specifications, norms, if you will, that allow compatibility of efforts to meet a goal. These are not the same thing as regulation. Industry standards are developed through a multi-stakeholder voluntary consensus process, and it is this process that gives standards their considerable power, that is, their broad acceptance around the world. These standards are not static. They can be changed to meet technological advances and new performance requirements. Performance-based standards promote innovation by allowing new products and services to come to the market in a way that is not a tradeoff with good security.

Madam Chair, I appreciate the challenge before us. The Executive order requires the framework to be developed within one year. A preliminary framework is due already within 8 months, and we have already begun to work on this. We have issued a request for information to gather relevant input from industry and other

stakeholders, and we are actively inviting stakeholders to participate in the cybersecurity framework process. The early response from industry has been very gratifying. Over the next few months, we will convene a series of deep dive workshops and use these workshops to develop the framework. This forum allows the needed collaboration and engagement. The first workshop was held in early April to start organizing the process, and next week will be our first full workshop.

Last week, we released the initial findings from an early analysis of the responses to the request for information. These responses range from individuals to large corporations and trade association from a few sentences on particular topics to comprehensive responses that ran well over 100 pages. Next week at the workshop hosted by Carnegie Mellon University in Pittsburgh, we will work with the stakeholder community to discuss the foundations of the framework and this initial analysis, and this will mark the transition to actually developing the framework.

In a related note, in June the Departments of Commerce, Homeland Security, and Treasury will submit reports regarding incentives designed to increase participation with the voluntary program. At 8 months we will have an initial draft framework including initial list of standards, guidelines and best practices, but even after a year the work will only have begun. Adoption and use of this framework will raise new issues that we need to address. The goal at the end of this process will be for industry to take and update the cybersecurity framework themselves, creating a continuous process to enhance cybersecurity.

The President's Executive order lays out an urgent and ambitious agenda but it is designed around an active collaboration between the public and private sectors. I believe that this partnership provides the needed capacity to meet the agenda and effectively will give us the tools to manage the cyber risk we face

I really appreciate the committee holding this hearing. We have a lot of work ahead of us, and I look forward to working with you to address these challenges. I am looking forward to answering any questions you may have.

[The prepared statement of Dr. Gallagher follows:]

Testimony of

Patrick D. Gallagher, Ph.D.
Under Secretary of Commerce for
Standards and Technology
United States Department of Commerce

Before the
United States House of Representatives

Committee on Energy and Commerce

"Cyber Threats and Security Solutions"

May 21, 2013

Introduction
Chairman Upton, Ranking Member Waxman, members of the Committee, I am Patrick Gallagher, Under Secretary of Commerce for Standards and Technology and Director of the National Institute of Standards and Technology (NIST), a non-regulatory bureau within the U.S. Department of Commerce. Thank you for this opportunity to testify today on NIST's role under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" and our responsibility to develop a framework for reducing cyber risks to critical infrastructure.

The Role of NIST in Cybersecurity
NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. Our work in addressing technical challenges related to national priorities has ranged from projects related to the Smart Grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips.

In the area of cybersecurity, we have worked with federal agencies, industry, and academia since 1972 on the development of the Data Encryption Standard. Our role to research, develop and deploy information security standards and technology to protect information systems against threats to the confidentiality, integrity and availability of information and services, was strengthened through the Computer Security Act of 1987 and reaffirmed through the Federal Information Security Management Act of 2002.

Consistent with this mission, NIST actively engages with industry, academia, and other parts of the Federal government including the intelligence community, and elements of the law enforcement and national security communities, coordinating and prioritizing cybersecurity research, standards development, standards conformance demonstration and cybersecurity education and outreach.

Our broader work in the areas of information security, trusted networks, and software quality is applicable to a wide variety of users, from small and medium enterprises to large private and public organizations including agencies of the federal government and companies involved with critical infrastructure.

Executive Order 13636, "Improving Critical Infrastructure Cybersecurity"
On February 13, 2013, the President signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which gave NIST the responsibility to develop a framework to reduce cyber risks to critical infrastructure (the Cybersecurity Framework). As directed in the Executive Order, NIST, working with industry, will develop the Cybersecurity Framework and the Department of Homeland Security (DHS) will establish performance goals. DHS, in coordination with sector-specific agencies, will then support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities, through a voluntary program.

A Cybersecurity Framework is an important element in addressing the challenges of improving the cybersecurity of our critical infrastructure. A NIST-coordinated and industry-led Framework will draw on standards and best practices that industry already develops and uses. NIST coordination will ensure that the process is open and transparent to all stakeholders, and will ensure a robust technical underpinning to the Framework. This approach will significantly bolster the relevance of the resulting Framework to industry, making it more appealing for industry to adopt.

This multi-stakeholder approach leverages the respective strengths of the public and private sectors, and helps develop solutions in which both sides will be invested. The approach does not dictate solutions to industry, but rather facilitates industry coming together to offer and develop solutions that the private sector is best positioned to embrace.

I would also like to note that this is not a new or novel approach for NIST. We have utilized very similar approaches in the recent past to address other pressing national priorities. The lessons learned from those experiences are informing how we are planning for and structuring our current effort. In 2007, the Energy Independence and Security Act (EISA) mandated NIST to develop a standards framework to help with the deployment of a nationwide, end-to-end interoperable Smart Grid. Following a similar approach to the one envisioned for the Cybersecurity Framework, NIST coordinated a forward leaning approach involving more than 1500 representatives from approximately 21 distinct domains that now constitute the Smart Grid.

This effort led to the development of a framework called the Smart Grid Roadmap that defined the domains of the Smart Grid and the interfaces for those domains, identified existing standards for these domains, prioritized standards needs and identified standards gaps. Many of these standards gaps are currently being addressed in various standards development organizations around the world. We are seeing the results of this effort pay off in many ways. Cybersecurity standards are being developed and adopted to secure different elements of the electrical grid. Standards based deployments of secure Smart Meters are enabling consumers safe and secure access to data about electricity usage. The U.S. Smart Grid Roadmap is being used as a template for frameworks in many countries around the world. Automakers are reaching agreement regarding chargers for electric vehicles. All these developments have helped address important policy objectives while also positioning the U.S. as a leader in Smart Grid development and deployment.

Another example of how NIST has brought together the public and private sector to address technical challenges is NIST's work in the area of Cloud Computing technologies. The unique partnership formed by NIST has enabled us to develop important definitions and architectures, and is now enabling broad federal government deployment of secure Cloud Computing technologies.

Developing the Cybersecurity Framework

The Cybersecurity Framework will consist of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks

for critical infrastructure. Once the Framework is established, the Department of Homeland Security (DHS), in coordination with sector-specific agencies, will then support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities through a voluntary program. Regulatory agencies will also review the Cybersecurity Framework to determine if current cybersecurity requirements are sufficient, and propose new actions to ensure consistency.

This approach reflects both the need for enhancing the security of our critical infrastructure and the reality that the bulk of critical infrastructure is owned and operated by the private sector. Any efforts to better protect critical infrastructure need to be supported and implemented by the owners and operators of this infrastructure. It also reflects the reality that many in the private sector are already doing the right things to protect their systems and should not be diverted from those efforts through new requirements.

The Important Role of Standards in the Cybersecurity Framework

I'd like to explain why this approach relies on standards, methodologies, procedures and processes, and why we believe it to be a critical part of our work under the Executive Order. First of all, by standards, I am referring to agreed-upon best practices against which we can benchmark performance. Thus, these are NOT regulations. Typically these standards are the result of industry coming together to develop solutions for market needs and are developed in open discussions and agreed upon by consensus of the participants.

This process also gives standards the power of broad acceptance around the world. Standards have a unique and key attribute of scalability. By this I mean, that when we can use solutions that are already adopted by industry, or can readily be adopted and used by industry, then those same solutions reduce transactions costs for our businesses and provide economies of scale when deployed in other markets, which makes our industries more competitive.

A partnership with industry to develop, maintain, and implement voluntary consensus standards related to cybersecurity best ensures the interoperability, security and resiliency of this global infrastructure and makes us all more secure. It also allows this infrastructure to evolve in a way that embraces both security and innovation – allowing a market to flourish to create new types of secure products for the benefit of all Americans.

Current Status of the Cybersecurity Framework

Underlying all of this work, NIST sees its role in developing the Cybersecurity Framework as partnering with industry and other stakeholders to help them develop the Framework. In addition to this critical convening role, our work will be to compile and provide guidance on principles that are applicable across the sectors for the full-range of quickly evolving threats, based on inputs from DHS and other agencies. NIST's unique technical expertise in various aspects of cybersecurity related research and technology development, and our established track record of working with a broad cross-section of industry and government agencies in the development of standards and best practices,

positions us very well to address this significant national challenge in a timely and effective manner.

NIST's initial steps towards implementing the Executive Order included issuing a Request for Information (RFI) this past February to gather relevant input from industry and other stakeholders, and asking stakeholders to participate in the Cybersecurity Framework process. Given the diversity of sectors in critical infrastructure, the initial efforts are designed help identify existing cross-sector security standards and guidelines that are immediately applicable or likely to be applicable to critical infrastructure.

The responses to the RFI – a total of 244 – were posted on NIST's website. Those responding ranged from individuals to large corporations and trade associations, and they provided comments as brief as a few sentences on specific topics, as well as so comprehensive that they ran to over 100 pages. NIST is currently conducting an analysis of these comments, with our initial observations shared publicly just last week.

NIST is also engaging with stakeholders through a series of workshops and events to ensure that we can cover the breadth of considerations that will be needed to make this national priority a success. Our first such session - held in April - initiated the process of identifying existing resources and gaps, and prioritized the issues to be addressed as part of the Framework. Next week at a workshop hosted by Carnegie Mellon University in Pittsburgh, we will again be working with stakeholders to discuss the foundations of the Framework and the initial analysis.

The approach to the Cybersecurity Framework set out in the Executive Order will allow industry to protect our Nation from the growing cybersecurity threat while enhancing America's ability to innovate and compete in a global market. It also helps grow the market for secure, interoperable, innovative products to be used by consumers anywhere.

Next Steps

The Executive Order requirement for the Framework to be developed within one year, with a preliminary Framework due within eight months, highlights this task's urgency. We have already initiated an aggressive outreach program to raise awareness of this issue and begin engaging industry and stakeholders. NIST will continue bring many diverse stakeholders to the table through a series of "deep-dive" engagements. Throughout the year, you can expect NIST to use its capabilities to gather the input needed to develop the Framework.

Next month, the Departments of Commerce, Homeland Security, and Treasury will submit reports regarding incentives designed to increase participation in the voluntary program. NIST will be supporting the report drafted by the Department of Commerce, which will analyze the benefits and relative effectiveness of such incentives.

In July NIST will host its third workshop to present initial considerations for the Framework, based on the analysis conducted of the responses to the RFI. This workshop will be the most in-depth of the four, with an emphasis on particular issues that have been

identified from the initial work – including the specific needs of different sectors. At eight months, we will have an initial draft Framework that clearly outlines areas of focus and initial lists of standards, guidelines and best practices that fall into those areas

In a year's time, once we have developed an initial Framework, there will still be much to do. For example, we will work with specific sectors to build strong voluntary programs for specific critical infrastructure areas. Their work will then inform the needs of critical infrastructure and the next versions of the Framework. The goal at the end of this process will be for industry itself to take "ownership" and update the Cybersecurity Framework– ensuring that the Framework will continue to evolve as needed.

Conclusion

The cybersecurity challenge facing critical infrastructure is greater than it ever has been. The President's Executive Order reflects this reality, and lays out an ambitious agenda founded on active collaboration between the public and private sectors. NIST is mindful of the weighty responsibilities with which we have been charged by President Obama, and we are committed to listening to, and working actively with, critical infrastructure owners and operators to develop a Cybersecurity Framework.

Thank you for the opportunity to present NIST's views regarding critical infrastructure cybersecurity security challenges. I appreciate the Committee holding this hearing. We have a lot of work ahead of us, and I look forward to working with this Committee and others to help us address these pressing challenges. I will be pleased to answer any questions you may have.

Mrs. BLACKBURN. Thank you. The gentleman yields back, ran a little bit over time there but that is OK. At this time I will begin the questioning, and I recognize myself for 5 minutes.

I want to talk with you first about what you are doing with this framework. Because I think all of us caught, it came to our attention that Secretary Napolitano in congressional testimony earlier this year was still seeking legislation giving DHS the authority to impose the critical infrastructure requirements, and it probably struck many of us odd—I know it did me—that you all are working on this and are looking at a voluntary cybersecurity framework. So shouldn't the Administration wait to see whether your process creates an effective cybersecurity framework before asking for new statutory authority to impose regulations?

Dr. GALLAGHER. So I think the Executive order lays out a clear goal of a voluntary-based system. We agree that the first priority is to allow the market to attempt to address this needed level of cybersecurity performance. That being said, the Executive order lays out sort of two goals once the framework is in place. One is a program to promote adoption of the framework, this voluntary framework by industry, and the other is a recognition that some of these sectors are already regulated, so we would like to see the framework used as a way to harmonize this. I think it would be a mistake if we do all this work on a broad, multi-sector framework for cybersecurity and then not have those practices embraced by those existing regulatory entities. So it really contains both of those pieces.

Mrs. BLACKBURN. Well, let me ask you this then. Why do you think the Administration issued the Executive order if they knew that you were already working and trying to create the framework, and do you think that there is going to be any further push for legislation? If you have got a year, you are going to meet a deadline within a year, you say you are 8 months away from delivering a product. You are holding your workshops, the multi-stakeholder workshops, you are bringing people to the table. So why are they bothering to issue the Executive order and then ask for legislation?

Dr. GALLAGHER. So the Executive order serves to basically align roles and responsibilities across the existing agencies, and you see that in the Executive order, that it choreographs the role of Homeland Security, NIST and other players in a process within our existing authorities. So you are correct: what we are doing now doesn't require any legislation. My personal view is that the primary need for legislation is going to become more important as we look at the implementation and the adoption of the framework. The real win in a framework process is that cybersecurity—good cybersecurity—is good business, and I think what we are going to be looking at is, what are the obstacles that get in the way of adoption of this framework, where are the areas where these practices require incentives and other—or maybe removing barriers to adoption, and so I think the ongoing discussion that has been happening with Congress will likely continue. The Administration looks forward to working with Congress on this, but I think industry won't need our help developing the framework but they may need our help looking at areas where there are barriers to putting this into meaningful use.

Mrs. BLACKBURN. Well, and I think that what we are hearing from industry is that good cybersecurity, solid cybersecurity steps are an imperative. They are not something that is just good business but they are something that are an imperative every single day, whether it is financial networks, whether it is the grid, as Mr. Waxman referenced, whether it is some of our health IT organizations. When you look at the number of attacks and the step-up in that such as the PLA attacks, you know that it is an imperative.

With that, Mr. Waxman, I yield you 5 minutes for questions.

Mr. WAXMAN. Thank you very much, Madam Chair. I agree with your last statement. This is an imperative issue.

Dr. Gallagher, the President's Executive order of Cybersecurity applies to all of the critical infrastructure sectors. I want to ask you about the one that I talked about in my opening statement, and that is the electric grid, because our Nation's critical infrastructure and defense installations are almost entirely dependent on the grid for electricity and they simply can't function without it. When Ed Markey and I wrote to the utilities asking them about cybersecurity, they reported that they feel they are under a constant state of attack. They are targets of daily cybersecurity attacks. Because the grid is so critical and is the target of so many cyber attacks, I think we need to make sure that we are adequately protected. The current industry-controlled approach of issuing mandatory electric reliability standards through protracted and consensus-based process has a poor track record. When it does issue standards, they are at least enforceable, but voluntary standards are not enforceable.

Dr. Gallagher, the cybersecurity framework envisioned by the Executive order would be voluntary. Isn't that right?

Dr. GALLAGHER. That is correct.

Mr. WAXMAN. And because there is no way for a federal agency to ensure compliance with voluntary standards, isn't that a correct statement that there is no way they can enforce it?

Dr. GALLAGHER. That is correct, from a regulatory or legal perspective.

Mr. WAXMAN. You can provide incentives for the private sector to adopt standards, but there is no actual enforcement. Isn't that right?

Dr. GALLAGHER. That is correct.

Mr. WAXMAN. The problem is that recommended voluntary cybersecurity measures have not been adopted by most utilities. I mentioned that in my opening statement, even to the point where compliance with voluntary measures to protect against the Stuxnet computer worm have not been taken, and that is the virus that destroyed uranium enrichment centrifuges in Iran. So I don't find these numbers that we have received from voluntary reporting by the industry encouraging.

The Executive order directs federal agencies to assess whether the cybersecurity regulations governing each sector are sufficient. If they are not adequate, the agencies are supposed to issue new regulations to mitigate the cyber risk, but that raises the question of whether agencies have the necessary statutory authority to issue such regulations. Under the Federal Power Act, the Federal Energy Regulatory Commission lacks authority to issue regulations to pro-

tect the electric grid. Even if they see that it is necessary, they can't do it.

Dr. Gallagher, the Executive order doesn't address this gap in authority, does it?

Dr. GALLAGHER. It does not address that specific issue, correct.

Mr. WAXMAN. So a voluntary approach to cybersecurity may make sense for some sectors but experience has shown that it cannot be relied upon to protect the electric grid. The FERC should have the authority to address cyber threats to the electric grid. That requires legislation from Congress. I hope we will work together on a bipartisan approach, I hope a consensus on the need for that legislation. This is a national security issue and I believe all of us want to work together. That is why we are here today, and we are all expressing our concern about this issue.

Madam Chair, I will follow your lead and yield back a big chunk of my time.

Mrs. BLACKBURN. Thank you, Mr. Waxman. At this time, Chairman Walden is recognized for 5 minutes.

Mr. WALDEN. I thank the chairwoman. Thank you very much, and Dr. Gallagher, thanks for being here.

Dr. Gallagher, networks are obviously very complex and interconnected and themselves rely heavily on information technology products and consumer information technology services. How clear is the delineation? You have the so-called IT exception, and how will that be applied?

Dr. GALLAGHER. So as I understand it, the IT exemption that is discussed in the Executive order pertains to whether the IT equipment and components are identified themselves as a critical infrastructure. In the framework process, they are clearly dependencies. So if we are talking about the energy sector or any other critical infrastructure that is depending on IT—this is about cybersecurity, after all—they will depend on the performance networks and the performance of IT-based equipment. And so the IT sector, the IT companies are already deeply involved with this process. I think the exemption applies to whether they are being specifically identified as a critical infrastructure. I don't think it means they are not involved deeply in the framework.

Mr. WALDEN. So you think they will be then?

Dr. GALLAGHER. Yes, they already are.

Mr. WALDEN. And obviously, flexibility is critical in engaging the private sector to respond to the very rapid evolving cybersecurity threats, especially since networks are themselves varied and rapidly evolving. I don't have to tell you that. How will the framework incorporate such flexibility?

Dr. GALLAGHER. Well, I think the way it adopts flexibilities by relying on the same process that industry relies on to actually develop things like the network itself. The Internet is actually a series of protocols and standards that allow this widespread interoperability. So it has to be as dynamic as the technology they are deploying. What we are basically arguing in the framework is, we want to leverage the same thing to address cybersecurity performance. So it is an industry-controlled process with their own technical experts. They can bring their own technologies to the table as

part of this multi-stakeholder process, and it can be as dynamic as the technology is to address this.

Mr. WALDEN. As you may know, our Subcommittee on Communications and Technology held several hearings on the issue of cybersecurity and cyber threats, and I think every single witness we had said be careful in this area to not overregulate because if you do, the bad actors will know what we have been instructed to do by statute, they will change up faster than you will ever keep up from a statutory standpoint, and that you will bind our hands and misallocate our capital and the resources. Is that a view you share?

Dr. GALLAGHER. So I think the tension between regulation and standards has always been there. Standards and regulation interplay with each other all the time, and frankly, it leads to a lot of confusion in this space. But they really serve different purposes. I mean, I am not an expert in this area, regulatory issues. We would have to work with Congress anyway. We would want to do that. But very simply, in my view, a regulation is needed when the market can't perform. In other words, we are talking about infrastructure whose failure would cause a catastrophic impact to the Nation, and so we don't want that to happen. But the advantage of industry doing as much as it can is self-evident because of what they bring to the table and the fact that so much of this equipment is owned and operated and managed by the private sector.

Mr. WALDEN. Well, I think that is the concern that we have. Later today we have a hearing subcommittee hearing on supply chain vulnerabilities, which, as you know, is a major national and international issue, and I don't know if you have any comments regarding some of those reports that have been in the news. Certainly our colleague, Mr. Rogers, and his committee in a bipartisan way have had some pretty important things to say in this area.

Dr. GALLAGHER. Well, let me start by saying we would like to work with you on that issue. I think supply chains are one of these dependencies that we talk about. The markets for equipment, the markets for software are global, they are interconnected, and we need to understand how do we put together resilient and secure systems out of potentially unresilient, low-trustworthy parts and components, how do we put trust into a system this heterogeneous and this diverse. It is really a very important issue and it is one that has already come up some level in the RFI process for the framework.

Mr. WALDEN. All right. My time is expired. Thank you, Madam Chair.

Mrs. BLACKBURN. The gentleman yields back. Mr. Dingell, you are recognized for 5 minutes, sir.

Mr. DINGELL. Madam Chairman, thank you. Welcome to you, Dr. Gallagher. I would appreciate a yes or no response to the questions if you please.

Dr. Gallagher, I note Section 7(e) of the Executive Order 13636 mandates you publish a final version of the cybersecurity framework no later than February 2014. Will you be able to meet that deadline? Yes or no.

Dr. GALLAGHER. Yes, sir.

Mr. DINGELL. Dr. Gallagher, do you believe that in general NIST has sufficient resources whether in terms of funding or manpower with which to comply with Executive Order 13636? Yes or no.

Dr. GALLAGHER. Yes.

Mr. DINGELL. Doctor, I note that Executive Order 13636 does not grant agencies additional statutory authority with which to address cybersecurity-related risks. Based on your consultations so far in establishing the cybersecurity framework, do you expect the Administration will request the Congress to grant it additional cybersecurity-related statutory authority? Yes or no.

Dr. GALLAGHER. Yes.

Mr. DINGELL. Now, Dr. Gallagher, in general, do you believe that the Administration should be granted additional statutory authority to address cybersecurity-related risks? Yes or no.

Dr. GALLAGHER. Yes.

Mr. DINGELL. Doctor, do you believe that Executive Order 13636 alone is sufficient to adequately address the myriad number of cybersecurity-related threats faced by industry and the government? Yes or no.

Dr. GALLAGHER. No.

Mr. DINGELL. Now, Doctor, a portion of your written testimony is dedicated to explaining the role of standards in Executive Order 13636. You state the standards are agreed-upon best practices against which we can benchmark performance. Thus, these are not regulations. Earlier in your testimony, you stated, and I quote, "Many in the private sector are already doing the right things to protect their systems and should not be diverted from these efforts through new requirements." Do these statements mean that NIST and the Administration do not support the establishment of mandatory cybersecurity regulations? Yes or no.

Dr. GALLAGHER. Well, I think——

Mr. DINGELL. And if you explain it—I think you are going to have to—please do it briefly. Go ahead.

Dr. GALLAGHER. As I said, I think we strongly prefer a private-sector-led solution. A voluntary industry-led consensus process is going to be more dynamic. It is going to be adoptable around the world. It can help shape the technology and the markets in a way that would not be possible if we took a regulatory approach. That being said, the final analysis we have to protect critical infrastructure, and so the real test is going to be as put into practice is it protective of cybersecurity, and if it is not, then I think there is a question for Congress and the Administration in terms of how to——

Mr. DINGELL. And I would assume that you expect that we are going to run into many occasions where we are going to have to figure out what we do and whether or not we are going to have additional changes in the executive orders, regulations or whether additional statutory authority is needed. Is that right?

Dr. GALLAGHER. I would certainly anticipate this will be part of an ongoing discussion, yes, sir.

Mr. DINGELL. Thank you, Doctor.

Now, Madam Chairman, I would like to note in closing that Section 4 of the Executive order establishes a limited information-sharing regime between the federal government and industry. It is

my hope that the committee will continue to examine this issue. It is also my hope that we shall hear from the Secretary of Homeland Security, who is important in the implementing of Section 4 about the effectiveness of information sharing as well as whether the Congress should authorize the liability exemptions that industry claims are necessary to making information sharing function well. I anticipate considerable need for us to engage in active oversight of these matters.

I thank you, Madam Chairman, for your courtesy. Doctor, I appreciate your courtesy and your assistance. I yield back the balance of my time.

Mrs. BLACKBURN. The gentleman yields back. At this time, Mr. Terry, you are recognized for 5 minutes.

Mr. TERRY. I waive.

Mrs. BLACKBURN. Mr. Terry waives. At this time, Mr. Rogers, you are recognized, and you waive. OK. Mr. Murphy, you are recognized for 5 minutes.

Mr. MURPHY. Thank you. I want to go over with regards to working with the private sector, and you had mentioned Carnegie Mellon University in your testimony there, and I understand there is a number of things that are classified in that process as well. You stated also that many in the private sector are already doing the right things. We would look at health policy and financial institutions and agriculture and transportation, et cetera, and we have a limited amount of time and resources to spend on bolstering protections and not spent on burdensome other requirements here. Can you assure us that the whole cybersecurity framework required by Executive order is not going to just be a bunch of regulations, it is going to allow these groups to all work with each other as well and to interconnect among them? So the universities, the private institutions, et cetera.

Dr. GALLAGHER. Well, I can assure you that is our intent, and the way we are trying to make sure that intent follows through is by giving the pen, if you will, to develop the framework to industry and these sectors themselves and then supporting that effort. It is really essential that this be their work product, that this reflects current best practice from across these sectors that identify cross-cutting issues because it is going to be a superior product. It is the only way to do this in the time frame, and it also allows an answer that can basically be driven into the market actually across the entire world.

Mr. MURPHY. Thank you. Madam Chair, I yield back.

Mrs. BLACKBURN. The gentleman yields back. Ms. Eshoo is recognized for 5 minutes.

Ms. ESHOO. Thank you, Madam Chair. Good morning, Dr. Gallagher. Thank you for being here. Thank you for your leadership at NIST, and I want to thank NIST for being one of the cosponsor of the first-ever hack-a-thon that took place in my congressional district this weekend on public safety apps. So I think some really important ideas are going to come out of that and benefit our country.

My first question to you is, you have referred to a critical infrastructure, as have members, and this whole issue of regulation, light touch and/or regulation. What do you consider to be critical infrastructure, number one?

Dr. GALLAGHER. Well, I don't read anything past what is is in the Executive order itself, which is an operational definition that defines it as something whose failure would cause catastrophic harm to the country, and then there is a process in the Executive order that allows for a more specific identification process.

Ms. ESHOO. And how do you, as part of this framework, how do you intend to address the integrity of the supply chain? Chairman Walden raised this, and I wanted to go back to it.

Dr. GALLAGHER. So I think from our view, in supporting an industry-led effort, it is going to basically look at how does the market identify trust in software, in components and in systems. We are talking about companies that will be buying equipment, presumably from supply chains that may be around the world that are going to integrate those into systems that control and manage their critical infrastructure. So the question is, how do we give them the tools to identify trustworthy components and systems in the context of that global market. It is one of these major dependencies that just is part of this type of a system, and we already see that issue coming up from our industry partners in the framework process.

Ms. ESHOO. Now, in this whole issue of cybersecurity, about 95 percent of it is private sector, 5 percent is the government, roughly, and I am pleased that NIST has placed such a prominent focus on public-private partnerships because they are very important. But as you work with the private sector, I think it is very important for you to hear not just from the large companies or the largest companies in the country but small and medium businesses because they offer a rather unique perspective, and given that the congressional district that I represent, people think, members, especially, that when they come to my district they visit Google and Facebook and Microsoft and that they have covered the entire ground. They haven't. I am proud that they are there and that I get to represent them but there is a lot more to it. So how will you ensure that the input of these small and medium sized businesses are incorporated into NIST's cybersecurity framework? And if you could be specific about this, how you are doing it.

Dr. GALLAGHER. In short, we are trying to do everything we can to ensure that companies of all sizes—it is not just the big companies, as you know. Small companies tend to be leading innovators in many cases. It would be a real problem if they were excluded from the process. But even as owner/operators of critical infrastructure, there are companies of all sizes that do that. What we tried to do is make sure that our engagement with the private sector through this process is not just in one mode. In other words, we have the major workshops where we——

Ms. ESHOO. But do you go to them? I mean, where do you go? Do you invite everybody to come to Washington?

Dr. GALLAGHER. No. In fact, we are going to be holding——

Mr. ESHOO. These small startups can't. They don't have time or money to come here.

Dr. GALLAGHER. That is correct, so we have done input that can be done electronically. The request-for-information process was completely virtual. And our workshops are going to be across the country, the first one in Pittsburgh, the second we anticipate in

southern California, and then the third one is still being worked out. So we do recognize the limitations that smaller companies have to do this, and we are trying to design the process so that there is few of barriers as possible to their participation.

Ms. ESHOO. Thank you. I yield back.

Mrs. BLACKBURN. The gentlelady yields back. Dr. Burgess, you are recognized for 5 minutes.

Mr. BURGESS. I thank the chair, and Dr. Gallagher, thank you so much for spending time with us this morning.

On the information that you provided to us, you talk about developing the framework and developing the standards that will be used, voluntary compliance by the industries involved, and one of the panelists we are going to hear from on the second panel, former CIA Director, Mr. Woolsey, talks about the danger from an electromagnetic pulse and talks about the need for surge arrestors to be built into infrastructure. Are you similarly developing the standards for those arrestors and resistors that will be built into the infrastructure for protecting our electrical grid and other systems?

Dr. GALLAGHER. So while remembering, in the United States, NIST does not write the standards. By law, federal agencies look to private-sector standards organizations for their needs. So we ourselves would not be developing the standards.

The framework process, since it is specific to cybersecurity, will probably not have within its scope sector-specific resiliency measures like electromagnetic pulse or geostorm or what have you. However, NIST does support those efforts directly. So in the case of a geomagnetic storms, a lot of the electrical measurement equipment and technology that is needed by the electrical utilities to provide that protective service is work that we do support from our laboratories.

Mr. BURGESS. That is the point I was going to make. Many of us remember the day in the late 1990s or maybe the early 2000s when our little card readers at the gasoline pumps stopped working because of some sort of solar event that had interfered with satellite technology, and so you have that ongoing work in process at NIST. Is that not correct?

Dr. GALLAGHER. That is correct. We think of ourselves as industry's national lab, so as these technical issues come up in their standards process where they want resilient equipment and services, our job is to work on that technology and support their efforts.

Mr. BURGESS. Well, again, we are going to hear a great deal more of this from a witness on our second panel but it just seems that it stands to reason as you build that or as you develop the voluntary compliance standards for that infrastructure that you would build this protection in so that industry and the private sector would be not only aware of the necessity but have a place to go. So often we get into these things and you get overwhelmed by vendors and you don't really know which is the best practice or the best technologies. So that is where I see NIST as really being able to provide some of that direction and some of that leadership in going forward in this. Is that a fair assessment?

Dr. GALLAGHER. Yes. I think it is ironic that the diversity of our approach in the United States, which is one of its strengths, also makes it complicated at times, but that is certainly a role that we

would be happy to take on to help facilitate, provide some clarity, particularly in this area.

Mr. BURGESS. I thank the chair. In the interest of time, I am going to yield back.

Mrs. BLACKBURN. The gentleman yields back. Mr. Green, you are recognized for 5 minutes.

Mr. GREEN. Thank you, Madam Chairman.

Mr. Gallagher, thank you for appearing before our committee today, and it is important that any framework established through the Executive order be truly voluntary. Mandated regulations could quickly become outdated due to a rapidly changing cyber threat landscape and may result in increasing uniformity that may inadvertently add vulnerabilities to intricate systems tailored to specific company operations and risk profiles. How will NIST ensure the framework remains a truly voluntary program?

Dr. GALLAGHER. Well, the most straightforward way is, we simply have no regulatory authority of any type that would make it compulsory. Insofar as supporting industry's intent to have this be something under their control, one of the things that I think we can do is work with them through the framework process to identify how this framework is muscular. I think one of the problems we face is that people are equating the term "voluntary" with "weak", and that is not necessarily the case. Most product safety standards in the United States, many things are in fact fully managed by industry, and industry is quite capable of putting in muscle—what we call conformity assessment tools—to ensure that in business-to-business interactions and so forth that they assure themselves, that they are complying with their own standards and protocols. And I think if that is done, it addresses the performance. I think if what they do is protective of the critical infrastructure, I think that is the best thing we can do to maintain this as a voluntary industry-led process.

Mr. GREEN. As the framework takes shape, demonstrating adherence to the framework should not require submission of company audit results. Sharing of sensitive information with third parties could greatly compromise cyber systems, so specific information regarding cyber systems must remain propriety to protect the information from the public and cyber criminals. Has NIST developed a method to determine adherence to the framework, and will they take into consideration the sensitive information that different companies and plants may provide?

Dr. GALLAGHER. So NIST itself would not play a role in assessing compliance with the framework. Our preference would be for industry to develop as part of the framework the vehicle by which they would determine the compliance mechanism. What we can do is share a number of best practices and models where that has occurred in other areas including smart grid and cloud computing and show them the pros and cons of these different models. It addresses many of the concerns you just raised, which is in the business environment, they can set this up so that they are not sharing competitively sensitive information and propriety information in a way that they don't want to. In other words, the conformance assessment program can be compatible with their business needs.

Mr. GREEN. I appreciate that. I know a lot of us represent different entities who have a big stake in this, and they are already doing a lot of things. In my area, my refineries, chemical plants, of course, all of us have utility plants, that this cybersecurity threat is being addressed now and they are standards being developed, sometimes by companies, sometimes by industry, and that is my concern, that we make sure that we don't get in the way of some of the innovations that literally can be found out every day.

So Madam Chairman, I appreciate the time. Thank you. I yield back.

Mrs. BLACKBURN. The gentleman yields back. Mr. Scalise, you are recognized for 5 minutes.

Mr. SCALISE. Thank you, Madam Chair. I appreciate you holding this hearing. Dr. Gallagher, thank you for being with us today.

You mentioned in your testimony that regulatory agencies will review the cybersecurity framework to determine if any requirements, if the current requirements are sufficient but also if there would be any proposed new types of actions. When I look at that and I see words like "requirements" and "actions," is that something that is synonymous with regulations?

Dr. GALLAGHER. Not to me, but you are not the first person that has noticed the connection.

Mr. SCALISE. So there are no proposals right now to come out with actual regulations when you talk about requirements or actions?

Dr. GALLAGHER. So in my experience, here is what I have learned when you are dealing with standard setting that potentially touches regulatory agencies. So some of these sectors are currently regulated. It would be a mistake for the framework to not be germane to what the regulators are doing. Then it wouldn't be addressing the underlying need to protect those sectors in this case. On the other hand, you don't want so close of a relationship that the standard setting is effectively a regulatory process.

Mr. SCALISE. I know you are familiar with legislation that we have moved through the House to expand the ability for the private sector to share information with the government to find out about threats but all on a voluntary basis where private information would be protected, where if a private entity didn't want to go and talk to DOD about maybe things that they are seeing from China or Russia or some other country or entity, they don't have to do that, but then there would be the ability for them to do it if that benefits them in looking at breaches that are maybe coming their way. And so voluntary is very different than new requirements that would be mandatory. You understand the difference that we are looking at there?

Dr. GALLAGHER. Yes. The intent of the framework is not to drive the establishment of new requirements. That portion of the Executive order, to my understanding, is a harmonization issue, which is we want any existing regulatory agency to consider the framework when it is complete. It may be something they can harmonize against, which would remove duplicative requirements to those companies. It could very well be that it addresses the underlying need, and they could actually lighten any specific regulatory requirements. But in our view, it would be a mistake for them not

to consider the framework in light of what they were doing before the framework was there.

Mr. SCALISE. So when you talk about the Executive order that would establish this framework, you also talked about incentivizing private companies, other entities that have critical infrastructure to adopt this new framework that you are developing at NIST. What types of incentives are you talking about?

Dr. GALLAGHER. So I think at this point we don't know what the specific incentives are, so the Executive order actually asks a number of agencies to contribute reports identifying potential areas. We have done this through a public comment period and we are distilling those comments now. I think the way to understand this is that we want the framework adoption to be tantamount to good business. In other words, good cybersecurity is good business. They are compatible functions within these companies, and I think the best way to view the incentives question is to what extent are there barriers or, in some cases, you know, counterincentives to doing the right thing. Those are the things I think we will work with you together to make sure that we align business interests with doing good cybersecurity.

Mr. SCALISE. Right, and again, in our legislation, we have some liability protections. We don't want somebody to feel like if they are coming to the government to work together in a partnership that that is not going to expose them to some other kind of liability if their intent is to protect their network and ultimately all of the users. I mean, my constituents, everybody's constituents that are out there that give personal information to various Web sites, they do it under agreements. If you are on Facebook or any other Web site, you have got an agreement. You know that there are agreements that your personal information is going to be protected. Of course, if some other country, some entity is trying to break through a firewall, then they are also trying to get your personal information. So you want that to be protected. So I am just trying to find out, does NIST have some definition of incentive when you are trying to get this?

Dr. GALLAGHER. At this time NIST does not but what I can share with you is a preliminary look at some of the comments coming in from the RFI to the Commerce Department. They include things like liability protections, exploring the establishment of insurance markets where the risk can be monetized in business-to-business relationships, procurement preferences for companies that are supporting the framework to offer high-quality products and services. It is things of that type.

Mr. SCALISE. And I would just ask—I know my time has run out—I would just ask if you could share that with the committee as you are developing those definitions of incentives, if you could just share that with us along the way and some of the things like the liability protections are things we have already hashed out and embedded here. Maybe you could look at those things that we have already identified as well.

Thanks a lot, and I yield back the balance of my time.

Mrs. BLACKBURN. The gentleman yields back. Mr. McNerney for 5 minutes.

Mr. MCNERNEY. Thank you, Madam Chairman.

Thanks, Dr. Gallagher, for your work on this issue, and you clearly have a good grasp of it and you are sharing the wealth so it is understandable.

One of the things that you mentioned and I think comes up often is the idea of performance-based standards, and I would like for you to just talk a little bit about what that means, maybe give an example, and also give an example of a non-performance-based standard so we will have a clear idea of what we are talking about here.

Dr. GALLAGHER. So simply, a performance-based standard is one where the standard addresses a given level of performance and it is less prescriptive about how you get it done. So an example would be this smartphone needs to talk to this network. That is a performance requirement for interoperability in that case but it doesn't prescribe the exact data format, electrical format that would happen. What a performance requirement then does is allow a diversity of technical solutions that can achieve the same performance level, and that is why these are preferred. They give companies, particularly in technology fast-moving areas, the flexibility and latitude to continue to innovate and perhaps even meet the performance requirement in improved ways.

Mr. MCNERNEY. Well, what would a performance-based standard in cyber look like or sound like?

Dr. GALLAGHER. Well, I think that is the exact question we are going to be putting in front of the industry groups through the framework process. You know, measuring and assessing good cybersecurity performance, and I am saying this as head of a measurement agency, is actually a challenging problem. You know, coming up with the right way of characterizing this, and I think it is probably going to be a diverse set of metrics that they look at. Some of these are going to be looking at best practices in terms of removing vulnerabilities. That would be one type, known vulnerabilities and minimizing that threat surface, if you will, in companies. And the other part is going to be this adaptive part of cybersecurity, which is, do you have the intrinsic capability to take new threat information and to adjust the protective measures you are taking within the company. So I wish I could give you an easy, straightforward answer to that one but I think that is going to be one of the issues that the entire framework community is going to be dealing with.

Mr. MCNERNEY. Well, I spent some time developing standards in the mechanical engineering fields, and it is long, it is painstaking, and often it gets watered down so much that it is not very useful, and I am worried about that in this sort of a framework. Do we have the chance of ending up with something that is so watered down that it is not useful?

Dr. GALLAGHER. So consensus, of course, doesn't mean unanimity, as you know from that experience, and I think you are exactly right. One of the threats you face in a multi-stakeholder process is that in an effort to achieve agreement, you go to the lowest common denominator. And that is why the performance goal of having high-performance cybersecurity is going to be so important to this. I think what we are striving for here is a framework that reflects best possible achievement at commercial levels of perform-

ance. That would allow additional support, for example, in the public-private space where support from our intelligence agencies and operational agencies can support the private sector but not asking them to carry out that role. But it also reflects that we can't race to the bottom and just find the lowest common denominator of technical performance and call that adequate.

Mr. MCNERNEY. Now, are you going to be including foreign companies in this collaborative process?

Dr. GALLAGHER. Yes.

Mr. MCNERNEY. It would be hard not to because——

Dr. GALLAGHER. I would hope they do, actually. One of the interesting parts of this is, by doing this through the market, and the market in fact is global, what we can do is end up with a baseline level of performance that is reflected in products and services sold around the world. In fact, if we had taken a regulatory approach first, that would be unlikely to happen because as soon as a U.S. regulatory agency said this is the requirement, it becomes a counterincentive to any adoption in other countries, where if this is coming from industry, very naturally I think one of the real strengths here is that we can drive this base level of performance into the global marketplace. That doesn't preclude governments from adding any additional requirements on top of that but I think it best for companies because it lets them sell their goods and services around the world, and it is good for us because the Internet is itself a global infrastructure, and I think if we can drive this intrinsic security performance up, that is better for all of us.

Mr. MCNERNEY. I think this is an opportunity for real, true bipartisan work. Thank you, Madam Chairman.

Mrs. BLACKBURN. The gentleman yields back. Mr. Latta, 5 minutes.

Mr. LATTA. I thank the chairlady, and I appreciate you all being here today. This is a topic that is not just on everyone's mind here in Washington but back home. You know, in the last 24 hours before I came back, there was an article in the New York Times, China back to hacking United States alleges, experts say agencies, firms battling new attacks. There was a front-page story yesterday also in the Washington Post about Chinese hackers, and it is a real issue, and I represent 60,000 manufacturing jobs back home and a lot of businesses that are very concerned with this. One of the things that I started doing with the cybersecurity with the FBI in Ohio, we have done cybersecurity events in the district, we are doing one next week, to get the FBI in to really explain to people how serious things are out there. So I really appreciate you all being here because it is a topic that is on top of everybody's mind.

In your testimony, on page 4, if I can just ask you a couple questions about that, it says that your request for information under the RFI this past February, you know, you have received 224 responses so far. Have you been able to analyze any of those responses and are you seeing any kind of a trend right now, and who has been responding? Is it overall in the industry or is it a broad section?

Dr. GALLAGHER. It is actually remarkably broad. As I said, we have heard from some of the largest companies and industry associations. I think in the next panel you will hear that many of the

participants there, their companies have participated in the process. It crosses all the sectors. We did publish last week, and it is posted on the NIST Web site, a preliminary analysis of the responses. In fact, we chart out and tabulate the areas that are represented and the types of issues that were coming up through the public comment period. That is part of the homework assignment that has been given to the framework participants for their first workshop in Pittsburgh next week.

Mr. LATTA. Well, thank you, and also, you know, just maybe to sum up, because in the interests of time, that, you know, one of the things, you commented in your testimony and also I have heard over and over from folks out there that one size does not fit all, that we can't create one thing here in Washington because, again, on the industry side, things are moving so quickly on theirs that we try to do something here, and we will be just three, four, five steps behind.

The other term that I always know that worries people back home is the word "voluntary" and they want to make sure that anything that is done is always voluntary, and as my colleague from Louisiana just mentioned in a question about incentives, incentivizing, those are terms that also we want to really make sure that we know what is going on. So Madam Chair, in the interest of time, I yield back.

Mrs. BLACKBURN. The gentleman yields back. Mr. Tonko, you are recognized for 5 minutes.

Mr. TONKO. Thank you, Madam Chair, and let me thank Chair Upton and Ranking Member Waxman for arranging today's very important hearing. Critical infrastructure represents a wide range of industries, and interestingly, many fall under the jurisdiction of E&C. So we need to take a serious look at how to improve these industries' resiliency from cyber threats.

Let me welcome you, Dr. Gallagher. I know that you have an awesome task assigned your way, but I also appreciated your recent visit to the core of my district. It was well received. And I commend NIST on its leadership in implementing some very important guidelines here. NIST has received tremendous feedback from stakeholders, and it appears that NIST has recognized that cybersecurity can best be addressed through a cooperative public-private partnership. So it is clear that this has been a collaborative effort, and I am grateful that you appear before this committee today.

President Obama expressed concerns with the cyber legislation recently considered in the House because of privacy and civil liberties issues. His Executive order makes promoting these rights an explicit priority. Many of the testimonies we will hear today will make mention of that importance. Has NIST or DHS's Office for Civil Rights and Civil Liberties been in discussion with privacy and civil liberties groups while working on implementation?

Dr. GALLAGHER. So in the case of the framework process, which is fairly new, I am not specifically aware of any discussions, but prior to that, through Commerce Department efforts looking at both privacy and non-critical infrastructure, we interacted quite extensively with those groups. I think from a framework perspective, it comes up in two areas. One is privacy is about sharing the ap-

propriate information you want to share and nothing else. That is a technically enabled capability, and so at the technical level, the capacity to implement privacy is in fact a deep part of cybersecurity and will be part of the framework process. The other part of the Executive order where this is obviously is in the information sharing and coming to terms with what information is needed to share to carry out the protective function.

Mr. TONKO. And according to your testimony, next month we are expecting reports about the potential incentives designed to increase participation in the framework program. Aside from liability protection, which was considered in the House as cyber legislation, and I think demanded by industry, what types of incentives are possible? Which of these will need legislation perhaps to implement and which can be done right away?

Dr. GALLAGHER. So what we are seeing in the RFI process includes a broad range of incentives. Some would absolutely require legislative action to occur. Those are things like liability protection, supporting reinsurance markets and how does that work. Looking at tax incentives potentially to support some of the capital investments to upgrade cybersecurity performance including, in some cases, supporting grant programs for promoting innovation, some of the R&D activities related to promoting good cybersecurity. Other areas appear to fall within existing authorities, and that would be things like alignment, do you create procurement preferences in the federal government that would support the adoption of the framework. In some cases, things were proposed that would not be a good idea and so I think the report will be very useful in particular to Congress as it considers this continuing question about how do you promote industry's work to do the right thing on cybersecurity and eliminate barriers and support adoption.

Mr. TONKO. Thank you. And 150 of the 244 responses to NIST's request for information discuss the workforce's cyber capabilities. We obviously have to recognize this workforce will be a vital and growing contributor to our economy in the future. It is not hard to imagine the need for constant training. So what types of education, training and research opportunities can we invest in to ensure that the private sector has access to the highly skilled personnel necessary to implement and maintain some rigorous cybersecurity standards?

Dr. GALLAGHER. I think this is going to continue to be an area that we will have to work on aggressively. So outside of the framework process, NIST was asked to be an interagency coordinator, if you will, on interagency efforts to look at cybersecurity education across the federal government, and it basically has three broad approaches. One is promoting widespread cybersecurity awareness to the public—very important because they are interacting with this infrastructure as well. The other one is promoting interest in those that would elect to take this direction as a career, so that is, do we have the cadre of talented people moving in this direction who would see cybersecurity as a place where they can contribute and have a worthwhile career. And then the final piece is for somebody who has made that decision, can they get the appropriate education and workforce-specific training where they can contribute by the

way both federal and non-federal, so we have worked with a lot of outside stakeholders.

When you have those three pillars, there is a pretty broad range of activities. Some are awareness campaigns and some are looking at working with leading universities. In fact, NSA and DHS have played a leading role in that space working with universities to accredit cybersecurity education, and in the middle that promoting interests are some of the things that are being done in high schools and middle schools trying to promote broader interest in cybersecurity and the roles that some of the career possibilities that are there for folks at that formative period of time.

Mr. TONKO. Thank you very much, Dr. Gallagher, and with that, Madam Chair, I yield back.

Mrs. BLACKBURN. The gentleman yields back. Mr. Lance, you are recognized for 5 minutes.

Mr. LANCE. I waive.

Mrs. BLACKBURN. Mr. Lance waives. Mr. Cassidy is gone. Mr. Olson for 5 minutes.

Mr. OLSON. Thank you, Madam Chair, and thank you, Dr. Gallagher, for being here this morning.

Cybersecurity is very important to my home district, Houston, Texas. Obviously we are the energy capital of the world. We have the world's largest petrochemical complex lining the 15-mile-plus Houston ship channel, which serves the Port of Galveston, the Port of Texas City, the Bayport Container Terminal and the Port of Houston. We have a massive pipeline infrastructure which supports that petrochemical industry. We have two nuclear reactors 90 miles away down in Bay City, Texas. We are about to become the third largest city in terms of population. Sorry to my colleagues from Chicago, but those are the facts.

So my point is, lots of damage can be done to America in terms of dollars to our economy, in terms of lives by cyber attacks in Houston, Texas, and as we know, one of the most important ways to combat cyber attacks is for companies and the federal government to work together to combat cyber attacks through robust information sharing, and that is why I voted for the Cyber Information Sharing and Protection Act last month because, as you know, the information-sharing process authorized by CISPA is completely voluntary, only ones and zeros, binary code, if my degree from Rice from 1985 in computer science is still relevant. No personally identified information will be exchanged between the private sector and the federal government. The House has done its job, and that is why I am encouraged by the Administration's commitment to a voluntary process that solicits input from industry to create the cybersecurity framework.

My question is, as you know, cyber attackers adapt quickly with new attack methods almost overnight. How does the Administration and NIST plan to balance any additional regulatory requirements with the need for industries to remain flexible and be able to adapt to the changing cybersecurity environment?

Dr. GALLAGHER. Well, one specific example I can give to that is something that you have probably heard quite a bit, which is the response capability for IT systems has to become quicker. In essence, we have to fully automate a lot of this response. It has to

move at the speed of computation rather than human speed, and that in some sense is a policy issue. A lot of the information-sharing debate is around that, how do we enable that flow of signatures and key information to enable that, and some of that is the underlying technology. If I receive that threat information and I am a system operator, how do I deploy that automatically? And so NIST has been working with industry on developing security automation tools and protocols that can be deployed and can be used within their systems and can provide an interoperability between different vendors of software and different vendors of IT equipment to enable share of cybersecurity-specific information across these platforms. So we are trying to support what I think is going to be a movement towards full-scale automation of a large amount of the cybersecurity activity.

Mr. OLSON. Thank you. I yield back the balance of my time.

Mrs. BLACKBURN. The gentleman yields back. Ms. Matsui, you are recognized for 5 minutes.

Ms. MATSUI. Thank you very much, and I would like to welcome Dr. Gallagher here. Cybersecurity is both a national and economic security issue, and I believe that industry and government must be partners in addressing our Nation's cyber threats. It is not a one-way street, and I believe the Administration's Executive order was a good first step but more will need to be done.

Last October, I wrote to the White House urging them to consider the implications of including interactive computer services such as search engines and social networking platforms. I believe the Executive order got it right and made it clear that there is a fundamental difference between networks that manage infrastructure critical to public safety and those that provide digital goods and services to the public.

Dr. Gallagher, how should federal agencies ensure that any sector-specific cybersecurity standards required under the cybersecurity framework are not imposed on non-critical infrastructure?

Dr. GALLAGHER. Well, as I said, I believe the question of imposition is going to be one that largely falls to Congress and, you know, those agencies with sector-specific responsibilities. I actually view this almost in reverse, which is the actions we are taking to work with this broad collection of companies and interests to develop a set of general practices for cybersecurity performance may in fact be usable, in fact, cost-effectively usable, very broadly, in fact, maybe in areas outside of the specific critical infrastructure. So it could very well be that companies that are in media and other areas would now find it easier to buy secure equipment and secure software and lower vulnerability. This would be, in my view, a win. So without imposing any requirement, we still get the benefit of improved security performance.

Ms. MATSUI. OK. Now, how will the Executive order and the cybersecurity framework assist federal agencies in enabling more uniform security measures across all government-operated data centers?

Dr. GALLAGHER. So this is part of the discussion that we have been working on pretty actively very recently, which is, how do we get the federal agencies to align to this framework process. I think

if the private sector is going to go to all this trouble in developing this high-performance cybersecurity baseline, then I think the federal government should leverage that for a number of reasons. One is, it will be a high-performing platform to use that as a baseline for any additional requirements that it would have internally, and also it helps achieve market scale. In other words, some of the government procurement now becomes supportive of helping the companies drive adoption.

Ms. MATSUI. OK. That is good.

Dr. GALLAGHER. So I don't think we have any answers to that yet but that is certainly something we are actively discussing right now.

Ms. MATSUI. OK. Now, with the electricity subsector already subject to mandatory and enforceable cybersecurity standards, how is NIST working to ensure that the framework will include these existing standards?

Dr. GALLAGHER. Well, what we have done is, we have invited those entities in from the beginning. So in fact, in the case of the electricity sector, that is fairly straightforward because in fact we are modeling a lot of this effort after the interaction we have had with that sector in smart grid. So we have well-established relationships with those companies, with those regulators, with those industry associations, and we have in fact not only invited them into the process but suggested that they, like other high-performing sectors, put their practices on the table as best practices for consideration under the framework.

Ms. MATSUI. OK. Now, another topic I would like to raise is securing the cloud. I am pleased that the Administration continues to pursue its Cloud First policy and is adopting cloud technologies to make the federal government more efficient and effective. Now, most government agencies are now adopting these cloud services. What kind of cyber protections and threats and what kinds of challenges do you foresee as the government continues to adopt cloud services?

Dr. GALLAGHER. So in the case of government adoption of cloud, almost more than the technological challenges of dealing with this are that cloud in some sense breaks policy. Government-used policy for IT is based on the assumption that we are the owner/operators, that this is an enterprise system within our agencies and we manage and configure and control all of these assets. Cloud changes that because many of these assets now are provided via contract; they are services. And that shift now creates a challenge, which is, how do I meet my responsibilities as an agency head to protect my IT systems when my relationship with those that are operating that equipment or holding my data or running my applications has evolved. And so what we have been trying to do is work with a process where the cloud community, the companies and cloud service providers, are working with the CIOs from across the federal government and basically mapping out the different use cases, very specific use cases where we can take a government application, expose the requirements that those agencies have to meet, and then turn to the business community and say how do you help us ensure that we meet those requirements in this new space. So that is leading to a pretty robust process where some of the more straight-

forward areas we have been able to be early adopters. Some of the more challenging areas, at least we have identified the specific things we have to work on if we are going to go there.

Ms. MATSUI. OK. Thank you. I see my time is up. Thank you.

Mrs. BLACKBURN. The gentlelady yields back. Mr. McKinley, you are recognized for 5 minutes.

Mr. MCKINLEY. Thank you, Madam Chairman.

Dr. Gallagher, you may or may not be familiar. In West Virginia in the Fairmont area on that I-79 corridor, there is a consortium of about 50 different firms that are very much involved called the West Virginia High Technology Consortium. This issue is probably one of the most important issues facing them, so as a personal privilege, I am asking if we can get someone from Commerce to come sit down and talk to them about this because it is by far one of the most important issues other than perhaps sequestration.

Dr. GALLAGHER. We would be happy to.

Mr. MCKINLEY. We got a few questions from some of them, and I would like to share that. One was, what is the percentage of industry that should be represented as a minimum to ensure that these initiatives have been successful?

Dr. GALLAGHER. So I frankly haven't approached this from what fraction have to be involved in the development process. In the normal industry-led consensus process, you often don't get high penetration where the majority of companies are involved. But those that have key technology and key drivers, the question is making sure that the standards aren't shaped without having the right ideas around the room. I think the more important test for success is at the other end, which is what is the level of adoption. If these are really useful, if these are aligned with business practices and if these are high-performance, good cybersecurity practices and we don't see widespread adoption, that will be something I worry about.

Mr. MCKINLEY. I guess as an engineer, I always like the metrics. I want to see how the metrics work. I know under Section 2, it defines from a 30,000-foot elevation what the definition of critical infrastructure, but down where you and I are on the ground, who is actually going to make those calls? What encompasses critical infrastructure?

Dr. GALLAGHER. I believe in the Executive order, that decision is made by the Department of Homeland Security. I know it is not NIST. And I believe it is based on determination under that operational definition that is given early in the Executive order. That determination is basically for purposes of supporting participation in the voluntary program.

Mr. MCKINLEY. And then in the Executive order, there is what is called the greatest risk list. That is interesting. Given all the discussion here in Washington lately about lists, who is going to be maintaining that list and following up with that list and who is going to be implementing based on that list?

Dr. GALLAGHER. I am not an expert on the list but my understanding is, that is Department of Homeland Security responsibility and it is to assist them in prioritizing in a risk-based fashion, so if they are going to be taking risk-based actions, they are trying to conform themselves of what would be the highest risk from in-

dustry so they can appropriately prioritize. But I would have to couch with that, you should double-check that with the Department of Homeland Security.

Mr. MCKINLEY. Thank you very much. I do hope that we will see you at the high-tech foundation where we can all get together and see if we can put to rest some of their concerns. When you are talking about 50 firms, probably as many as 50 firms all interacting, it is very much of a concern how much is their exposure.

Dr. GALLAGHER. One of the great things we don't have to worry about here is the companies not being behind this. They, I think, understand more than anyone how critically important this is, and that is probably our biggest ally in this entire effort.

Mr. MCKINLEY. Thank you very much. Madam Chairman, I yield back the balance of my time.

Mrs. BLACKBURN. The gentleman yields back. Ms. Schakowsky, you are recognized for 5 minutes.

Ms. SCHAKOWSKY. Thank you, Dr. Gallagher. I am trying to understand how the framework interfaces with the CISPA legislation. You know, there were some of us including the White House who felt that there were some deficiencies in the bill as it was voted on in the House, particularly dealing with reasonable efforts on the part of the companies, which of course we want to voluntarily comply, but in making sure that personally identifiable information wasn't shared among each other or with the federal government, and actually at the time when we were holding hearings in the Intelligence Committee, Paul Smoker from the Financial Services Roundtable argued that companies should be responsible for minimization, stating, "The provider of the information is in the best position to anonymize it," and then there was also a question of John Engler, President of the Business Roundtable, if he thought it was too much of a burden to ask the private sector to "take reasonable steps where reasonable steps can be taken" to minimize information, and Engler replied, "No, I think it's reasonable. I think it's exactly fine." So that was one of the issues that raised in the SAP, the statement recommending a veto of the legislation, and the other was the broad immunity provision that was given. Is the framework consistent with what the White House has said about CISPA? Is it different? If you could explain that?

Dr. GALLAGHER. So the way I understand it, of course, nobody is in disagreement that we have to enable information sharing. So the debate about CISPA in some ways are technical issues about how do you appropriately limit the scope of the information that is being shared, and the scope of the liability protection, and I leave that to the experts. What the framework does is in some ways enable that information sharing. In other words, if you receive threat information through information sharing, can you act on it, how do you deploy that protection through your system. In some ways, the framework may provide an answer to this question of cost-effectiveness of some of the things like minimization. If it is costly now for a smaller company to minimize information, it could very well be that through the framework process, we identify some technical means that are embedded in the technology that are supportive of this. So I think it is not that the framework depends on compatibility with CISPA or with the Administration position but it is re-

lated to information sharing in the sense that the adaptive part of cybersecurity, taking new threat information and being able to act on it, is a key part of the performance level we need to have. Hopefully the framework can provide some technical assistance in that as it goes forward, and it will be nice because that technology assistance will be coming directly from the industries that have to put it into practice.

Ms. SCHAKOWSKY. I thank you for that, and I yield back.

Mrs. BLACKBURN. The gentlelady yields back. Mr. Griffith, 5 minutes.

Mr. GRIFFITH. Thank you.

I appreciate you being here today, and obviously we are all trying to struggle through some concerns about privacy and appropriateness and when the government should be looking and when they shouldn't. But I think most of those questions you have already answered, and so I am willing to yield back, Madam Chair.

Mrs. BLACKBURN. The gentleman yields back. Mr. Rush, you are recognized for 5 minutes.

Mr. RUSH. I want to thank you, Madam Chairman, and some of these questions may have been asked and answered already, but I think I have a different kind of slant on it.

The Department of Homeland Security, nothing that cyber attacks against federal agencies increased 782 percent between 2006 and 2012 for 48,562 separate incidents reported in 2012 alone, and a number of experts have estimated that the economic impact from cyber crime to be in the billions of dollars each and every year, and we know that here in the United States, our most critical infrastructure including the electric grid, oil pipelines, communications networks and financial institutions, all are vulnerable to manipulation or attack by malicious actors who use technology in all parts of the world, and my constituents are as alarmed as most of America is about it. So are you confident that NIST has all the tools and the authority it needs to successfully implement cybersecurity framework in order to minimize and mitigate the risks of attack on the digital infrastructure?

Dr. GALLAGHER. I think if the responsibility fell solely on our shoulders, my answer would be absolutely not. I would not believe we would have the capacity. But the approach we have taken is to actually get behind an industry-led effort. And so since so much of the capacity and the know-how and the expertise and the technology and the leadership comes from industry, and our role is to convene and support that effort, I am quite comfortable that we can do that.

Mr. RUSH. So this alliance of industry, are you satisfied with the level of participation and the level of concrete outcomes so as to prevent organized cyber attack?

Dr. GALLAGHER. I am in fact very satisfied. My biggest concern when the Executive order process was announced was, would the concerns over potential regulation later, which has been part of the public debate, basically result in companies electing not to participate in the framework process. That de facto boycott would have been devastating. That would have been a failure of this entire process. And in fact, the opposite has happened. I would say there has been a very strong tipping-in effect. Companies, I think, have

fully appreciated that letting them drive this process and own it and run it at market scale has enormous advantages, and I have been gratified, and I think the origin of any optimism I have here is based on the fact that we have so many leading companies participating in this effort. It is going to make all the difference.

Mr. RUSH. I don't know of anything that I can think of that doesn't have challenges, and what are the challenges that this framework faces and what are some of the challenges that NIST faces?

Dr. GALLAGHER. I would agree. In fact, the sign of maturity that you should look for in a couple months is that we are up to our eyeballs in challenges. That means that this has become very real. I think there is going to be lots of them. At the very highest level, I think the challenge I am most interested to see how to resolve is the integration of cybersecurity into the business practices of these entities. This can't be a bolt-on, add-on activity that companies do. It has to be embedded in what they do, and that means integration with the risk management that they do, with their business functions, with their costs. It has got to be good business to do good cybersecurity, and I think that is going to raise a number of interesting challenges. Some of those may touch on the incentive discussions that we have already had. But I think that among what will certainly be a long list of technical challenges and areas where we just have to do better and find better solutions.

Mr. RUSH. Thank you, Madam Chair.

Mrs. BLACKBURN. The gentleman yields back. Mr. Johnson, you are recognized for 5 minutes.

Mr. JOHNSON. Thank you, Madam Chair. First of all, thank you, Dr. Gallagher, for being here today. I don't really have any questions but just a brief comment.

I spent nearly 30 years of my professional career in information technology, and I certainly understand the challenges that we face with cybersecurity. There are those that will always be out there that because they can, some of them for no other reason than that, try to wreak havoc and disrupt our networks. Some have a much more malicious intent in stealing information that doesn't belong to them, taking down our capabilities and so forth. So I am grateful to be serving on a committee here that takes this issue very, very seriously because I think it is indeed a very, very serious issue and I look forward to working with my colleagues and the Administration to make sure that we do the right things, and with that, Madam Chair, I will yield back.

Mrs. BLACKBURN. The gentleman yields back. Chairman Pitts?

Mr. PITTS. I will waive.

Mrs. BLACKBURN. The chairman waives. Mr. Harper?

Mr. HARPER. Thank you, Madam Chair, and Dr. Gallagher, thank you taking the time. You can see by the attendance in here, this is a very important subject, and we appreciate your insight today.

I am blessed to have a great university in my congressional district, Mississippi State University, which is designated as a National Center of Academic Excellence by the National Security Agency and the Department of Homeland Security in information assurance education. So my question is, what has academia's role

been in the formulation of cybersecurity framework, and do you see that role expanding?

Dr. GALLAGHER. I do, and I think that it is going to draw on the two great strengths of academia. I think on one hand it is the education of our youth and providing the knowledge base and the talent and the expertise to address this. This is not an easy thing, and it is going to need our best and brightest minds on it. And the other area is actually in the research function of our universities. I think we don't have all the answers. I think there is areas where the technology can do better, and I think we count on them to come up with those breakthrough ideas that will make this all a much more addressable problem. So I think it is going to draw on their two core strengths.

Mr. HARPER. Thank you, Dr. Gallagher, and with that, I yield back, Madam Chair.

Mrs. BLACKBURN. The gentleman yields back, and Dr. Gallagher, that concludes our questioning for today. You have been very patient, and it will conclude our first panel, but before you go, I have to tell you, you mentioned for your workshops, you have said southern California and Pittsburgh. Nashville, it ought to be on that list. We would appreciate that. And we will go into recess for a moment while we set the second panel.

[Recess.]

Mrs. BLACKBURN. At this time we are ready to begin our second panel. I thank you all for moving quickly into your spots so that we can move forward. We welcome our second panel: Mr. Dave McCurdy, President and CEO of the American Gas Association; Mr. John McConnell, Vice Chairman of Booz Allen Hamilton and former Director of National Intelligence; Ambassador James Woolsey, Chairman of Woolsey Partners and former Director of Central Intelligence; Mr. Mike Papay, the Chief Information Security Officer and Vice President for Cyber Initiatives at Northrop Grumman; Dr. Phyllis Schneck, Vice President and Chief Technology Officer, Global Public Sector for McAfee. And I yield to Mr. Lance for the next brief introduction.

Mr. LANCE. Thank you, Madam Chair. I have the honor of introducing Charles Blauner from Citi, who is the head of information security for that great company, and he has extensive experience in both New York and London, and he is a resident of the district that I serve. He lives in Basking Ridge, Bernards Township, Somerset County, New Jersey. Thank you, Madam Chair.

Mrs. BLACKBURN. The gentleman yields back, and we continue with Mr. Duane Highley, the President and CEO of Arkansas Electric Cooperative Corporation. Mr. Highley is appearing on behalf of the National Rural Electric Cooperative Association. And Mr. Robert Mayer, the VP of Industry and State Affairs at the United States Telecom Association. You all sound like the cast of characters in a sci-fi movie, and we are delighted that you all are here. Mr. McCurdy, we begin with you for 5 minutes of testimony to summarize.

STATEMENTS OF HON. DAVE MCCURDY, PRESIDENT AND CEO, AMERICAN GAS ASSOCIATION, AND FORMER CHAIRMAN OF THE HOUSE INTELLIGENCE COMMITTEE; JOHN M. (MIKE) MCCONNELL, VICE CHAIRMAN, BOOZ ALLEN HAMILTON, AND FORMER DIRECTOR OF NATIONAL INTELLIGENCE; AMBASSADOR R. JAMES WOOLSEY, CHAIRMAN, WOOLSEY PARTNERS LLC, AND FORMER DIRECTOR OF CENTRAL INTELLIGENCE; DR. MICHAEL PAPAY, VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER, NORTHROP GRUMMAN INFORMATION SYSTEMS; DR. PHYLLIS SCHNECK, VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, GLOBAL PUBLIC SECTOR, MCAFEE, INC.; CHARLES BLAUNER, GLOBAL HEAD OF INFORMATION SECURITY, CITIGROUP, INC., ON BEHALF OF THE AMERICAN BANKERS ASSOCIATION; DUANE HIGHLEY, PRESIDENT AND CEO, ARKANSAS ELECTRIC COOPERATIVE CORPORATION, ON BEHALF OF THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION; AND ROBERT MAYER, VICE PRESIDENT, INDUSTRY AND STATE AFFAIRS, UNITED STATES TELECOM ASSOCIATION

STATEMENT OF DAVE MCCURDY

Mr. MCCURDY. Thank you, Madam Chair, and thank the ranking member as well for the opportunity to be here. I am Dave McCurdy, President and CEO of the American Gas Association, and also relevant to this hearing, I am a former chairman of the House Intelligence Committee in this body, and just to start off, thank you for your comments earlier about Moore, Oklahoma, which was in my district as well years ago.

AGA represents over 200 local gas companies that deliver natural gas to more than 71 million U.S. residential, commercial, and industrial gas customers. AGA is an advocate for local natural gas utility companies and provides a range of programs to natural gas pipelines, marketers, gatherers and industry associates. Natural gas is the foundation fuel for a clean and secure energy future, providing benefits for the economy, our environment and our energy security.

Alongside the economic and environmental opportunity natural gas offers comes a responsibility to protect its distribution pipeline systems from cyber attacks. Web-based tools have made natural gas utilities more cost-effective, safer and better able to serve our customers. However, the opportunity costs of a more connected industry is that we have become a target for sophisticated cyber terrorists. This said, natural gas utilities are meeting the threat daily via skilled personnel, a commitment to security, and the cybersecurity partnership with the federal government.

This government-private partnership in cybersecurity management is critical for us. Our utilities deliver and our systems are the safest energy delivery system in the world. This said, industry operators recognize there are cyber vulnerabilities with employing web-based applications for industrial control and business operating systems. Because of this, gas utilities adhere to myriad cybersecurity standards and participate in an array of cybersecurity initiatives. However, the industry's leading cybersecurity tool is a longstanding cybersecurity information-shar-

ing partnership with the federal government. Natural gas utilities work with government at every level to detect and mitigate cyber attacks, in particular, AGA members with the Transportation Security Administration, Pipeline Security Division of TSA, the agency tasked with overseeing distribution pipeline cybersecurity. In addition, gas utilities collaborate with ICS-CERT on cybersecurity awareness, detection and mitigation programs. Simply put, TSA and ICS-CERT understand cyber threats, natural gas utilities understand their operations, and we work together to protect critical infrastructure.

AGA's perspective in this is that since the Executive order's impact on gas utility cybersecurity could be significant, we participated on the Executive order's cyber dependent infrastructure identification, cybersecurity framework collaboration, and the incentive working groups. In addition, AGA chairs the Cybersecurity Working Group of the Oil and Natural Gas Pipeline and Chemical Sector Coordinating Council, a panel established to address Executive order activities, and if I could, Madam Chair, in response to the questions from the committee make just a couple quick observations.

Clearly, there is certain disagreement within sector-specific agencies about whether natural gas facilities should be considered critical cyber dependent, cyber dependent being the word infrastructure. For natural gas entities which answer to multiple federal agencies, this uncertainty is unsettling. Regardless of the ultimate answer, we hope that the Infrastructure Identification Working Group will decide this question in an open and collaborative fashion.

With regard to Dr. Gallagher's testimony on the NIST cybersecurity framework, at present the NIST cybersecurity framework development process appears headed in the proper direction. This said, natural gas utilities have some general concerns. First, the framework development process could benefit from more consideration of existing cybersecurity standards, including TSA standards applicable to gas utilities. In addition, framework provisions must be flexible and not morph into regulations, which will quickly become outdated due to an ever-changing cyber threat landscape. And finally, the framework must be flexible enough to allow companies to tailor cybersecurity systems to their own operational needs. And third, the Executive order directs DHS to help develop incentives that will spur industry adoption of the NIST framework. However, most of the proposed incentives put forth so far are little more than government services like enhanced cybersecurity support that in fact should be in any cybersecurity program. The fact is, absent new statutory authority to provide meaningful incentives like information safe harbors and cybersecurity liability protections, the government is limited in what it can do to entice participation. Industry would be better served via reinforced support for federal programs that provide training, onsite cybersecurity evaluations and system compromise support.

And lastly, Madam Chair, the case for cybersecurity legislation or CISPA, ultimately AGA does believe there is a role for cybersecurity legislation to help counter cyber attacks and protect

networks against future incursions, critical infrastructure needs, government to help identify, block and/or eliminate cyber threats. Harnessing the cybersecurity capabilities of the government intelligence community, so my colleagues, former colleagues on my left here, on behalf of the private sector and networks will go a long way towards overall network security. AGA supports——

Mrs. BLACKBURN. Mr. McCurdy, please sum up.

Mr. MCCURDY. AGA supports the recently passed legislation and urges the Senate to follow suit, and we thank you for the opportunity to testify and will answer questions.

[The prepared statement of Mr. McCurdy follows:]

Hon. Dave McCurdy
President & CEO

Dave McCurdy
President and CEO
American Gas Association

Testimony before the House Committee on Energy & Commerce
"Cyber Threats and Security Solutions"

May 21, 2013

Chairman Upton, Ranking Member Waxman, and Members of the Committee, I am Dave McCurdy, President and CEO of the American Gas Association. Also relevant to this hearing, I am a former Chairman of the House Intelligence Committee and have been involved in cybersecurity policy for over 20 years. Thank you for inviting me to share my perspectives on critical infrastructure cybersecurity.

AGA represents more than 200 local energy companies that deliver natural gas to more than 71 million residential, commercial and industrial gas customers in the United States. AGA is an advocate for local natural gas utility companies and provides a broad range of programs and services for member natural gas pipelines, marketers, gatherers, international gas companies and industry associates. Today, natural gas meets almost one-fourth of U.S. energy needs.

Natural gas is the foundation fuel for a clean and secure energy future, providing benefits for the economy, our environment and our energy security. Alongside the economic and environmental opportunity natural gas offers our country comes great responsibility to protect its distribution pipeline systems from cyber attacks. Technological advances over the last 20 years have made natural gas utilities more cost-effective, safer, and better able to serve our customers via web-based programs and tools. Unfortunately, the opportunity cost of a more connected, more efficient industry is that we have become an attractive target for increasingly sophisticated cyber terrorists. This said, America's investor-owned natural gas utilities are meeting the threat daily via skilled personnel, robust cybersecurity system protections, an industry commitment to security, and a

400 N. Capitol St. NW 4th Floor, Washington, DC 20001 P 202-824-7111 F 202-824-7098 E dmccurdy@aga.org www.aga.org

successful ongoing cybersecurity partnership with the Federal government.

Government-Private Partnerships & Cybersecurity Management: A Process that Works for Natural Gas Utilities

America's natural gas delivery system is the safest, most reliable energy delivery system in the world. This said, industry operators recognize there are inherent cyber vulnerabilities with employing web-based applications for industrial control and business operating systems. Because of this, gas utilities adhere to myriad cybersecurity standards and participate in an array of government and industry cybersecurity initiatives. However, the most important cybersecurity mechanism is the existing cybersecurity partnership between the federal government and industry operators. This partnership fosters the exchange of vital cybersecurity information which helps stakeholders adapt quickly to dynamic cybersecurity risks.

Background: *The Homeland Security Act of 2002* provides the basis for Department of Homeland Security (DHS) responsibilities in protecting the Nation's critical infrastructure and key resources (CIKR). The Act assigns DHS the responsibility for developing a comprehensive plan for securing CIKR. This plan, known as the National Infrastructure Protection Plan (NIPP), identifies 18 critical infrastructure sectors within which natural gas transportation is a subsector of the Energy and Transportation Sectors. The NIPP states that more than 80 percent of the country's energy infrastructure is owned by the private sector, and that the Federal Government has a statutory responsibility to safeguard critical infrastructure. For this reason, information-sharing amongst industry operators and the government intelligence community is critical to cyber infrastructure protection.

AGA-Government Cybersecurity Partnerships: Natural gas utilities work with government at every level to detect and mitigate cyber attacks. In particular, AGA works closely with the Transportation Security Administration, Pipeline Security Division, the government entity designated to oversee physical and cybersecurity operations of distribution pipelines. AGA views our relationship with TSA as a true partnership that benefits all stakeholders because it allows government and pipeline owner/operators to exchange

cybersecurity information typically not shared in a regulatory compliance-driven environment. In addition, gas utilities collaborate with the DHS *Industrial Control Systems Cyber Emergency Response Team* (ICS-CERT) on cybersecurity awareness, detection, and mitigation programs. This process calls on operators to submit suspicious cyberactivity reports to ICS-CERT. In turn, ICS-CERT advises operators of cyber vulnerabilities, mitigation strategies, and forensic analyses. This open communication bolsters the industry's overall cybersecurity posture, and advances ICS-CERT's mission. Simply put, ICS-CERT understands cyber threats; natural gas utilities understand their operations; and the two work in tandem to protect targeted critical infrastructure.

AGA also strongly encourages industry participation in DHS-led training programs and system evaluation programs, as well as relevant cybersecurity programs operated by other agencies. Moreover, DHS officials regularly meet with industry groups, such as the AGA Board of Directors and individual member companies, to review and assess ongoing cyberthreats. Bottom line, as cybersecurity threats to gas industry operations have evolved, there has been a corresponding improvement in how gas utilities respond to these threats due to our substantive cybersecurity partnership with DHS.

The following is a list of additional government-natural gas industry cybersecurity partnerships:

- *DHS Cybersecurity Briefings*. Industry operators participate in DHS briefings to receive threat and risk information and analytics. The briefings provide information on the state of the ONG sector in reference to emerging threats, security incidences, and trends. AGA is leading the collaborative effort between the government intelligence community and private industry to improve on timely, credible, and actionable information sharing.

- *DHS Control Systems Security Program*. DHS offers industry operators opportunities to enhance their knowledge of control system cybersecurity via ICS-CERT training, online forums, recommended practices, advisories, and interactive live assistance. Industry operators also receive *United States*

Computer Emergency Readiness Team (US-CERT) activity summaries and advisory communications; submit incident reports for analysis; and engage in the Industrial Control Systems Joint Working Group for information exchange.

- *Oil & Natural Gas Sector Coordinating Council (ONG SCC) Cybersecurity Working Group*. Industry operators participate in this DHS-sponsored forum for coordination of ONG cybersecurity strategy, policy, and communication. The ONG SCC provides a venue for operators to mutually plan and execute sector-wide cybersecurity programs, exchange information, and assess progress toward protecting ONG sector critical infrastructure.

- *TSA Cyber Security CARMA Program*. Sponsored by TSA, this program seeks to develop a national cyber risk management framework to help industry identify where internal risk management activities align with industry-wide risk management activities. AGA co-chairs this collaborative effort and facilitates operator participation and contribution.

- *Coordinate Federal Government Risk Assessment Programs*. AGA coordinates meetings with the Department of Energy, Federal Regulatory Energy Commission, TSA, and ICS-CERT to encourage government entities to align various cybersecurity risk assessment programs. The objective is to compare/contrast the programs and identify useful synergies.

AGA-Industry-Government Cybersecurity Guidelines: Partnership between the private sector and the government is critical to address cybersecurity threats to critical infrastructure. As such, AGA and industry operators also collaborate with government partners to produce effective cybersecurity practices and guidelines. Below are a few examples.

- *Transportation Security Administration, Pipeline Security Guidelines.* Guidelines developed through a collaborative effort of government and pipeline asset owners. Used by natural gas pipeline companies,

natural gas distribution companies, and liquefied natural gas facilities as a framework to protect critical/non-critical pipeline infrastructure. AGA served as a subject matter expert in drafting the cybersecurity chapter.

- *DHS Control Systems Security Program, Cyber Security Evaluation Tool (CSET).* A software tool that guides users through a step-by-step process to assess the cybersecurity posture of industrial control systems and information technology networks. AGA participated in the development, testing, and distribution of this material and contributes regular updates.

- *Department of Energy, Roadmap to Achieve Energy Delivery Systems Cybersecurity*. A framework to improve cybersecurity within the energy sector via a collaborative vision of industry, vendors, academia, and government stakeholders. The framework includes goals and deadlines over the next decade. AGA has contributed to this resource since 2006.
- *Interstate Natural Gas Association of America (INGAA), Control System Cyber Security Guidelines for the Natural Gas Pipeline Industry*. Guidelines designed to assist natural gas pipelines in managing control system cybersecurity requirements. Aligns with TSA Pipeline Security Guidelines and other standards used across the oil and natural gas industries. AGA reviewed its development and promotes it as a valuable resource to member companies.
- *AGA and INGAA, Security Practices Guidelines, Natural Gas Industry Transmission and Distribution*. Guidelines that provide recommended cybersecurity practices and procedures for transmission and distribution segments of the natural gas industry. AGA and INGAA developed this guidance for natural gas pipeline and utility operators.

Non-Standardization of Cybersecurity Practices is Paramount

In the recent past, concerns over increasing cyberattacks on critical infrastructure have led to legislative efforts

to create a set of top-down cybersecurity regulations. AGA remains concerned that prescriptive cybersecurity regulations will have little practical impact on cybersecurity and, in fact, will hinder implementation of robust cybersecurity programs. First and foremost, prescriptive cybersecurity regulations would fundamentally transform the productive cybersecurity relationship natural gas utilities have with the TSA Pipeline Security Division from a successful partnership to a more standard regulator-regulated mode, forcing companies to focus more resources on compliance activities than on cybersecurity itself. Also, from a practical perspective, it is unlikely that any set of cybersecurity regulations will be dynamic enough to help companies fight constantly changing and increasingly sophisticated threats.

Across the natural gas industry, cybersecurity effectiveness is maximized through the diversity of individual company cybersecurity approaches, e.g. Defense in Depth strategies and customized detection and mitigation systems appropriate for individual company networks. Companies also turn lessons learned from government-private industry cybersecurity information sharing partnerships into actions designed to protect their specific systems. In sum, as cybersecurity risks and threats change, so do vulnerabilities. Ongoing implementation of new and diverse cybersecurity tools and procedures, based on unique individual company requirements, helps companies adapt to a dynamic cyberthreat environment and bolsters overall gas utility industry cybersecurity.

The Cybersecurity Executive Order, Private Sector Perspective

The Administration's Executive Order (EO), *Improving Critical Infrastructure Cybersecurity* establishes national policy on critical cyber infrastructure security. Because the EO's direct impact on private sector cybersecurity programs is significant, AGA, AGA's multi-company Cybersecurity Strategy Task Force and individual companies have been working collaboratively with government stakeholders on the various EO directives since its release. In addition, AGA chairs a joint cybersecurity working group of the Oil & Natural Gas, Pipeline and Chemical Sector Coordinating Councils, a working group established specifically to address EO activities. As such, AGA is uniquely situated to share insight received from multiple sectors.

In general, we believe the EO's voluntary process is the right approach and we actively participate in the working groups that lead DHS' coordination of interagency and public and private sector efforts in implementing the EO. These working groups include, Stakeholder Engagement, Cyber-Dependent Infrastructure Identification, Planning and Evaluation, Situational Awareness and Information Exchange, Incentives, Cybersecurity Framework Collaboration (with NIST), Assessments of Privacy and Civil Rights and Civil Liberties, and Research and Development. The working groups have sponsored constructive work sessions with stakeholders, including gas utilities. Moreover, DHS has made a substantive effort to address industry concerns about true public-private collaboration, technical expertise, transparency, and scheduling.

Overall, the EO is simply the beginning of a long march to improve national cybersecurity. AGA is hopeful, and will work to ensure that throughout this process gas utility cybersecurity concerns will be addressed. Below are a few of our specific concerns and observations.

Identifying Critical Infrastructure. The executive order confines itself largely to "critical infrastructure", defined in Section 2 of the EO as *"systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."* From the start, AGA has suggested that the identification process include the informed participation of critical infrastructure owner/operators. And while the government has acceded to this industry wish, the results to date have been mixed.

A general stakeholder concern at every working session is that the EO process is hurried and that the tight timelines require DHS to value rapidity more than process and content, making it difficult for proper assessment and vetting of information. Notably, the Cyber-Dependent Infrastructure Identification (CDII) process has suffered in this process. While it appears that DHS is acting prudently, identifying only cyber infrastructure at 'greatest risk' of resulting in catastrophic consequences if compromised, the criteria proposed for that

identification process continues to morph without transparency and consultation with stakeholders.

Since 2007, DHS has used criteria listed in the National Critical Infrastructure Prioritization Program (NCIPP) to identify and prioritize critical infrastructure that could through destruction or disruption have catastrophic national or regional consequences. The identified assets provide the foundation for infrastructure protection and risk reduction programs executed by DHS and its public and private sector partners. Unfortunately, as part of the EO's new CDII process, when natural gas owner/operators assessed their operations using the NCIPP criteria and arrived to conclusions that their infrastructure was not at 'greatest risk', DHS changed the criteria without notice, comment or collaboration. Natural gas owner/operators also participated in the DHS-developed Cybersecurity Assessment & Risk Management Approach Model (CARMA), a risk evaluation process that assesses cybersecurity risks that stakeholders and task force leaders agreed would be relevant to the EO's CDII process. Again, after evaluation, conclusions show that sector infrastructure is not at the 'greatest risk'. Furthermore, this analysis matches internal assessments performed by various industry trade associations.

Clearly there is disagreement within sector specific agencies (DHS, DOE, etc.) about whether or not natural gas facilities should be considered critical cyber-dependent infrastructure. For natural gas entities, which answer to multiple sectors specific agencies, this is unsettling. Regardless the ultimate answer, we remain hopeful that the government-industry CDII partnership will decide this question in an open, collaborative and scientific fashion.

Cybersecurity Information Sharing Program. Section 4 of the EO creates a cybersecurity information sharing program, directing DHS, the Department of Justice, and the Office of the Director of National Intelligence to set up cyber threat information sharing processes with targeted private sector entities. Without question, improved information sharing can and will benefit critical infrastructure cybersecurity. However, for industry to fully engage in an information sharing program, information protection mechanisms (safe harbors) and liability protections must be afforded to owners/operators who participate in the program. Without such protections, companies may be unwilling to participate because of the possibility of information leaks as well as due to

competitive concerns and legal liability pressures.

NIST "Cybersecurity Framework". Section 7 of the EO directs the National Institutes of Standards and Technology (NIST) to develop, via an open review process, a "Cybersecurity Framework" designed to improve critical infrastructure cybersecurity. The Framework will utilize risk and performance based standards/best practices; technology neutral applications; voluntary consensus standards and industry best practices; and cross-sector security standards applicable to all critical infrastructure. Ultimately, NIST's goal is to create a framework that is "prioritized, flexible, repeatable, performance-based, and cost-effective" to help critical infrastructure owner/operators manage cyber risk.

At present, NIST's Cybersecurity Framework development process appears headed in the proper direction, primarily due to internal technical expertise and substantive stakeholder involvement. However, an upcoming stakeholder workshop (May 29-30) will be the determining factor as to what extent industry comments are incorporated into the final product. Our primary concerns with the voluntary Framework are:

- The Framework development process largely ignores time-tested and effective information sharing partnership efforts between the public and private sectors over the past several years – most notably the gas industry's existing cybersecurity partnership with TSA, ICS-CERT, etc.

- Framework provisions must remain flexible and not morph into mandated regulations, which will quickly become outdated due to an ever-changing cyber threat landscape.

- Framework inflexibility will also create vulnerabilities in intricate systems tailored to specific company operations and risk profiles. That is, simply building more defenses is no longer effective; the focus has shifted to increased monitoring and better and faster incident response, which requires robust cybersecurity programs and effective information sharing.

Overall, AGA appreciates the opportunity to participate in a standards development process that has potential to impact our cybersecurity programs. We look forward evaluating the final product on its merits. Ultimately, if there is a valid basis for its incorporation and/or the Framework does not conflict with existing domestic and international cybersecurity standards and/or regulations, gas utilities will be strongly encouraged to adopt it.

Industry Adoption of Cybersecurity Framework. Section 8 of the EO directs DHS to create a "voluntary" program to spur critical infrastructure entities to adopt the NIST Framework Specifically, DHS will work with other agencies to review the Framework and develop implementation guidance to address sector-specific operating environments. More importantly, DHS will work with the Departments of Commerce and Treasury to report on existing incentives that might spur industry participation in the voluntary program as well as any additional incentives (i.e. liability protections) that would require new statutory authority. Sector agencies will also report annually on which critical infrastructure owner/operators participate in the program. Overall, just how "voluntary" this program ends up becoming is an open question. As AGA and other critical infrastructure industries have argued, voluntary government programs often morph into de facto mandatory compliance programs because companies feel compelled to participate rather than risk opening themselves up to litigation for not engaging in a program that has the imprimatur of the federal government.

This program for incentivizing participation in the NIST Framework does create concerns. First of all, many of the proposed incentives are basic activities the government should already be providing under any reasonable public/private cybersecurity partnership. More importantly, if some entities ultimately decide to not adopt the voluntary NIST Framework, it is neither appropriate nor necessary to incentivize their participation (or punish non participation) by offering/not offering "incentives" such as favored status in government contracting, greater access to cybersecurity training and support, expedited security clearances and the like. Fact is, without new statutory authority to provide meaningful incentives like information-sharing safe harbors for entities that share cybersecurity information with the government and liability protections for companies with robust cybersecurity programs, there is a limit to what the government can do to entice companies to participate in

the Framework.

More significant, measurable, and non-controversial than incentives would be increasing opportunities for companies to request government cyber readiness appraisals and assistance in the event of a system compromise. This can be done by reinforcing support for existing highly-regarded programs such as DHS ICS-CERT red team/blue team training and onsite cybersecurity evaluations, and the Department of Energy's Cybersecurity Capability Maturity Model onsite testing. The vast majority of natural gas utilities are already taking serious steps, commensurate with the known risks, to protect their systems from cyberthreats. These companies have a continuing interest in knowledge relating to new threat vectors, indicators and mitigation measures, and don't need incentives or direct federal involvement to help manage their cyber vulnerabilities.

Agency Adoption of NIST Cybersecurity Framework. Section 10 of the EO notes that once the NIST Framework has been preliminarily drafted agencies with cybersecurity regulatory responsibilities will review their existing authorities to determine whether they are sufficient given the cyberthreat landscape, and whether they can implement the NIST Framework via regulation. If agencies determine that their current cybersecurity regulatory requirements are insufficient then they shall propose new "actions" to mitigate cyber risks. This section clearly pushes sector agencies to create new cybersecurity regulations. These new requirements would, at a minimum, be based upon the NIST Cybersecurity Framework; however, there is plenty of suggestion in Section 10 that agencies move beyond the framework, or seek the authority to do so. We are hopeful this will not lead to regulation for regulations sake. For example, despite having the statutory authority necessary, TSA Pipeline Security Division has chosen not to issue cybersecurity regulations for natural gas utilities in large part because of the successful security partnership we have collectively developed.

The Case for Cybersecurity Legislation.

Despite our concerns about prescriptive cybersecurity standards, AGA does believe that there is a role for

cybersecurity legislation, particularly as it relates to improving public-private cybersecurity information sharing and related liability protections.

Information Sharing. To help counter cyberattacks and protect networks against future incursions, critical infrastructure needs government to help them identify, block and/or eliminate cyberthreats as rapidly and reliably as possible. From a functional perspective, this will require streamlining the process by which actionable threat intelligence is shared with private industry. Harnessing the cybersecurity capabilities of the government intelligence community on behalf of private sector networks will go a long way towards overall network security. The recently passed H.R. 624, *The Cyber Intelligence Sharing and Protection Act* (CISPA) provides a positive roadmap by establishing a cybersecurity partnership between critical infrastructure and the defense/intelligence community and DHS to distribute cyberthreat information, interpret and share potential threat impacts, and work with critical infrastructure to keep their networks safe.

Liability Protection, *SAFETY Act*. Another avenue for legislation surrounds offering liability protection for companies with robust cybersecurity programs – standards, products, processes, etc. The Administration's recent executive order (EO) on cybersecurity underscores this need. The EO directs sector agencies, the intelligence and law enforcement community to establish a cybersecurity information sharing partnership; tasks the National Institute of Standards and Technology with establishing a quasi-regulatory set of cybersecurity standards (a "cybersecurity framework"); and orders DHS to incentivize critical infrastructure to adhere to the NIST standards. What the EO cannot do is provide liability protections for critical infrastructure entities that make the effort to participate in a public-private cybersecurity program, regardless of whether it is created via EO or some future law.

AGA supports employing the *SAFETY Act* as an appropriate avenue for providing companies that participate in a government-private industry cybersecurity partnership with liability coverage from the impacts of

cyberterrorism. *SAFETY Act* applicability in this area seems plain:

- The SAFETY *Act* exists in current law, and a related office at DHS has been reviewing and approving applications for liability coverage in the event of an act of terrorism or cyber attack for over a decade. This office utilizes an existing review and approval process which would allow for immediate granting of liability protections from cyber attacks.

- Because the *SAFETY Act* can apply to a variety of areas ranging from cybersecurity standards (cyber best practices, etc.), to procurement practices and related equipment (SCADA, software, firewalls, etc.) companies can layer their liability protection.
- We are aware of no other existing statute that offers similar liability protections. Moreover, we do not see the need to write new law to address liability protections from cyber incidents when the *SAFETY Act* is already applicable.

This said, there are some areas where we believe the *SAFETY Act* could be a little stronger as it applies to cyber matters. First, and foremost, the statute could be expanded to make specific reference to liability protections from "cyber" events (cyber attacks, cyber terrorism, etc.) and more specific reference to coverage for cybersecurity equipment, policies, information sharing programs, and procedures. While there is coverage under the Act currently for cyber attacks, specifically identifying "cyber attacks" as a trigger for liability protections would strengthen the overall concept.

THE NATURAL GAS UTILITY CYBERSECURITY POSTURE

AGA's policy priorities for cybersecurity include preserving our current cybersecurity partnership with the Transportation Security Administration, Pipeline Security Division, enhancing government-private industry cybersecurity information sharing, opposing burdensome or counterproductive cybersecurity regulation, and supporting robust liability protections for entities that are serious about protecting their networks. If ultimately achieved, these items will only bolster an already solid industry cybersecurity commitment.

America's natural gas utilities are cognizant of enduring cyber threats and the continued need for vigilance through cybersecurity protection, detection, and mitigation mechanisms. There is no single solution for absolute system protection. However, through a combination of cybersecurity processes and timely and credible information-sharing amongst the government intelligence community and industry operators, America's natural gas delivery system remains protected, safe and reliable, and will remain so well into the future.

Mrs. BLACKBURN. Thank you.

Mr. McConnell, you are recognized for 5 minutes, and as a reminder, you have the timers in front of you.

STATEMENT OF JOHN M. (MIKE) MCCONNELL

Mr. MCCONNELL. Thank you, Madam Chairman. I want to first of all make the point that I am speaking as a citizen. I do not represent any company or organization.

I have one main point to make to the committee. Legislation is required. Legislation is required. If we don't have it, we will not solve this problem. Now, the debate will be whether you incentivize participation by the private sector or you compel. That is something that Congress will have to debate.

I have four main points to make. The government produces unique information. That is the community that I come from, unique information. It is not produced anywhere else in the world inside the United States. It is code breaking, it is intelligence, it is understanding threats before they happen. We must determine a way to share the information with the private sector. That means we have to change the rules. That is a requirement that will only be achieved through legislation.

The second point I would make is, we must establish cybersecurity standards. They must be able to evolve and they must be dynamic. That will give us two choices to make: do you incentivize, as discussed earlier in the first panel, or do you compel. That is going to be a decision that this Congress will have to wrestle with, but one way or the other, we must have those standards. We also must finally address the privacy concerns, and I have fingerprints over a bill called FISA, Foreign Intelligence Surveillance Act. So the congressional record will show the 2-year debate, actually 3 years—I was only involved for 2 years—to get that to closure. The issue is, we must be able to do the intelligence mission of the country while protecting the privacy and civil liberties of our citizens. I have a single recommendation: put it in law what you don't want to happen, and the community will react to that law because we are a nation of laws. It is the responsibility of the Congress to oversee and ensure that that law is complied with.

Now, the debate will be, is screening traffic coming in through an international gateway for malware, is that reading a citizen's mail. That will be the debate. You will have to wrestle with that question to get it resolved because today the Chinese, because they are clumsy and because they have a policy of building cyber tools for warfare but they have a policy of economic espionage, they are stealing the intellectual lifeblood of this country. We have to deal with that, and we strip out that malware at the international gateway. Fortunately for us, the Iranians, because they are hammering U.S. banks with denial-of-service attacks, are causing the Nation to focus on this issue. I have been focused on it for 20 years. We are finally getting to a point of addressing it. It will require legislation. Thank you for your time.

[The prepared statement of Mr. McConnell follows:]

Statement for the Record 20 May 2013

Statement of John M (Mike) McConnell

Former Director of National Intelligence

Former Director of the National Security Agency

For Testimony before the House Committee on Energy and Commerce for

A hearing entitled "Cyber Threats and Security Solutions"

Mr. Chairman, Members of the Committee,

It is an honor to appear before your Committee today to offer my views on the important topic of Cyber Threats and Security Solutions. You will see in the series of Op-Eds that I have attached to this statement which have been produced over several years, I have long standing concerns for the security interests of the nation, going back to my days as the Director of the National Security Agency. I encourage members of Congress to consider comprehensive legislation that will create the necessary legal framework required to address and mitigate these threats.

I would like to make three basic points:

1. The nation is at strategic risk from "cyber war" and the potential for "cyber terrorism"
2. There also is strategic risk to the nation from "cyber economic espionage" which currently is bleeding the nation of its competitive advantage
3. Without needed cyber security legislation to frame and force full cooperation across the government and the private sector, we will not achieve the required level of cyber security capabilities to protect the nation and its interests.

Cyber threats are well documented and will not be repeated here except to say that nation-states are creating 1000s of zero-day, cyber tools each year to enable two things and which introduce a third concern:

1. Success in any kinetic conflict with another nation and
2. Success in penetrating computer systems for economic espionage, i.e., to steal proprietary intellectual capital. R&D, innovation, business plans, and source code to obtain competitive advantage. (As you are aware, the US, by policy and practice, does NOT engage in economic espionage.)

3. It is just a matter of time before some of these cyber exploitation and attack tools proliferate to extremist groups who want to change the world order. The equivalent of suicide bombers we have witnessed in recent years could be harnessed as "suicide cyber attacks" on the critical infrastructures of the nation.

While the attached op-eds provide my views on above, I will make the following recommendations for the Committee to consider. These recommendations are made on the basis of my experience for over 45 years in threat intelligence and my experience watching the Department of Defense (DoD) become transformed as the result of comprehensive legislation in 1986 commonly referred to as "Goldwater-Nichols" which forced DoD to operate as a joint unified force in the nation's defense. All efforts to force jointness and interoperability prior to 1986 had been piecemeal or unsuccessful.

WHAT IS REQUIRED AT A MINIMUM:

1. SHARING OF SENSITVE INFORMATION PRODUCED ONLY BY THE GOVERNEMENT WITH THE PRIVATE SECTOR: The US Government, through its intelligence and law enforcement operations, produces valuable information on the cyber threats. This information, most often, is sensitive or classified on the basis of national security rules for protecting sources and methods developed in World War II and used during the Cold War. Those rules served us well in those periods, but the rules now must be modified to force sharing of sensitive data with the private sector in the new era of global cyber threats. The bill produced by House Permanent Select Committee on Intelligence (HPSCI) and passed by the House addresses these concerns.
2. ADOPTION OF HIGHER CYBER SECURITY STANDARDS BY INDUSTRY: The role of government is to cause creation of the needed higher security standards; the debate will be how? I recommend that legislation be written to allow the private sector to create the standards and the role of government only can be to "agree or disagree" the standards are sufficient. The process needs to be iterative until standards are agreed and there must be a way to evolve and update the standards based on new threats or technology advances.
3. INCENTIVISE THE PRIVATE SECTOR TO ADOPT AND USE THE HIGHER CYBER SECURITY STANDARDS: The legislation should contain provisions to provide "Liability Protection" against suits for data breaches to those private sector firms that adopt and use the agreed cyber security standards.
4. PRIVACY CONCERNS: The US Intelligence Community (USIC) is authorized and tasked to collect and analyze information on foreign intelligence. There are concerns, based on historical precedent, that the Executive Branch might use the USIC to collect or intrude on the privacy of US Persons. These concerns can and should be addressed by legislation that makes collection of information about US Persons without appropriate authorization and oversight illegal. We are a nation

of laws and it is up to the Legislative Branch to frame those laws, provide authorization and appropriations to carry out the law and provide the necessary oversight to ensure those laws are not broken. In my 45 years of experience in the USIC, I have observed, firsthand, how the law drives behavior. If laws are broken, the Constitution leads us through a process to address any wrong doing.

Mr Chairman, Members of the Committee, thank you again for the opportunity. I look forward to your questions.

Patchwork Strategy Is Not Nearly Enough to Combat Cyberthreats

From CYBERSECURITY on Page 23

task represent a significant new challenge to its team.

The National Preparedness Leadership Initiative at Harvard has done extensive research on the characteristics of "meta-leaders" who take an enterprise-wide approach to problems, which is what's called for in the NIST effort. Meta-leaders lead their own agencies, and they lead up, speaking "truth to power" to those more senior; they also lead across all agencies involved in a particular event, and in so doing, they develop situational awareness to create a path forward, often in the face of incomplete information.

For NIST to bring all of the parties together and create meaningful change, I believe that its senior leaders must become directly involved in this effort, bringing to it these enterprise-wide leadership skills, and the engagement of the Department of Commerce, and interagency and business leadership. The commercial finance, energy and other private industry players need to understand that the government can provide unique, sensitive information and help create information sharing standards across industries that are consistent, and the government needs to better understand the needs of the private sector. We won't overcome these challenges without executive branch "meta-leadership."

NIST is planning a series of upcoming discussions with private industry this summer to develop a framework for cybersecurity practices to help critical infrastructure manage risk. These would benefit from hands-on attention now and throughout the process from the Institute's senior leaders, other senior leaders across the government sector and senior leaders from the private sector.

On the legislative side, the House has again passed a bill that would foster information sharing, allowing the government and businesses to share data about cyberattacks, potential threats and other information in a manner that avoids antitrust or classification issues. The bill also would grant legal protections to businesses that have been hacked as long as they met standards for protecting their networks. The question will be "who sets the standards"? In my view, industry should set the standards with a simple "agree or disagree" response by the government until agreed-upon standards are established with a method to evolve.

Currently, the Obama administration and many privacy advocates fear the bill provides too few protections against the improper sharing and use of individuals' private information, and they have raised questions about the ability of private companies to shirk their responsibilities for protecting information under the cloak of immunity privileges.

I believe there is middle ground — some liability protection is important, but the protection standards required of industry must be strong and enforceable. Just as meta-leadership is needed around the parameters of the executive order, meta-leaders must step forward around the congressional effort.

The U.S. Chamber of Commerce, which has been a leading opponent of cyber legislation out of fear of additional regulations on industry, must look beyond its traditional point of view. Leaders in Congress — many of whom have seen in classified reports the scope and depth of the cyberthreat — need to bring the business community and privacy advocates to the table in a more urgent, thoughtful way. The Obama administration must do its part through the NIST effort on the executive front and by engaging with Congress on the issue.

In Saudi Arabia last year, 30,000 computers at the Saudi Aramco oil company were attacked and all data deleted in a cyber-attack. Week after week, U.S. banks are hit with denial-of-service attacks. Billions of dollars of patented intellectual capital — plans for building advanced systems — have been stolen by China and other countries. And our banking system, our electric grids, our transportation systems — the lifeblood of our daily lives — every day operate in cyberattackers' cross hairs with largely inadequate protections.

New kinds of leaders need to step forward and bring their meta-skills to this urgent, enterprisewide problem. We need sensitive information shared by the government to the private sector, cyber-penetration information shared by the private sector to government, agreed-upon standards for protection of the nation and liability protection for industry. And we need all this before our nation is trying to recover from an attack or the continued bleeding of our intellectual capital and asking after the fact, "Why didn't we know it was coming?"

Mike McConnell is the vice chairman of Booz Allen Hamilton and previously served as director of national intelligence under Presidents George W. Bush and Barack Obama. He retired from the U.S. Navy in 1996 as a vice admiral.

Just as meta-leadership is needed around the parameters of the executive order, meta-leaders must step forward around the congressional effort.

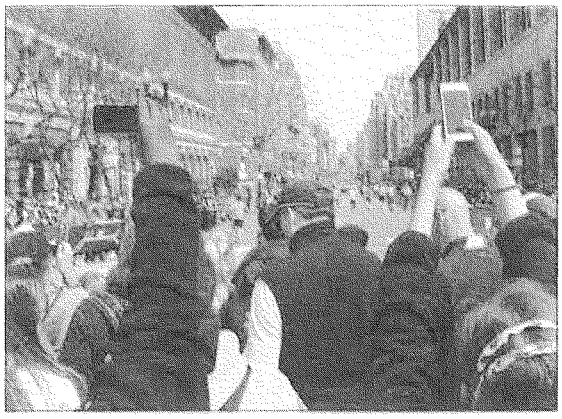
MIKE MCCONNELL

On Cybersecurity, Nation Needs 'Meta-Leadership'

When tragedy struck the Boston Marathon, law enforcement and national security officials sifted through untold amounts of information and identified suspects within three days. Data came from literally everywhere: video from business-owned cameras; individual bystanders' cellphone pictures, information from the media and large amounts of material collected by investigators themselves.

Information was shared from multiple public and private sources, analyzed and acted on instantly. It was a real-time case study, unfolding before the eyes of the world, about the power of information sharing – and it illustrated the critical role information sharing must play to prevent cyberattacks and cyberespionage that could lead to another kind of devastation.

In February, President Barack Obama issued an executive order to set up a structure for information sharing between the public and private sectors, and the House of Representatives just passed another version of cyber legislation to enhance protections when information is shared. But both of these efforts face obstacles in the debates over privacy and the fear of regulation — unless effective leaders step forward.



AP

Spectators take cellphone pictures of the Boston Marathon on April 15, before two bombs exploded at the finish line. Information sharing among police and public played a key role in identifying the bombers, the author writes.

If these efforts fail to achieve their purpose of significantly enhanced information sharing between the government and private sectors, the nation will achieve some limited kind of information sharing, but it will come in response to a major attack, and the plan will be assembled quickly and haphazardly after the fact. The nation will get a solution: a patchwork solution — something we should work now to avoid.

Today, under the president's order, leadership of the effort to collaboratively develop a Cybersecurity Framework with the private sector has been assigned to the National Institute of Standards and Technology, under the Department of Commerce.

NIST is an excellent arbiter of the technical details, but the political skills and the market understanding required for this

See CYBERSECURITY on Page 24

The Washington Post

http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

Mike McConnell on how to win the cyber-war we're losing

By Mike McConnell
Sunday, February 28, 2010; B01

The United States is fighting a cyber-war today, and we are losing. It's that simple. As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking.

The problem is not one of resources; even in our current fiscal straits, we can afford to upgrade our defenses. The problem is that we lack a cohesive strategy to meet this challenge.

The stakes are enormous. To the extent that the sprawling U.S. economy inhabits a common physical space, it is in our communications networks. If an enemy disrupted our financial and accounting transactions, our equities and bond markets or our retail commerce -- or created confusion about the legitimacy of those transactions -- chaos would result. Our power grids, air and ground transportation, telecommunications, and water-filtration systems are in jeopardy as well.

These battles are not hypothetical. Google's networks were hacked in an attack that began in December and that the company said emanated from China. And recently the security firm NetWitness reported that more than 2,500 companies worldwide were compromised in a sophisticated attack launched in 2008 and aimed at proprietary corporate data. Indeed, the recent Cyber Shock Wave simulation revealed what those of us involved in national security policy have long feared: For all our war games and strategy documents focused on traditional warfare, we have yet to address the most basic questions about cyber-conflicts.

What is the right strategy for this most modern of wars? Look to history. During the Cold War, when the United States faced an existential threat from the Soviet Union, we relied on deterrence to protect ourselves from nuclear attack. Later, as the East-West stalemate ended and nuclear weapons proliferated, some argued that preemption made more sense in an age of global terrorism.

The cyber-war mirrors the nuclear challenge in terms of the potential economic and psychological effects. So, should our strategy be deterrence or preemption? The answer: both. Depending on the nature of the threat, we can deploy aspects of either approach to defend America in cyberspace.

During the Cold War, deterrence was based on a few key elements: attribution (understanding who attacked us), location (knowing where a strike came from), response (being able to respond, even if attacked first) and transparency (the enemy's knowledge of our capability and intent to counter with massive force).

Against the Soviets, we dealt with the attribution and location challenges by developing human intelligence behind the Iron Curtain and by fielding early-warning radar systems, reconnaissance satellites and undersea listening posts to monitor threats. We invested heavily in our response capabilities with intercontinental ballistic missiles, submarines and long-range bombers, as well as command-and-control systems and specialized staffs to run them. The resources available were commensurate with the challenge at hand -- as must be the case in cyberspace.

Just as important was the softer side of our national security strategy: the policies, treaties and diplomatic efforts that underpinned containment and deterrence. Our alliances, such as NATO, made clear that a strike on one would be a strike on all and would be met with massive retaliation. This unambiguous intent, together with our ability to monitor and respond, provided a credible nuclear deterrent that served us well.

How do we apply deterrence in the cyber-age? For one, we must clearly express our intent. Secretary of State Hillary Rodham Clinton offered a succinct statement to that effect last month in Washington, in a speech on Internet freedom. "Countries or individuals that engage in cyber-attacks should face consequences and international condemnation," she said. "In an Internet-connected world, an attack on one nation's networks can be an attack on all."

That was a promising move, but it means little unless we back it up with practical policies and international legal agreements to define norms and identify consequences for destructive behavior in cyberspace. We began examining these issues through the Comprehensive National Cybersecurity Initiative, launched during the George W. Bush administration, but more work is needed on outlining how, when and where we would respond to an attack. For now, we have a response mechanism in name only.

The United States must also translate our intent into capabilities. We need to develop an early-warning system to monitor cyberspace, identify intrusions and locate the source of attacks with a trail of evidence that can support diplomatic, military and

legal options -- and we must be able to do this in milliseconds. More specifically, we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment -- who did it, from where, why and what was the result -- more manageable. The technologies are already available from public and private sources and can be further developed if we have the will to build them into our systems and to work with our allies and trading partners so they will do the same.

Of course, deterrence can be effective when the enemy is a state with an easily identifiable government and location. It is less successful against criminal groups or extremists who cannot be readily traced, let alone deterred through sanctions or military action.

There are many organizations (including al-Qaeda) that are not motivated by greed, as with criminal organizations, or a desire for geopolitical advantage, as with many states. Rather, their worldview seeks to destroy the systems of global commerce, trade and travel that are undergirded by our cyber-infrastructure. So deterrence is not enough; preemptive strategies might be required before such adversaries launch a devastating cyber-attack.

We preempt such groups by degrading, interdicting and eliminating their leadership and capabilities to mount cyber-attacks, and by creating a more resilient cyberspace that can absorb attacks and quickly recover. To this end, we must hammer out a consensus on how to best harness the capabilities of the National Security Agency, which I had the privilege to lead from 1992 to 1996. The NSA is the only agency in the United States with the legal authority, oversight and budget dedicated to breaking the codes and understanding the capabilities and intentions of potential enemies. The challenge is to shape an effective partnership with the private sector so information can move quickly back and forth from public to private -- and classified to unclassified -- to protect the nation's critical infrastructure.

We must give key private-sector leaders (from the transportation, utility and financial arenas) access to information on emerging threats so they can take countermeasures. For this to work, the private sector needs to be able to share network information -- on a controlled basis -- without inviting lawsuits from shareholders and others.

Obviously, such measures must be contemplated very carefully. But the reality is that while the lion's share of cybersecurity expertise lies in the federal government, more than 90 percent of the physical infrastructure of the Web is owned by private industry. Neither side on its own can mount the cyber-defense we need; some collaboration is inevitable. Recent reports of a possible partnership between Google and the government point to the kind of joint efforts -- and shared challenges -- that we are likely to see in the future.

No doubt, such arrangements will muddy the waters between the traditional roles of the government and the private sector. We must define the parameters of such interactions, but we should not dismiss them. Cyberspace knows no borders, and our defensive efforts must be similarly seamless.

Ultimately, to build the right strategy to defend cyberspace, we need the equivalent of President Dwight D. Eisenhower's Project Solarium. That 1953 initiative brought together teams of experts with opposing views to develop alternative strategies on how to wage the Cold War. The teams presented their views to the president, and Eisenhower chose his preferred approach -- deterrence. We now need a dialogue among business, civil society and government on the challenges we face in cyberspace -- spanning international law, privacy and civil liberties, security, and the architecture of the Internet. The results should shape our cybersecurity strategy.

We prevailed in the Cold War through strong leadership, clear policies, solid alliances and close integration of our diplomatic, economic and military efforts. We backed all this up with robust investments -- security never comes cheap. It worked, because we had to make it work.

Let's do the same with cybersecurity. The time to start was yesterday.

Mike McConnell was the director of the National Security Agency in the Clinton administration and the director of national intelligence during President George W. Bush's second term. A retired Navy vice admiral, he is executive vice president of Booz Allen Hamilton, which consults on cybersecurity for the private and public sector.

Lessons Learned in World War Two Pacific Are Relevant to Today's Cyber Security Challenges

(Originally published in Defense Systems on June 26, 2012)

by Mike McConnell

Earlier this month, I had the pleasure of speaking at a commemoration in Hawaii of the 70th Anniversary of the allied victory at Midway — a critical turning point in the war in the Pacific and one that was largely made possible by the U.S.'s ability to break Japanese codes, thereby allowing Pacific Commander Admiral Nimitz to know where the enemy was — and where they were headed.

The Battle of Midway happened a long time ago, but not so long ago that I haven't had the pleasure of crossing paths with some of its key figures. My role, as a former Naval Intelligence officer and the nation's chief code breaker as the Director of the National Security Agency in the 90's, was to provide context and to introduce a real American hero and one of last surviving members of Admiral Nimitz's code-breaking team, Rear Admiral Max Showers. As a 22-year-old ensign, Admiral Showers was a hands-on participant in the successful code breaking and code group recovery effort that turned the war.

As he spoke with riveting clarity at the Midway commemoration, RADM Showers told listeners he was "absolutely certain, despite all the books and articles that have speculated otherwise, the US did not have the information and could not have prevented the successful Japanese attack on Pearl Harbor." While RADM Showers has always served as a role model and inspiration for dedicated public service to me, I have to differ with my respected, senior friend – and it's a disagreement that pertains not just to the past, but, more importantly, to the future.

The U.S. was successful in breaking the Japanese Imperial Naval code "after Pearl Harbor" because that is when we were forced to put the needed resources and talent on a problem of national significance. Had we started our code breaking efforts at the same level of commitment and intensity in the late 30's or even in 1940, we would have been successful in decrypted and translating information to provide Japanese intentions and the disposition of their forces well before Pearl Harbor.

Is Past Prologue?

Today, we find the nation in very much the same posture as 1941, albeit pre-December 7, 1941. The former CIA Director and present Secretary of Defense, Leon Panetta, has stated that our next catastrophic event is likely to be a "Cyber Pearl Harbor" It's hardly scaremongering. The nation is bombarded daily by nation-states with policies of cyber

economic espionage that are successful extracting terabits of sensitive, competitive information that drives the US business engine. Our strength has been our ability to invent and innovate and this information is being massively taken on a daily basis. Additionally, nation states are building thousands of cyber-attack tools intended for degradation and destruction in war or conflict. Sooner or later, some of these cyber-attack tools will get inadvertently released in the cyber global commons or intentionally sold to some terrorist group hoping to change the current world order to fit their view of the future.

We have the information and ability today to prevent a Cyber Pearl Harbor. The question is, will we take steps to avoid it, or will we wait for it to happen? The US Intelligence Community (USIC) recovers vast amounts of threat vector information that could be used to screen and protect the nation – in both the public and private sector. However, our current laws and policies do not allow the USIC to share the information in an effective way – their hands are tied, a dynamic that serves only our foes,. While there are as many as seven draft bills in Congress to address these issues, the arguments against are framed by concerns for privacy and civil liberties on one side and concerns about "regulating" industry on the other.

Public-Private Partnership: It's Achievable (and A Model Already Exists)

To protect the nation, we need robust and timely sharing of sensitive information between the government and the private sector in a "public-private" partnership.

Of course, nearly any time the prospect of public-private partnerships involving IT security are discussed, the concept is battered, equally, by two somewhat opposing camps — on one side, privacy advocates and, on the other, those who oppose any regulation of businesses.

I believe that the privacy concern can be addressed via legislation and regulation that clearly defines what would be illegal practices for the government to do, and the regulation concern could be addressed via opt-in-only mechanisms that encourage participation via a number of benefits, including more information, liability protections and the benefits of standards.

The more critical point is that there is an excellent model already in place for a public-private partnership, focusing, no less, on information sharing in the IT space, and its roots go back nearly 50 years.

The National Security Telecommunications Advisory Committee (NSTAC) facilitates information sharing between the public and private sectors related to threats to the operations of our national telecommunications infrastructure. Having evolved out of the National Communications System, which began in the JFK era, NSTAC works — for the

shared benefit of the public — and it works well. It's one example of a model for cooperation that could be harnessed to address today's growing cyber threats.

Beyond the example of NSTAC, there's a more fundamental truth at hand. Good security – whether cybersecurity or any other kind of security — requires *communications*, namely the controlled sharing of relevant information. If you don't have that – or deny the common sense that underpins it — you're only going to have a facsimile of security, not the real thing.

Now is the time for all sides to relax opposition to work together to frame and pass the needed legislation for effective cyber defense. Otherwise, like Pearl Harbor and 9-11, we will strongly react "after the fact" when damage has been inflicted. What a waste.

Mike McConnell is a former vice admiral in the United States Navy. During his naval career he served as director of the National Security Agency (NSA) from 1992-1996; serving first under President George H. W. Bush and later under President Clinton. As a civilian Mr. McConnell served as the Director of National Intelligence (DNI) for two years, a position of Cabinet rank, under Presidents George W. Bush and Barrack Obama. He is currently Vice Chairman at Booz Allen Hamilton.

China's Cyber Thievery is National Policy, and It Must Be Challenged

by Mike McConnell, Michael Chertoff, and William Lynn

This piece originally appeared in the Wall Street Journal in January 2012.

Only three months ago, it would have been a violation of national security rules for us to share what we are about to say, even though, as the former Director of National Intelligence (DNI), Secretary of Homeland Security, and Deputy Secretary of Defense, we have long known this to be true: The Chinese government has a national policy of economic espionage in cyberspace. In fact, the Chinese are the world's most active and persistent practitioners of cyber espionage today.

Evidence of China's economically devastating thefts of proprietary technologies and other intellectual property of U.S. companies is growing exponentially, and only in October 2011 were the details declassified in a report to Congress by the Office of the National Counterintelligence Executive. By contrast, as a matter of official national policy, the United States does not engage in or allow economic espionage.

The report is a powerfully frank summation of what we believe is the potentially catastrophic impact these actions could have on the U.S. economy and global competitiveness over the next decade. Evidence indicates that China intends to help build its economy by intellectual property theft rather than by innovation and investment in research and development, two strong suits of the U.S. economy. Indeed, the nature of the Chinese economy today offers a powerful motive to do so, potentially costing the U.S. our technological leadership, billions in capital and probably millions of jobs.

For the last two years, we each have been speaking and writing publicly about the growing threat of potential cyber attacks on our critical infrastructure – the ability of cyber terrorists to cripple our financial networks or power grid. But this report finally reveals what we could not say before: That the threat of cyber 'economic espionage' looms even more ominously.

According to 2009 estimates by the United Nations, China today has a population of 1.33 billion people, with 468 million, about 36 percent of the population, living on less than $2 a day. While Chinese poverty has declined dramatically in the last 30 years, income inequality has increased, with much greater benefits going to the relatively small portion of educated people in urban areas where only about 25 percent of the population lives.

The statistical bottom line is this: China has a massive, inexpensive workforce, ravenous for economic growth. It is much more efficient for the Chinese to steal innovations and intellectual property -- the 'source code' of advanced economies – than it is for them to incur the cost and time of creating their own. Instead, they can and do turn those stolen ideas directly into production, creating products faster and cheaper, and outselling the United States and others worldwide. There is ample public evidence this is already occurring.

Cyberspace is an ideal medium for the theft of intellectual capital because of the ability to easily penetrate systems for transfer of large amounts of data, and the difficulty in confirming specific perpetrators.

Unfortunately, it is also difficult to extrapolate an estimated economic cost of these thefts to the U.S. economy – the report to Congress calls the cost "large," and notes that this includes corporate revenues, jobs, innovation and impacts to national security. Although a rigorous assessment has not been done, we think it is safe to say that "large" easily means billions of dollars and millions of jobs.

So how do we protect ourselves from this economic threat? First, we must acknowledge the threat's severity, understanding that the impacts are more long term than immediate. And we need to respond to this 'economic espionage' with all of the diplomatic, trade, economic and technology tools at our disposal, enhancing them as needed.

The report to Congress notes that the U.S. Intelligence Community (USIC) has improved its collaboration to better address cyber espionage in the military and national security areas. Yet today's legislative framework severely restricts the USIC from fully addressing domestic economic espionage. The USIC must have a stronger role in collecting and analyzing this economic data and making it available to appropriate government and commercial entities.

Congress and the administration must also create the means to actively force more information sharing. Frankly, while organizations proclaim to share information, it is usually the opposite, and this must be actively enforced.

The U.S. also must make the broader investment in education to produce many more workers with science, technology, engineering and math (STEM) skills. Our country reacted to the Soviet Union's 1957 launch of Sputnik with math and science education investments that launched the age of digital communications. Now is the time for a similar approach to build the skills our nation will need to compete in a global economy vastly different from 50 years ago.

Finally, Corporate America must do its part, too. If we are to ever understand the extent and impact of cyber espionage, companies must be more open and aggressive about identifying, acknowledging and reporting cyber theft incidents. Already, Congress is considering legislation to require this, and the idea deserves support. Additionally, companies must invest more in the training of staff in cyber skills; it is shocking how many cyber breaches result from simple human error.

In this coming election year, debate over the U.S. economy will be on center stage, as will China and its role in issues such as monetary policy. If we are to act quickly to prevent irreversible long term damage, the economic issues behind cyber espionage must share some of that spotlight as well.

Mike McConnell *was the director of the National Security Agency in the Clinton Administration and the director of national intelligence during President George W. Bush's second term. A retired Navy vice admiral, he is executive vice president of Booz Allen Hamilton, which consults on cybersecurity for the private and public sector.*

Michael Chertoff *was the Secretary of the Department of Homeland Security under President George W. Bush. He is now is senior counsel in Covington & Burling's Washington, DC office.*

William J. Lynn *was the Deputy Secretary of Defense in the Obama Administration and the Under Secretary of Defense in the Clinton Administration.*

To Win the Cyber War, We Have to Reinforce the Cloud

Mike McConnell

This article originally appeared in the Financial Times on April 25, 2011

Many challenged my grim assessment early last year, when I called for America to develop a new strategy to address the kinds of cyber attacks that could cripple our nation's infrastructure. If there were a cyber war, I told Congress, we would lose. The unfortunate truth is that, a year later, we are no better prepared – and the stakes have risen.

Since then, more details have emerged on the early 2010 attacks on Google and two dozen other companies, connecting them to China. Alongside the revelations about the Stuxnet attack on Iran and the Wikileaks saga, t he question today is no longer whether the cyber threat is real – that was last year's discussion. The challenge now is what to do about it, while balancing security, privacy, openness and innovation.

We should immediately focus on protecting critical infrastructure – the power grid, financial networks, air traffic control and other transport infrastructure — by realigning their use of the internet. To do this we must create new "protected lanes" inside the global superhighway. I call this potential area "dot.secure": a series of highly protected lanes for those operating vital infrastructure, within the free and open world of the .com global network.

The WikiLeaks saga has generated intense debate about whether the release of such information is in the public interest. To be clear, I am not an advocate of doing away with the freedom of our citizens and their use of the internet. But I would also argue that we are a nation of laws, and everyone is entitled to privacy – individuals, businesses and, yes, government. To do its business effectively the government must be able to exchange information with other governments in private. Businesses must be able to protect innovation and patented information; individuals must be able to keep the ownership of their new ideas.

There also needs to be defined areas of the internet where that can take place – where individuals can post to blogs, create videos, comment on the news and be completely anonymous – and other places where access to specific data is restricted. Equally we must develop access systems for sensitive business where an individual is limited to data essential to his or her task.

Highly secure and open areas of the internet do exist today. The defence department runs ".mil," a domain with limited gateways, military grade encryption, perimeter security and support from the National Security community to identify foreign threats. The government's ".gov" domain has a similar goal of limited gateways, but will also benefit from high-grade encryption.

On the other side of the information highway, the .com lanes are open with easy movement and access, requiring only the level of security that an individual or business requires for themselves. These open lanes are less costly to maintain, and will benefit even more from the economies of cloud computing, a powerful, cost-efficient shared computing environment.

What's missing is the middle ground; dot.secure. The nation's finance, electric, power, water, land transport, air traffic control, industrial control systems must be protected within the security of the restricted lanes. Each month, we understand more about how to heighten security in the economically efficient "cloud", and our technicians develop more nuanced approaches to security architecture. Beyond that, cloud operators can focus on network intrusion prevention and response to protect information and its users.

We need to apply the evolving knowledge of cloud-security to our infrastructure through a new government / private partnership. The administration and Congress know the seriousness of cyber threats, but they are not moving fast enough to address them.

As we look at this challenge, we must remember that cyberspace is more than just the internet. It is a domain itself. For America to protect the foundation of our economy and way of life as we have in the other domains, we cannot wait for the next big attack to shock us into action.

The writer was the director of the National Security Agency in the Clinton administration and the director of national intelligence during President George W. Bush's second term. He is executive vice president of Booz Allen Hamilton.

Mrs. BLACKBURN. Thank you, Mr. McConnell.
Ambassador Woolsey, you are recognized for 5 minutes.

STATEMENT OF R. JAMES WOOLSEY

Mr. WOOLSEY. Thank you, Madam Chairman. I am going to talk about a little different kind of cyber than normally comes into the picture. Congressman Burgess referred earlier to Dr. Peter Pry's and my op-ed in the Wall Street Journal this morning on this subject.

It has to do with electromagnetic pulse. We don't get to define ourselves the problems we want to deal with and ignore them because they don't fit into some bureaucratic category of ours. Both Russia and China as well as North Korea and Iran include the use of electromagnetic pulse against our infrastructure as part of information warfare and cyber warfare, and they are working hard at it.

Electromagnetic pulse may hit the world, the United States and other parts of it, through solar activity, and some people focus principally on this called coronal mass ejections. It is essentially a huge solar storm, much better than anything we normally experience. It happens about once every 100 years, and we are somewhat overdue for one of these. These could have a very, very powerful effect on our electric grid. But insofar as we are talking about human activity, the basic problem is that a detonation of even a relatively small blast nuclear weapon 30 kilometers or more above the United States, let us say on a warhead that is in orbit or one that is carried aloft even by a weather balloon, can seriously, very seriously damage and indeed destroy a substantial share of the electricity connections that hold together our electric grid. One estimate from the report of the commission to assess the threat to the United States of electromagnetic pulse, a congressional commission that reported in 2004 and in 2008, is that with a relatively low-level attack launched only by a weather balloon could take out approximately 70 percent of the country's electricity with a single blast.

What is going on here is that gamma rays are one of the products of a nuclear detonation. We are all used to thinking of nuclear detonations as being more powerful and more damaging if there is a lot of blast because blast is what would be used to attack a specific target on the ground—a military installation, an ICBM silo or whatever. Electromagnetic pulse is different. It is something that occurs because of the gamma rays that are sent out by a nuclear detonation but an extremely effective electromagnetic pulse weapon could have a lot of radiation and very little blast—two, three, four single-digit blast efforts coupled with a lot of gamma rays and nuclear emanations of different kinds. What that produces, even if it as high as several hundred kilometers, is three waves of electromagnetic pulse, the first and third being the damaging ones, the first one attacking essentially all electronic connections, and the third one attacking the grid itself, particularly the transformers and the long-range transfer systems.

The Chinese leading theorist on this subject, Chang Mengxiong, says that information war and traditional war have one thing in common, namely that the country which possesses a critical weapon such as atomic bombs will have first-strike capabilities. As soon

as its computer networks come under attack and are destroyed, the country will slip into a state of paralysis and the lives of its people will ground to a halt. North Korea appears to be attempting to implement information warfare doctrine with electromagnetic pulse. In December of 2012, it demonstrated that it had the capability to launch a satellite on a polar orbit circling the earth at an altitude of 500 kilometers. That high, it is not entirely clear that we would be able to destroy that satellite essentially carrying a nuclear weapon in orbit. We have canceled all of our programs dealing with boost-phase or space-based defensive systems, and indeed, the Administration has not even requested any study money for this type of system, which would potentially have a substantial effect on this type of threat.

I would urge—and finally, I see the time is over—I would urge that we not get bogged down in the issue of volunteerism versus government order. On something like this, we have to have a national policy and a national commander-in-chief, presumably the President, but with someone reporting to him who is in charge of dealing with this kind of threat. The taking out of our electric grid takes out all 17 other critical infrastructures. It takes out food, it takes out water, it takes out natural gas, it takes out practically everything you can think of. The casualty estimates for electromagnetic pulse attack in the congressional report are up in the range of two-thirds of the country dying under such an attack because there would be after a very short period of time no food, no electricity, no water, etc.

Mrs. BLACKBURN. Ambassador, if you would wrap up.

Mr. WOOLSEY. The North Koreans have already tested both low-yield and we believe high-gamma-ray nuclear weapons. They have tested satellites, put a satellite in orbit. The Iranians have put three satellites in orbit and are in the process of working very hard on having a nuclear weapon. We could well within months have two rogue states who are capable of launching this type of attack against the United States as part of their information warfare cyber campaign.

Thank you, Madam Chairman.

[The prepared statement of Mr. Woolsey follows:]

R. JAMES WOOLSEY
TESTIMONY
BEFORE THE
HOUSE COMMITTEE ON ENERGY AND COMMERCE
May 21, 2013

This hearing is about cyber threats and solutions. But I am going to talk about a dimension of the cyber threat that is not usually considered a cyber threat in Western doctrine, but is in the playbooks for an Information Warfare Operation of Russia, China, North Korea, and Iran. These potential adversaries in their military doctrines include as a dimension of cyber warfare a wide spectrum of operations beyond computer viruses, including sabotage and kinetic attacks, up to and including nuclear electromagnetic pulse (EMP) attack.

It is vitally important that we understand that a nuclear EMP attack is part of cyber and information warfare operations as conceived by our potential adversaries. Our cyber doctrine must be designed to deter and defeat the cyber doctrines of our potential adversaries by anticipating how they plan to attack us--but our doctrine currently does not.

Our cyber and information warfare doctrines are dangerously blind to the likelihood that a potential adversary making an all-out information warfare campaign designed to cripple U.S. critical infrastructures would include an EMP attack.

The assessment that nuclear EMP attack is included in the cyber and information warfare doctrine of potential adversaries, and the effects of an EMP attack described here, are based on the work of the Congressional EMP Commission that analyzed this threat for nearly a decade (2001-2008). The Congressional Strategic Posture Commission and several other major U.S. Government studies independently arrived at similar conclusions, and represent collectively a scientific and strategic consensus that nuclear EMP attack upon the United States is an existential threat.

What is EMP? A nuclear weapon detonated at high-altitude, above 30 kilometers, will generate an electromagnetic pulse that can be likened to a super-energetic radio wave, more powerful than lightning, that can destroy and disrupt electronics across a broad geographic area, from the line of sight from the high-altitude detonation to the horizon.

For example, a nuclear weapon detonated at an altitude of 30 kilometers would project an EMP field with a radius on the ground of about 600 kilometers, that could cover all the New England States, New York and Pennsylvania, damaging electronics across this entire region, including electronics on aircraft flying across the region at the time of the EMP attack. The EMP attack would blackout at least the regional electric grid, and probably the entire Eastern Grid that generates 70 percent of U.S. electricity, for a protracted period of weeks, months, possibly years. The blackout and EMP damage beyond the electric grid in other systems would collapse all the other critical infrastructures--communications, transportation, banking and finance, food and water--that sustain modern civilization and the lives of millions.

Such an EMP attack, a nuclear detonation over the U.S. East Coast at an altitude of 30 kilometers, could be achieved by lofting the warhead with a meteorological balloon.

A more ambitious EMP attack could use a freighter to launch a medium-range missile from the Gulf of Mexico, to detonate a nuclear warhead over the geographic center of the United States at an altitude of 400 kilometers. The EMP field would extend to a radius of 2,200 kilometers on the ground, covering all of the contiguous 48 United States, causing a nationwide blackout and collapse of the critical infrastructures everywhere. All of this would result from the high-altitude detonation of a single nuclear warhead.

The Congressional EMP Commission warned that Iran appears to have practiced exactly this scenario. Iran has demonstrated the capability to launch a ballistic missile from a vessel at sea. Iran has also several times practiced and demonstrated the capability to detonate a warhead on its medium-range Shahab III ballistic missile at the high-altitudes necessary for an EMP attack on the entire United States. The Shahab III is a mobile missile, a characteristic that makes it more suitable for launching from the hold of a freighter. Launching an EMP attack from a ship off the U.S. coast could enable the aggressor to remain anonymous and unidentified, and so escape U.S. retaliation.

The Congressional EMP Commission warned that Iran in military doctrinal writings explicitly describes making a nuclear EMP attack to eliminate the United States as an actor on the world stage as part of an Information Warfare Operation. For example, various Iranian doctrinal writings on information and cyber warfare make the following assertions:

- "Nuclear weapons...can be used to determine the outcome of a war...without inflicting serious human damage [by neutralizing] strategic and information networks."

- "Terrorist information warfare [includes]...using the technology of directed energy weapons (DEW) or electromagnetic pulse (EMP)."

- "...today when you disable a country's military high command through disruption of communications you will, in effect, disrupt all the affairs of that country....If the world's industrial countries fail to devise effective ways to defend themselves against dangerous electronic assaults, then they will disintegrate within a few years."

China's premier military textbook on information warfare, written by China's foremost expert on cyber and information warfare doctrine, makes unmistakably clear that China's version of an all-out Information Warfare Operation includes both computer viruses and nuclear EMP attack. According to People's Liberation Army textbook *World War, the Third World War--Total Information Warfare*, written by Shen Weiguang, "Therefore, China should focus on measures to counter computer viruses, nuclear electromagnetic pulse...and quickly achieve breakthroughs in those technologies...":

> *With their massive destructiveness, long-range nuclear weapons have combined with highly sophisticated information technology and information warfare under nuclear deterrence....Information war and traditional war have one thing*

> *in common, namely that the country which possesses the critical weapons such as atomic bombs will have "first strike" and "second strike retaliation" capabilities ....As soon as its computer networks come under attack and are destroyed, the country will slip into a state of paralysis and the lives of its people will ground to a halt. Therefore, China should focus on measures to counter computer viruses, nuclear electromagnetic pulse...and quickly achieve breakthroughs in those technologies in order to equip China without delay with equivalent deterrence that will enable it to stand up to the military powers in the information age and neutralize and check the deterrence of Western powers, including the United States.*

North Korea appears to be attempting to implement the information warfare doctrine described above by developing a long range missile capable of making a catastrophic nuclear EMP attack on the United States. In December 2012, North Korea demonstrated the capability to launch a satellite on a polar orbit circling the Earth at an altitude of 500 kilometers. An altitude of 500 kilometers would be ideal for making an EMP attack that places the field over the entire contiguous 48 United States, using an inaccurate satellite warhead for delivery, likely to miss its horizontal aimpoint over the geographic center of the U.S. by tens of kilometers. North Korea's satellite did not pass over the United States--but a slight adjustment in its trajectory would have flown it over or near the U.S. bull's eye for a high-altitude EMP burst.

North Korea appears to have borrowed from the Russians their idea for using a so-called Space Launch Vehicle to make a stealthy nuclear attack on the United States. During the Cold War, Moscow developed a secret weapon called a Fractional Orbital Bombardment System (FOBS) that looked like a Space Launch Vehicle, but was designed to launch a nuclear warhead southward, away from the United States initially, but deliver the warhead like a satellite on a south polar orbit, so the nuclear attack comes at the U.S. from the south. The United States has no Ballistic Missile Early Warning (BMEW) radars or missile interceptors facing south. We might not even see the attack coming.

Miroslav Gyurosi in *The Soviet Fractional Orbital Bombardment System* describes Moscow's development of the FOBS:

> *The Fractional Orbital Bombardment System (FOBS) as it was known in the West, was a Soviet innovation intended to exploit the limitations of U.S. BMEW radar coverage. The idea behind FOBS was that a large thermonuclear warhead would be inserted into a steeply inclined low altitude polar orbit, such that it would approach CONUS from any direction, but primarily from the southern hemisphere, and following a programmed braking maneuver, re-enter from a direction which was not covered by BMEW radars.*

"The first warning the U.S. would have of such a strike in progress would be the EMP...," writes Gyurosi.

The trajectory of North Korea's satellite launch of December 12, 2012 looked very much like a Fractional Orbital Bombardment System for EMP attack. The missile launched southward, away

from the United States, sent the satellite over the south polar region, approaching the U.S. from the south, at the optimum altitude for EMP attack--although the test trajectory deliberately avoided flying over the United States.

North Korea appears to have borrowed from Russia more than the FOBS. In 2004, a delegation of Russian generals met with the Congressional EMP Commission to warn that design information for a Super-EMP nuclear warhead had leaked from Russia to North Korea, and that North Korea might be able to develop such a weapon "in a few years." A few years later, in 2006, North Korea conducted its first nuclear test, of a device having a very low yield, about 3 kilotons. All three North Korean nuclear tests have had similarly low yields. A Super-EMP warhead would have a low-yield, like the North Korean device, because it is not designed to create a big explosion, but to produce gamma rays, that generate the EMP effect.

According to several press reports, South Korean military intelligence concluded independently of the EMP Commission that Russian scientists are in North Korea helping develop a Super-EMP nuclear warhead. In 2012, a military commentator for the People's Republic of China stated that North Korea has Super-EMP nuclear warheads.

One design of a Super-EMP warhead would be a modified neutron bomb, more accurately an Enhanced Radiation Warhead (ERW) because it produces not only large amounts of neutrons but large amounts of gamma rays, that cause the EMP effect. One U.S. ERW warhead (the W-82) deployed in NATO during the Cold War weighed less than 50 kilograms. North Korea's so-called Space Launch Vehicle, which orbited a satellite weighing 100 kilograms, could deliver such a warhead against the U.S. mainland--or against any nation on Earth.

Iran may already have a FOBS capability, as it has successfully launched several satellites on polar orbits, assisted by North Korean missile technology and North Korean technicians. Iranian scientists were present at all three North Korean nuclear tests, according to press reports.

What is to be done about the Cyber and EMP threats?

Technically, it is important to understand that surge arrestors and other hardware designed to protect against EMP can also protect against the worst-case cyber scenarios that, for example, envision computer viruses collapsing the national power grid. For example, surge arrestors that protect Extra High Voltage transformers from EMP can also protect transformers from damaging electrical surges caused by a computer virus that manipulates the grid Supervisory Control And Data Acquisition Systems (SCADAS).

Administratively, a coherent and effective answer will not likely arise from uncoordinated decisions made independently by the thousands of individual industries at risk. Because cyber preparedness should encompass EMP preparedness--and since EMP is an existential threat--it is imperative that Government play a supervisory and coordinating role to achieve protection against these threats swiftly.

House Energy & Commerce Committee Hearing:
Cyber Threats and Security Solutions
10:00 am, May 21, 2013

One page Overview of Dr. Mike Papay's Statement:

Northrop Grumman is one of the leading cybersecurity providers to the federal government and has expansive and in-depth knowledge, experience and expertise in these critical aspects of our nation's technology framework. We build, supply, and manage cyber solutions for customers that include the Department of Defense, intelligence community, civilian agencies, international governments, state and local government and the private sector. Northrop Grumman is honored to be trusted with the challenge of protecting some of the world's most targeted systems.

The Defense Industrial Base's information sharing program has demonstrated the benefits of industry-government collaboration. Northrop Grumman was a founding member of this groundbreaking framework. While this effort has demonstrated that public/private information sharing can yield many successes, we also learned that some of the toughest challenges are not technological but cultural and legal. Northrop Grumman was proud to announce last week that it will participate in the next generation government- private sector information sharing program, DHS' Enhanced Cybersecurity Services (ECS) program.

Given our experience, Northrop Grumman very much appreciates the seriousness and urgency of the cyber threat. We do believe that the President's Executive Order (EO) is an important step in the right direction. The EO's ultimate success will be determined by the effectiveness of the individual agencies' efforts in implementing their assigned responsibilities. We appreciate the government's ongoing outreach to industry and we recently actively engaged with NIST to support the development of its Cybersecurity Framework. However, the EO alone cannot address the full range of cybersecurity issues. Legislation is still required to facilitate and encourage companies to secure their own networks and break down the barriers to sharing cyber threat information.

We applaud the House of Representatives recent passage of cybersecurity legislation, especially the strong bipartisan vote in favor of the Cyber Intelligence Sharing Protection Act, which we hope will build momentum towards bills passing both chambers.

Northrop Grumman is committed to utilizing our experience to support the development of successful cyber policies. We encourage legislation that improves the agility of the federal acquisition process to address rapidly evolving cyber threats, increases investments in cybersecurity technology and training of our current workforce, and supports the development of the next generation of scientists and engineers. We must be mindful, however, that our nation's cybersecurity cannot be fixed with one law or policy change. Effective cybersecurity policies should be risk- based and as adaptable as the threat itself. These cyber efforts must also carefully balance civil liberties and greater security. These are not mutually exclusive goals. Indeed, if we do not strengthen our cyber defenses, we imperil the civil liberties that we hold dear.

Mrs. BLACKBURN. And thank you.
Dr. Papay for 5 minutes.

STATEMENT OF MICHAEL PAPAY

Mr. PAPAY. Madam Chair and other members of the committee, Northrop Grumman appreciates the opportunity to discuss this critically important topic with you today. I am Mike Papay. I am the Chief Information Security Officer and Vice President for Cyber Initiatives for Northrop Grumman. That means I cover both the internal cyber business of Northrop Grumman as well as the external cyber strategy.

Northrop Grumman is one of the leading cybersecurity providers to the federal government and has expansive and in-depth knowledge, experience and expertise in these critical aspects of our Nation's technology framework. We build, supply and manage cyber solutions for customers that include the Department of Defense, intelligence communities, civilian agencies, international governments, state and local governments, and the private sector. Northrop Grumman is honored to be trusted with the challenge of protecting some of the world's most targeted systems.

The Defense Industrial Base's information sharing program has demonstrated the benefits of industry-government collaboration. Northrop Grumman was a founding member of this groundbreaking framework. While this effort has demonstrated that public-private information sharing can yield many successes, we also learned that some of the toughest challenges are not technological but cultural and legal. Northrop Grumman was proud to announce last week that it will participate in the next-generation government-private sector information-sharing program, DHS's Enhanced Cybersecurity Services.

Given our experience, Northrop Grumman very much appreciates the seriousness and urgency of the cyber threat. We do believe that the President's Executive order is an important step in the right direction, but the EO's ultimate success will be determined by the effectiveness of the individual agencies' efforts in implementing their assigned responsibilities. We appreciate the government's ongoing outreach to industry, and we recently actively engaged with NIST to support the development of its cybersecurity framework. However, the EO alone cannot address the full range of cybersecurity issues. Legislation is still required to facilitate and encourage companies to secure their own networks and break down the barriers to sharing cyber threat information.

We applaud the House of Representatives' recent passage of cybersecurity legislation, especially the strong bipartisan vote in favor of the CISPA, which we hope will build momentum towards bills passing both chambers.

Northrop Grumman is committed to utilizing our experience to support the development of successful cyber policies. We encourage legislation that improves the agility of the federal acquisition process to address rapidly evolving cyber threats, increases investments in cybersecurity technology and training of our current workforce, and supports the development of the next generation of scientists and engineers. We must be mindful, however, that our Nation's cybersecurity cannot be fixed with one law or policy change. Effec-

tive cybersecurity policies should be risk-based and as adaptable as the threat itself. These cyber efforts must also carefully balance civil liberties and greater security. These are not mutually exclusive goals. Indeed, if we do not strengthen our cyber defenses, we imperil the civil liberties that we hold dear.

Please consider Northrop Grumman a resource. We look forward to working with Members of Congress on both sides of the aisle and the Administration to make our world safer and more secure.

I look forward to answering any questions you might have.

[The prepared statement of Mr. Papay follows:]

House Energy & Commerce Committee Hearing:
"Cyber Threats and Security Solutions"
10:00 am, May 21, 2013

Prepared Statement for Record
Dr. Michael Papay
Chief Information Security Officer &
Vice- President, Cybersecurity Initiatives,
Northrop Grumman

Chairman Upton, Ranking Member Waxman and other members of the committee, Northrop Grumman appreciates the opportunity to discuss this critically important topic with you. My name is Mike Papay and I am the Chief Information Security Officer and Vice President for Cyber Initiatives at Northrop Grumman. In this capacity I am responsible for both Northrop Grumman's internal network security and I lead the company's cyber strategy development.

Secretary Janet Napolitano recently stated in a joint hearing before the Senate Committee on Commerce, Science, and Transportation and Senate Committee on Homeland Security and Governmental Affairs, quote, "We know that our adversaries are seeking to sabotage our power grid, our financial institutions, and our air traffic control systems. These intrusions and attacks are coming all the time and they are coming from different sources and take different forms, all the while increasing in seriousness and sophistication," unquote. I would add that emerging cyber threats also are targeting many of our nation's corporations, including small businesses, and individuals.

Exploitable vulnerabilities in our information infrastructure pose one of the most significant threats to our national and economic security facing us today – perhaps the most significant threat. The age in which we live is built on digitized information. Everything we do, the way we learn, the way we communicate depends on and produces digitized information. Digitized information governs the

medical care we receive, the security of our bank accounts, the quality of the water we drink and the food we eat, our ability to communicate with one another, and our access to the energy to heat our homes in the winter, keep them cool in the summer and power our way of life. As we become increasingly dependent on computers and digital technology, the quality of our lives improves. At the same time, we also become more vulnerable to threats to that technology, cyber attacks. If we hope to maintain our freedom, our security and our standards of living in this age, we must enhance and strengthen our cyber defenses.

Broadly defined, cybersecurity refers to the protection of our digitized assets from exploitation and attack on networks, systems, information, physical infrastructure, users and their privacy. Northrop Grumman is one of the leading cybersecurity providers to the federal government and has expansive and in-depth knowledge, experience and expertise in these critical aspects of our nation's technology framework. We build, supply, and manage cyber solutions for customers that include the Department of Defense, intelligence community, civilian agencies, international governments, state and local government and the private sector. Northrop Grumman is honored to be trusted with the challenge of protecting some of the world's most targeted systems. We pride ourselves on developing innovative solutions to tackle the toughest cyber challenges. We understand that effective cybersecurity not only means defending computers, networks and data, but also includes enhancing the security of the products we manufacture. From unmanned aircraft to radar systems, we work to make our products less vulnerable to cyber attacks.

Over the past decade, Northrop Grumman has implemented a set of internal cybersecurity controls that we continue to evolve to protect our own and our customers' intellectual property and

sensitive data. Essential elements of our cybersecurity practices include leveraging threat information from multiple sources and deploying cutting edge technologies. We have implemented security standards and architectural approaches, as recommended by the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO) Community and SANS Critical Security Controls.

We also focus on internal cybersecurity awareness training as part of our internal protection efforts. Northrop Grumman has developed its own internal cybersecurity training and a "Cyber Academy" that provides more in-depth cyber education to our employees and senior leaders. To further heighten cybersecurity awareness, Northrop Grumman conducts internal spear phishing exercises on our employees to enhance awareness.

Given the dynamic nature of cyber threats, it is essential to make the necessary investments to stay ahead of the threat. Northrop Grumman partners with a range of universities and has created the Cybersecurity Research Consortium with MIT, Carnegie Mellon, Purdue and USC to facilitate the development of next- generation cyber solutions. As part of the Consortium, Northrop Grumman sponsors graduate fellowships to research and address the hard problems of our customers. Our goal is to accelerate the pace of innovation in cybersecurity and ensure a talent pipeline of top researchers in this field. In addition to the Cybersecurity Research Consortium, Northrop Grumman has supported the establishment of the CYNC Cyber Incubator at University of Maryland- Baltimore College. The CYNC program sponsors innovative, technology-driven startup companies, addressing critical market needs for companies from across the country looking to further develop and commercialize their technologies.

These investments not only are focused on technological innovation, but also are meant to help build the talent pipeline for the next generation of cybersecurity innovators.

According to a 2010 U.S. Department of Commerce study, the number of science, technology, engineering, and math (STEM) jobs is expected to grow 17% in the next decade. I was privileged to serve on the 2012 Homeland Security Advisory Council's Task Force on CyberSkills. This Council focused on identifying far-reaching improvements that would enable DHS to recruit and retain the cybersecurity talent it needs. One of the council's recommended objectives was to radically expand the pipeline of highly qualified candidates for cyber jobs through innovative partnerships with community colleges, universities, organizers of cyber competitions, and other federal agencies. Northrop Grumman sees this as a critical objective for our company as well, which is why we have sponsored the nation's first ever cybersecurity honors program at the University of Maryland- College Park. We are also focusing our educational efforts on middle and high school students as the founding sponsor of the CyberPatriot program, which this year hosted over 1,200 teams from all 50 states, and DoD schools in Europe and the Pacific.

Due to the complexity and prevalence of cyber threats, no organization can or should face them alone. Industry specific peer-to-peer information sharing is critical because at the end of the day, we are all in this together. Northrop Grumman participates in many other industry venues committed to high levels of cybersecurity, including the Transglobal Secure Collaboration Program (TSCP), Internet Security Alliance, National Security Telecommunications Advisory Committee, and National Infrastructure Advisory Council.

The Department of Defense's Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) Program has demonstrated the benefits of industry-government collaboration. Northrop Grumman was a founding member of this groundbreaking framework, first established in 2007. The program had to overcome initial skepticism, even among participants, that industry members and the government could collaborate effectively to address cybersecurity risks. While the program demonstrated that public/private information sharing can yield many successes, we also learned that some of the toughest challenges are not technological but cultural and legal. As we all worked together, we found that sharing cyber threat information empowered us to respond faster, be proactive in defense, and more effectively secure the sensitive information that our Nation entrusts in us.

Northrop Grumman was proud to announce last week that it will participate in the next generation government- private sector information sharing program, the Department of Homeland Security's Enhanced Cybersecurity Services (ECS) program. ECS is an information sharing program to assist critical infrastructure owners and operators in enhancing the cybersecurity protections of their information systems from unauthorized access, exploitation and data exfiltration. Under ECS, DHS will share classified and unclassified cyber threat "indicators" with designated Commercial Service Providers, and the Commercial Services Providers will utilize the threat indicators to provide approved cybersecurity services to authorized critical infrastructure entities.

Given our experience, Northrop Grumman very much appreciates the seriousness and urgency of the cyber threat. We do believe that the President's Executive Order (EO) is an important step in the right direction. The EO sets the broad parameters for dealing with cybersecurity. The EO's ultimate success will be determined by the effectiveness of the individual agencies' efforts in implementing their assigned responsibilities. We appreciate the agencies' ongoing outreach to industry with respect to

those activities and we are committed to participating in those efforts. For example, we recently actively engaged with the National Institute of Standards and Technology (NIST) to support the development of its Cybersecurity Framework. Successful cyber strategies will constructively build upon what is currently working and not simply layer on new bureaucracy or requirements that add costs without improving overall cybersecurity. Either way, the EO alone cannot address the full range of cybersecurity issues. Legislation is still required to facilitate and encourage companies to secure their own networks and break down the barriers to sharing cyber threat information.

We applaud the House of Representatives passage of the Cyber Intelligence Sharing and Protection Act, the Federal Information Security Amendments Act, the Cybersecurity Enhancement Act, and the Advancing America's Networking and Information Technology Research and Development Act in the past few weeks. We are optimistic that this package of bills, especially the strong bipartisan vote in favor of the Cyber Intelligence Sharing and Protection Act, will help build momentum towards legislation passing both chambers.

Northrop Grumman strongly supports policies that accomplish the following cybersecurity goals:

- Strengthening critical infrastructure protection;
- Facilitating the two way sharing of threat information across the public and private sectors,
- Ensuring the protection of personal information and proprietary data;
- Requiring autonomous, continuous monitoring and threat assessment to enable the real-time situational awareness of the nation's networks and missions;

- Improving the agility of the federal acquisition process to address rapidly evolving cyber threats;
- Ensuring that the cyber risk of each program or product acquired by the government for critical functions are appropriately considered;
- Increasing investments in cybersecurity technology and training of our current workforce and supporting the development of the next generation of scientists and engineers;
- Ensuring the necessary marketplace incentives to encourage industry leaders to continue raising their levels of cybersecurity;

Northrop Grumman is committed to utilizing our experience to support the development of successful cyber policies. We must be mindful, however, that our nation's cybersecurity cannot be fixed with one law or policy change. Effective cybersecurity policies should be risk-based and as adaptable as the threat itself. These cyber efforts must also carefully balance civil liberties and greater security. These are not mutually exclusive goals. Indeed, if we do not strengthen our cyber defenses, we imperil the civil liberties that we hold dear.

Please consider Northrop Grumman a resource. We look forward to working with Members of Congress on both sides of the aisle and the administration to make our world safer and more secure.

Thank You. I would be happy to answer any questions that you may have.

Mrs. BLACKBURN. Thank you, Dr. Papay.
Dr. Schneck, you are recognized for 5 minutes.

STATEMENT OF PHYLLIS SCHNECK

Ms. SCHNECK. Good afternoon, and thank you, Vice Chairman and other members of the committee, and thank you very much on behalf of McAfee for the opportunity to testify here today.

I am the Vice President and Global Chief Technology Officer for Public Sector for McAfee looking at how our products adapt to protect global government, federal, State and local, and critical infrastructure, and I also have the honor of vice chairing the Information Security and Privacy Advisory Board that reports up to this committee. So thank you very much for that.

McAfee protects 160 million points of presence across the world, global cybersecurity products, largest peer placed security company on the planet, wholly owned subsidiary of the Intel Corporation with headquarters in Santa Clara, Plano, Texas, as well as our large labs operation in Oregon.

I want to start in the spirit of this testimony with an anecdote of the attack called Night Dragon on February of 2011 that McAfee led an investigation where we saw five oil and gas companies lose their oil exploration diagrams, all that intellectual property in a matter of weeks, and it was sent off to another country, and overnight as we put the whole story together, worked with our partners to share that information, worked with other companies, wanted to warn the sector, legal counsel came out in the middle of the night and said please don't, and they were deeply concerned at that point that if the stock prices of those companies affected and others throughout the sector dropped the next morning, McAfee would be liable. At the same night, I got an angry phone call from a high-ranking official in law enforcement very upset that we didn't share the information with him sooner. This is a position that we are all in at some time, and this is what we need to fix. We should never have to choose between protecting a sector, protecting our country versus legal liabilities. So in that spirit, I want to talk about two things, the science and policy, that I believe that we can use to fix this.

First, culling one of many technologies because it pertains so directly to the energy sector. The cybersecurity community has evolved. Instead of what we call blacklisting or letting everything in and then looking very carefully to figure out what we think might be bad and trying to block it, we instead what we now call whitelisting: only let in the things that we know are good, only let instructions execute if we know that they are good, and as a wholly owned subsidiary of Intel, I can tell you that we can do that all the way to the chip at the hardware. But going and evolving to that technology is difficult, and I will explain why in a moment, but this technology has expanded our ability to protect components as a community of the electric grid, of the energy sector, and across critical infrastructure.

The other piece is information sharing. We greatly applaud the efforts of NIST, of DHS, looking at how we partner together, public and private. We all see an enormous piece of this picture but it is not enough until we put it together. We all fight an adversary that

is fast and loose, has no legal boundaries and can execute on a moment's notice with all the power in the world and all the money in the world. If we can take our information and share it and put that puzzle together, we regain the power of our electronic infrastructures. This is what they cannot do. If you think about really sharing information at light speed between machines, we call this security connected at McAfee, but if you when block something, you are able to instantly in milliseconds warn other components around you and around the network and take their warnings, that is golden. And between people, like what happened in Night Dragon, we want to be able to share that, and we need the protections to do so.

The key here is the small to medium businesses that were mentioned earlier, over 99 percent of our business fabric, many of those in the energy sector. We are missing not only not being able to protect them—they are probably building the next-gen engine—but we are missing the information we get from that entire piece of the global business sector by not getting that information back in, and that partnership with NIST and with Homeland Security exemplifies the importance of global standards to do this. And I want to highlight the financial community, the financial sector, who has gone out and worked with NIST and DHS to build those global standards to be able to share, no matter what product you have to be able to share mathematical indicators, preserving civil liberties and just doing math on what might be dangerous coming toward you.

How do we do this? With positive incentives. First off, driving by innovation. That whitelisting technology, our customers begged for that in the CIP requirements but it was mandated that they only use blacklisting, so for compliance so they wouldn't get penalized, they used a weaker form and were not as secure. Now 2 years later, because regulation moves so slowly, we are finally looking at getting whitelisting in there as an acceptable form of "compliance."

The other piece: liability protections. Help us share. There is so much information we want to share, per previous testimony, be able to get information from the government, give information to the government and provide again that privacy, that civil liberties that makes our country so unique. We have to be able to do all this and we have to be able to get it right. This is the agility and the alacrity that today is only enjoyed by the cyber adversary. Today at 320 gigs per second on the finest routing equipment in the world, bad people are sending bad things to good infrastructure. This is our danger to the energy infrastructure. You could risk intellectual property theft. You could risk credential harvesting where people pretend to be you and access our infrastructure and effect negative change, and also of course destruction and the things that we see in the movies. Insurance provisions, tax provisions, all these other positive incentives help us drive the innovation to put our information together and to improve technology as fast as the adversary does to us.

Thank you very much for requesting McAfee's views on these issues. I am happy to answer any questions.

[The prepared statement of Ms. Schneck follows:]

Summary of McAfee's Dr. Phyllis Schneck's Statement, May 21, 2013
Cyber Threats and Security Solutions – Energy and Commerce Committee

McAfee, an Intel company, works with many companies in the energy sector and does indeed have perspectives on the sector's threat environment. Energy is the infrastructure of infrastructures in that it supports so many others. At the same time, cyber is becoming the nexus and enabler of critical infrastructures, as more systems make use of the Internet, which puts the "smart" in smart grid, for example. This, of course, also opens up vulnerabilities.

Cyber bad actors are increasingly targeting energy, as incidents like Stuxnet and an apparent successor, Duqu, illustrate. Attacks on energy companies can be subtler than seeking to destroy physical facilities; they can be targeted toward gaining sensitive IP (a type of cyber espionage), or they can be extortion (80% of power companies in Mexico, 60% in India say this is most common cyberthreat).

Attempts to modernize energy distribution, say in the U.S., have brought together once separate domains – the equipment itself, the system control and data acquisition (SCADA) and the provider's IT network. If any one of those domains is connected to the Internet, they can receive malicious code from the Internet.
You don't have to attack with cyber directly, either, as the recent bank heists show. There humans hacked a database to get credentials (usernames/passwords), then used those to create fake bank cards and rob the ATMs. The cyber event was the initial database intrusion; the rest was done by humans.

Because of its vulnerability, the energy sector is regulated regarding cyber security. The problem is that sometimes that regulation is overly specific about a technology and ends up hindering rather than helping companies to be optimally secure. We urge the adoption of a faster review process, possibly an annual review of rules, and we also urge that regulations be outcome-based. For sectors not already regulated, we urge information sharing, innovation, and positive incentives.

Sharing real-time information about malicious codes between the government and private sector can make a real difference in our ability to thwart bad actors. But many in the private sector hesitate to share information because of concerns about liability. The Rogers/Ruppersberger bill, or something like it, would fix this and better enable public-private partnerships that NIST and DHS have already started. We hope sufficient privacy protections will help cement the broad coalition needed to make this bill law.

Innovation, such as treating networks as smart, adaptive ecosystems that both produce and consume intelligence about threats, is also key. McAfee calls this concept Security Connected – an open, dynamic, adaptable yet connected security platform. Positive incentives include tax incentives, liability protections for companies sharing information, insurance reforms, and R&D initiatives.

STATEMENT OF DR. PHYLLIS SCHNECK, VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, GLOBAL PUBLIC SECTOR

McAFEE, INC.

BEFORE:

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON ENERGY AND COMMERCE

"CYBER THREATS AND SECURITY SOLUTIONS"

MAY 21, 2013

Good morning Chairman Upton, Ranking Member Waxman, and other members of the Committee. I am Phyllis Schneck, Vice President and Chief Technology Officer, Global Public Sector for McAfee, Inc., a subsidiary of Intel Corporation. We appreciate the Committee's interest in cyber security threats and solutions, particularly as they affect critical infrastructures.

My testimony will focus on the following areas:

- The threat landscape for the energy sector
- The particular vulnerabilities of the energy sector
- The liabilities of regulation for cyber security in the energy and other critical infrastructures
- Security solutions: information sharing, innovation, and positive incentives

First I would like to provide some background on my experience and on McAfee.

I have dedicated my entire professional career to the security and infrastructure protection community. My technical background is in high performance computing and cryptography. In addition to my role with McAfee, I serve as Chairman of the Board of Directors of the National Cyber Forensics and Training Alliance (NCFTA), a partnership between government, law enforcement, and the private sector for information analytics that has been used to prosecute over 400 cyber criminals worldwide.

Earlier, I worked as Vice President of Threat Intelligence at McAfee and was responsible for the design and application of McAfee's™ Internet reputation intelligence. I am the Vice Chair of the Information Security and Privacy Advisory Board (ISPAB) and have also served as a commissioner and working group co-chair on the public-private partnership for the Center for Strategic and International Studies (CSIS) Commission to Advise the 44th President on Cyber Security.

Additionally, I served for eight years as chairman of the National Board of Directors of the FBI's InfraGard™ program and as founding president of InfraGard Atlanta, growing the InfraGard program from 2000 to over 33,000 members nationwide. Prior to joining McAfee, I was Vice President of Research Integration at Secure Computing. I hold a Ph.D. in Computer Science from Georgia Tech, where I pioneered the field of information security and security-based high-performance computing.

McAfee's Role in Cyber Security

McAfee protects businesses, consumers and the public sector from cyber-attacks, viruses, and a wide range of online security threats. Headquartered in Santa Clara, California, and Plano, Texas, McAfee is the world's largest dedicated security technology company and is a proven force in combating the world's toughest security challenges. McAfee is a wholly owned subsidiary of Intel Corporation.

McAfee delivers proactive and proven solutions, services, and global threat intelligence that help secure systems and networks around the world, allowing users to safely connect to the Internet and browse and shop the web more securely. Fueled by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

To help organizations take full advantage of their security infrastructure, McAfee launched the Security Innovation Alliance, which allows organizations to benefit from the most innovative security technologies from thousands of developers, who can now snap into our extensible management platform. Today, more than 160 technology partners—large and small businesses all committed to continuous innovation in security—have joined the alliance, with more to be announced soon.

Threat Landscape for the Energy Sector

It's hard to overstate the importance of securing the nation's power grid – a grid on which so many other of our critical infrastructures depend. The energy sector feeds water, agriculture, transportation, finance, communications, information technology, the military and homeland security, not to mention healthcare and education. It's no exaggeration to call energy the infrastructure of infrastructures.

At the same time, cyber is becoming the nexus and enabler of critical infrastructures -- especially energy – as more and more systems make use of the Internet. Cyber puts the "smart" in smart grid, for example. The problem is that the very thing that makes the grid smart—the ability of myriad embedded systems to communicate with each other, often using a combination of legacy and proprietary equipment alongside more modern

solutions—has expanded the attack surface, making it vulnerable to cyberthreats. Open systems invite hacking.

Attacks on the Energy Infrastructure are Growing

The story of Stuxnet is like that of a sensational crime that generates a flurry of media attention and speculation when it happens, but eventually fades from the news even though the mystery remains unsolved. The Stuxnet worm first came to the public's attention in 2010, when it attacked several facilities around the world, including Iran's nuclear enrichment infrastructure, taking control of programmable logic controllers that control the automation of mechanical processes and disrupting centrifuges and turbines.

Since then, more advanced variants of the malware have been reported in various places globally. In a 2010 survey on critical infrastructure security by McAfee and the Center for Strategic and International Studies (CSIS), nearly half of the respondents from the energy sector said they had found Stuxnet on their systems. Stuxnet has one intent: sabotage.

More recently, an apparent descendant of Stuxnet called Duqu has been reported in energy facilities in at least eight countries. Perhaps authored by the creators of Stuxnet, or at least using the older worm's source code, Duqu has not been used in any actual attacks to date – although it is capable of doing damage – but rather appears to be probing for sensitive information and weaknesses that could be exploited in future attacks.

While the physical destruction of facilities, with potentially deadly consequences, is a genuine concern, many cyberthreats are subtler in intent, seeking to gain sensitive intellectual property (a type of espionage) or to commit extortion. In fact, extortion is the most prevalent cyberthreat reported by the global energy sector. In the McAfee/CSIS study noted earlier, one in four power companies globally said they had been victims of extortion. In some countries, the incidence is alarmingly high: 80 percent in Mexico, for example, and 60 percent in India.

One of the challenges in confronting cyberthreats to the energy sector is that they take many forms, have disparate goals, and originate with a variety of sources, making it difficult to know which systems are at risk, which require protection, at what level, and at what cost.

Vulnerabilities of Energy Systems

The increased vulnerability of the energy sector is due, ironically, to well-intentioned efforts to modernize energy distribution. Energy system operators have historically been concerned with three technology domains: the industrial control systems (ICS) that run turbines, generators and other heavy-duty equipment; the system control and data acquisition, or SCADA, systems that oversee the ICS. SCADA systems don't actually run equipment but enable operational teams to monitor and manage the ICS through consoles known as "human-machine interfaces," or HMI. The third domain is the provider's organizational IT network—its internal databases and business applications.

In the past, these three domains operated separately, which of course was inefficient. As companies became more networked, they began automating the delivery of data across domains – which is useful but also means that an intruder could gain access to all three domains by entering just one of them. Add to this the fact that 70% of the energy grid is more than 30 years old, and the fact that workers can now reprogram systems through their smartphones – meaning the Internet – and you have quite a few points of vulnerability.

One area of vulnerability is in systems that are connected to the Internet and that also connect to non-cyber components. In this situation malicious instructions from the Internet can initiate actions on machines that connect to physical/kinetic infrastructure. This vulnerability occurs in systems where the monitoring systems connect to the physical systems via the Internet for remote access, efficiency and convenience.

Another area of vulnerability is, of course, from destructive malware: malicious instructions being introduced to a network via Internet files, USB drives, or other access. The malware itself can cause mass outages.

It's also worth noting that the threat landscape is not limited to cyber intrusions per se; people can use cyber tools to do the damage themselves. Witness the recent bank heists via ATMs. In this case, people hacked a database to harvest credentials, getting access to usernames and passwords so they could then get access to physical systems. The "cyber event" was a database intrusion, and the actions that followed were carried out by people. Just as people used fake ATM cards to rob the AT machines, people could also use illegally obtained credentials to cause harm to energy infrastructure that is controlled by computer access.

The Path Forward: Existing Regulation Must Become More Flexible

The good news is that both government and industry are well aware of these vulnerabilities and realize how important it is to protect the grid. The energy sector is highly regulated regarding cyber security, and operators must meet certain prescribed critical infrastructure protection (CIP) requirements. On the face of it, having CIP requirements sounds helpful. In practice, however, the regulatory process gets in the way of what started out as a good idea, making it, in practice, not helpful and maybe even harmful. McAfee has firsthand experience with this situation.

Two years ago some of our large energy customers came to us saying that that one of the CIP requirements seemed to mandate anti-virus protection to the exclusion of other, more modern, types of defenses. A/V is based on the concept of blacklisting, which creates a static list of what code will not be allowed into a system. In a dynamic threat landscape, however, the black list loses its accuracy in milliseconds. It both includes innocents and fails to block some recently turned bad actors. Blacklisting leads to a false positive rate and lack of detection that is not conducive to cyber security or network performance.

Whitelisting, on the other hand, fixes the false positive issues and allows for the fact that the adversary will penetrate any security walls we try to build. In concept, a "white list" is a list of *always accepted* actors, excluding other attempted entrants, thus eliminating the need to know if they cause harm. This can apply to IP addresses at the network layer or, as McAfee has implemented it for critical infrastructure, instructions at the kernel level of the operating system. This latter case is a nice fit for components with well-defined functionality that can be bounded with a white list approach, such as electric meters, other critical infrastructure components or ATM machines. There is a finite set of instructions that should ever run on such devices. Those instructions are on a "white list," and nothing else is permitted to execute on those devices, even if it penetrates the other security and enters the device. The instruction itself is worthless if it is not whitelisted.

Returning to the regulatory situation, once our customers pointed it out, we noticed that the CIP requirement did indeed seem to mandate A/V, or blacklisting. This meant that if an operator were to implement whitelisting, they could be in violation of the rule. The operator could file for a Technical Feasibility Exception, but absent that they would be faced with a violation. They were thus forced between being compliant and being secure – exactly the wrong result in the view of both government and industry. We brought this situation to the attention of energy regulators, who sympathized with the concern. However, getting the language changed would have required a process in which none of our customers cared to engage, so the rule still stands.

Now, a year and a half later, that old rule is due to be supplanted by a new rule that is technology-neutral and does not present a problem. That new rule is just in the comment phase, however, and will most likely not become effective until 2015. In this case the regulatory process, while well intended, is slow, cumbersome and – worst of all – dangerous, leaving a critical infrastructure without the latest cyber security technology.

Contrast this to our cyber enemies, who innovate swiftly and execute at the speed of light. By the time this rule is changed, our enemies will have moved onto something different. Innovation from the private sector can move along swiftly as well – if the regulatory process allows it.

For sectors such as energy, which are subject to cyber regulation, we urge the adoption of a faster review process, possibly an annual review of the rules. Any standard should be oriented towards outcomes rather than being prescriptive. The aim should be to give affected industries the ability to mix and match technologies to achieve the outcomes sought by regulators. Such an approach would also help promote security – and resilience – in situations where firms within an industry are different and have different organizational and security challenges.

For sectors that are not regulated, we believe that information sharing, industry innovation and positive incentives are what's needed.

Security Solutions

Information Sharing

Information sharing between the government and the private sector – and between private sector entities themselves – can be a powerful tool to thwart cyber adversaries. We commend NIST and DHS for the information sharing efforts they have initiated and fully support that processes each has begun. By information I mean not just general facts about threats but real-time malicious code that's being observed in systems around the world that can be shared instantaneously with global experts so that people and systems can act upon that information immediately. The financial services sector is particularly good at doing this through the FS Information Sharing and Analysis Center (ISAC), and other sectors have set up ISACs as well. But the information sharing process is not nearly as robust as it could be, mainly because private entities know they could incur liabilities.

The Rogers/Ruppersberger Bill

During the last Congress and again this year, your colleague on this committee, House Intelligence Committee Chairman Mike Rogers (R-Michigan), along with his Ranking Member Dutch Ruppersberger (D-Maryland), introduced the *Cyber Intelligence Sharing and Protection Act*, or CISPA. The House has once again passed the bill.

CISPA gives the federal government new authority to share classified cyber threat information with approved companies so they can better protect themselves and their customers from cyber attacks. The bill also empowers participating businesses to share cyber threat information with others in the private sector and enables the private sector to voluntarily share information with the government.

The reason this is so important is that leading information technology companies, security providers and their customers are uniquely positioned to act as early warning systems that can identify and help address attacks on a real time basis, including APTs, botnets and other incursions. But under current law these private sector actors can't share the information needed to effectively combat these threats. Better enabling information sharing, including liability protections for private entities sharing cyber threat information in good faith, will help the private sector execute with the alacrity shown by our cyber adversaries and will enhance the public-private partnership that is so vital to meeting the cyber security challenge.

Ensuring that sufficient privacy protections are part of any information-sharing bill will help cement the broad consensus necessary to enact this proposal. Although the privacy and civil liberties improvements in the version of CISPA the House recently passed are significant, we would urge the sponsors to continue the ongoing dialogue with the privacy and civil liberties communities to address any remaining legitimate policy concerns.

Security Solutions – Innovation

The private sector is embracing innovation to constantly improve our capabilities to be resilient and challenge ourselves across industry, government, and owners of critical infrastructure. This is how we plan to win back the agility now enjoyed by the adversary. As mentioned earlier NIST is enabling innovation through partnerships with industry, and we applaud their efforts.

At McAfee we believe in a connected, adaptable, open and dynamic security platform to guide security decisions made by machines and people. We emphasize the importance of every network component being both a producer and consumer of intelligence. This intelligence can then be shared within the network and externally (as allowed by policy) to enable an adaptive, learning ecosystem that gets smarter as it protects.

This ecosystem concept is well described in the white paper from the National Protection and Programs Directorate within the Department of Homeland Security. Done correctly, networks can detect behaviors over time and begin to recognize, almost biologically, threats before those threats can overtake network functionality. Maturity models have shown that for any size organization, a wise design up-front leads to increasing security and decreasing cost over time. This ecosystem model would work well for the energy sector

We call this dynamic, comprehensive and open platform Security Connected.
Such a platform can enable any entity, any product, any utility, and any company small or large, to become part of a greater system where the detection of a threat on the Internet is used as protection going forward – at the speed of light. This is the agility our adversaries cannot achieve.

Security Solutions – Positive Incentives

As a front-line organization on cyber security, we know that innovation and cooperation between government and industry is vital. And the best way to get cooperation is with positive incentives, not more regulations. Congress must provide the necessary tools and assurances we need to lock down our nation's critical infrastructures. Steps that can be taken now include:

- Establishing cybersecurity as a national priority with funding for research and development, scholarships, competitions and other incentives to create a new generation of cybersecurity career professionals.

- Tax incentives to encourage businesses to invest in cyberdefense, including accelerated depreciation schedules or tax credits for adopting proven security technologies.

- Liability protections for companies that share information about malicious network intrusions with the government. Right now, liability fears can suppress timely sharing of vital threat data. Liability protections should also be available

for companies that use vetted technologies and services to protect themselves from cyber attacks. No legislation is needed to achieve this goal – simply encouraging the Department of Homeland Security to take the lead use its existing authority under the *SAFETY Act*, which provides liability protections to sellers and users of DHS reviewed and approved cyber security tools.

- Insurance reforms: Government could enhance the insurance market by providing it with a backstop program. To that end, Congress should consider extending the reach of the *Terrorism Reinsurance Program Reauthorization Act* (or TRIPRA) to include cyber attacks.

Thank you for requesting McAfee's views on these important issues. I am happy to answer any questions.

Mrs. BLACKBURN. Thank you.
Mr. Blauner for 5 minutes.

STATEMENT OF CHARLES BLAUNER

Mr. BLAUNER. Chairman Blackburn, Ranking Members, members of the committee, my name is Charles Blauner. I am the Global Head of Information Security for Citi, and I set the information security strategy for Citi. I am accountable for the information security risk posture across all of our lines of businesses, functions and regions. In addition, I serve as the Chairman of the Financial Service Sector Coordinating Council, also known as FSSCC, which coordinates protection of critical financial services infrastructure focusing on operational risks. I appreciate the opportunity to be here today to testify on behalf of the ABA.

I would like to begin by commending the House for its recent passage of the Cyber Intelligence Sharing and Protection Act. This legislation, if enacted, will greatly facilitate information sharing regarding the serious threats to our Nation's critical infrastructures. We are also supportive of the Administration's Executive order, which provides important direction to both the public and private sector to enhance our Nation's cybersecurity protections.

There are three key points I would like to highlight today. First, the public and private partnership between government and the financial services sector is critical to protecting firms against cyber threats, and we pledge to continue this collaboration to further our mutual goals. The most recent example of our collaboration is a unified response to the cyber attacks that have targeted the U.S. financial services sector since September 2012. This partnership, facilitated by the FS–ISAC, or the Financial Services Information Sharing and Analysis Center, allows for real-time collaboration on measures to mitigate the attacks and provides a forum to request and acquire specific governmental technical assistance.

Second, the ABA believes that the development and implementation of the NIST cybersecurity framework should leverage existing standards, regulations or processes. Financial institutions are already subject to significant federal and state law and regulations that emanate from the Gramm-Leach-Bliley Act of 1999. These requirements are substantially similar to those developed by NIST, and it is extremely important that the implementation of the NIST cybersecurity framework be leveraged and complementary to the existing audit and examination process. Otherwise we will end up with redundant audit requirements that become a compliance exercise and do absolutely nothing to enhance cybersecurity.

Third, the ABA also believes that timely cross-sector information sharing is key to cybersecurity protection. While the existing mechanisms play a vital role in incident response coordination, improving and encouraging information sharing is essential to protecting the financial services sector and the Nation. It is of utmost importance to increase the volume, timeliness and quality of threat information shared by federal agencies, law enforcement and the U.S. intelligence community with the private sector so they may better protect themselves against cyber threats. Thus, we need our government partners to expedite the processing of security clearances and to declassify and more broadly disseminate threat information

critical to enhancing our Nation's ability to protect itself from cyber threats.

It is important to note that a key factor in the success of information sharing is trust, which takes years to develop. The ABA, the FS–ISAC and FSSCC have worked hard to develop trust between its members and public and private sector partners. We can't afford to dismantle that trust, and we will continue to develop trust and confidence now sharing efforts.

The ABA also believes that foundational work needs to be done to share our goal of enhanced cybersecurity. The development of technical capabilities relies on robust research and development that can quickly yield new commercial products to protect individual firms and critical shared infrastructure. I would also like to note that these efforts, often supported by the resources of banks like Citi and other large financial firms, help create tools and defenses that help banks of all size cope with cyber threats. Beyond technical capabilities, the demand for skilled resources outstrips supply today. A coordinated effort is required to develop a skilled worker force as up to the task of defending us against today's and tomorrow's cyber threats.

In conclusion, cybersecurity is top priority for banks and other financial services companies. We have invested an enormous amount of time, energy, and resource into placing the highest level of security, and we are subject to stringent regulatory requirements. We also look forward to continuing to work with Congress and the Administration towards our mutual goal of protecting our Nation's critical infrastructure.

Thank you, and I would be happy to answer any questions you might have.

[The prepared statement of Mr. Blauner follows:]

May 21, 2013

Testimony of

Charles Blauner

On behalf of the

American Bankers Association

before the

Energy and Commerce Committee

of the

United States House of Representatives

Testimony of Charles Blauner

On behalf of the

American Bankers Association

before the

Committee on Energy and Commerce

of the

United States House of Representatives

May 21, 2013

Chairman Upton, Ranking Member Waxman, my name is Charles Blauner, Global Head of Information Security for Citi. In that capacity, I set Citi's information security strategy and am accountable for Citi's information security risk posture across all lines of business, functions, and regions. I appreciate the opportunity to be here today representing the American Bankers Association (ABA), which represents banks of all sizes and charters and is the voice for the nation's $14 trillion banking industry and its two million employees.

I would like to begin by commending the House for its recent passage of the Cyber Intelligence Sharing and Protection Act (CISPA). This legislation, if enacted, will greatly facilitate information sharing regarding the serious threats to our nation's critical infrastructures. We are also supportive of the Administration's executive order, which provides important direction to both the public and private sector, and like CISPA aims to enhance our nation's cybersecurity protections.

In addition to my role at Citi I am proud to currently serve as the Chairman of the Financial Services Sector Coordinating Council (FSSCC), which is the coordinator for Financial Services for the protection of critical infrastructure, focused on operational risks. Citi is extremely supportive of the FSSCC and its sister organization, the Financial Service Information Sharing and Analysis Center (FS-ISAC). ABA has also been deeply involved in these two organizations since their inception, and will be represented as the Vice Chair of the FSSCC starting in July of this year while continuing to serve on the FS-ISAC board. Companies and associations taking on these roles are but one example of the high level of collaboration within our sector when it comes to cybersecurity.

Cybersecurity is a top priority for banks and other financial services companies. We have invested an enormous amount of time, energy and resources to put in place the highest level of security among critical sectors, and we are subject to the most stringent regulatory requirements.

The public-private partnership has been critical to protecting firms in our industry against cyber threats and we pledge to continue this collaboration to further our mutual goals.

My testimony today focuses on four key points:

- How the organization and regulation of the financial services sector bolsters cybersecurity and reduces the risks associated with cyber attacks;
- How the development and implementation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework should leverage existing standards, regulations, and processes;
- How timely cross-sector public-private information sharing is the key to cybersecurity protection; and lastly,
- What foundational work needs to be done to support our shared goal of enhanced cybersecurity.

I. The Organization and Regulation of the Financial Services Sector Bolsters Cybersecurity

As Congress and the Administration contemplate changes to the national cybersecurity framework, it is important to consider the cybersecurity measures collaboratively taken by our sector, through the operations of the FSSCC and the FS-ISAC—the private side of our sector—in conjunction with the Financial and Banking Information Infrastructure Committee (FBIIC)—the public side. Also important are the stringent laws and regulations within the financial services sector. This, along with our longstanding working relationship with the U.S. Department of the Treasury (our sector-specific agency regarding critical infrastructure protection) has been very effective.

Let me briefly describe the key components of the public-private partnership.

Financial Services Sector Coordinating Council: FSSCC's mission is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure. The Council has 55 volunteer member associations and financial institutions representing clearinghouses, commercial banks, credit rating agencies, exchanges/electronic communication

networks, financial advisory services, insurance companies, financial utilities, government-sponsored enterprises, investment banks, merchants, retail banks, and electronic payment firms.[1] During the past decade the partnership has continued to grow, both in terms of the size and commitment of its membership as well as the breadth of issues it addresses. Members commit their time and resources to FSSCC with a sense of responsibility to their individual firms and for the benefit of financial consumers and the nation. At a sector level, FSSCC's role is focused on strategy and policy.

Financial Service Information Sharing and Analysis Center: The FS-ISAC was established by the financial services sector in response to the Presidential Directive 63 of 1998. That directive—later updated by the Homeland Security Presidential Directive 7 in 2003—mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure. Constantly gathering reliable and timely information from financial services providers, commercial security firms, federal, state and local government agencies, law enforcement and other trusted resources, the FS-ISAC is positioned to quickly disseminate physical and cyber threat alerts and other critical information throughout the financial sector. Compared to the FSSCC, the FS-ISAC's primary role is operational.

Financial and Banking Information Infrastructure Committee: FBIIC, led by Treasury and chartered under the President's Working Group on Financial Markets, is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. Essential to the FSSCC's success is the public sector's commitment to the public-private sector partnership outside of the already mature regulatory regime.

The deep involvement of ABA and Citi in both the FSSCC and the FS-ISAC is not unusual within the financial services sector. Many financial organizations are heavily involved in both. ABA, which represents banks of all sizes and types, has been a primary driver behind expanding the FS-ISAC's reach from under 100 in 2004, to over 4,000 member firms today to ensure that vital cyber threat information and the means to manage those threats reaches as many financial organizations as possible.

---

[1] A listing of FSSCC members is contained in Appendix 1.

The financial services sector develops and implements leading practices through the FSSCC, the FS-ISAC and the FBIIC. For example, under the joint partnership of the FSSCC and FBIIC, our sector has developed leading practices to assess and mitigate risks associated with the resiliency of the telecommunications infrastructure including critical undersea cables, pandemic flu preparations, and other important risks or threats facing the security and resilience of the sector.

The most recent example of the high degree of interaction and collaboration between these bodies is our sector's unified response to cyber attacks that have targeted the U.S. financial services sector since September, 2012. These attacks, against an increasing number of financial organizations, have at times impacted availability of consumer internet banking websites. From the very start of these attacks, the FS-ISAC was able to organize the affected organizations into a group to collaborate in real-time on measures to mitigate the attacks. Individual organizations were able to, through FBIIC and Treasury, request specific governmental technical assistance as necessary. Due to the tight relationship between the FS-ISAC and the FSSCC, actions such as these are factored into the actions taken by the FSSCC as the Council makes and refines legislative and administrative policy recommendations.

While the financial services sector is effectively organized for critical infrastructure protection purposes, the sector is also subject to federal and state laws, regulations, guidance, and examination standards relating to cybersecurity, many of which emanate from the general financial safety and soundness standards and customer information security provisions contained within the Gramm-Leach-Bliley Act of 1999. For example, financial institutions must comply with guidance produced by the Federal Financial Institution Examination Council (FFIEC), an organization made up of the agency heads of all the depository institution regulators. This guidance sets the standards for financial institution's information systems, outlining the minimum control requirements and directing a layered approach to managing information risks.

Likewise, the Securities and Exchange Commission (SEC) and the self-regulatory organizations (SROs), such as the Municipal Securities Rulemaking Board (MSRB), the Financial Industry Regulatory Authority (FINRA), and the National Futures Association (NFA), review the cybersecurity programs of exchanges, broker-dealers and clearing organizations as part of their ongoing supervisory exams and related activities. Insurance companies' privacy and security programs are subject to review by state insurance regulators. Health and long-term care insurers'

privacy and security programs also are subject to review by the Department of Health and Human Services (HHS).

As I will discuss in greater detail later in this statement, and as a recent GAO report outlines, financial sector regulations, guidance, and examination standards are substantially similar to the National Institute of Standards and Technology (NIST) Special Publication 800-53, mapping essentially to all of the recommended controls for federal information systems.[2] ***This is an extremely important point, as a key FSSCC recommendation regarding implementation of the NIST Cybersecurity Framework is that existing audit and examination processes be leveraged and complementary, and not have redundant audit requirements.***

II. Development and Implementation of the NIST Cybersecurity Framework Should Leverage Existing Standards, Regulations, and Processes

ABA continues to support the efforts of the Administration and Congress to limit cybersecurity threats to business, our government, and the American people through a more integrated approach.[3] We applaud the release of the Executive Order and believe implementation of the Cybersecurity Framework envisioned in the Order can be an important tool in improving our nation's overall cybersecurity.

NIST has said that, in conducting its work, it will consider integration of standards with existing frameworks. To this end, ***ABA believes it is particularly important that NIST's efforts to develop a Cybersecurity Framework complement and build upon existing cybersecurity standards adopted by the U.S. financial services industry.*** As already noted, the financial sector's critical infrastructure is subject to a significant number of federal and state laws, regulations, guidance, and examination standards relating to cybersecurity. We also agree with NIST that an important objective of its efforts should be to encourage widespread adoption of the Cybersecurity Framework across critical industries, as the financial industry's cybersecurity is contingent on the safety and security of other critical sectors, such as telecommunications and energy.

---

[2] GAO, *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use*, GAO-12-92 (Washington, D.C.: December 9, 2011).

[3] The FSSCC Comment Letter in Response to the NIST Request for Information, "Developing a Framework to Improve Infrastructure Cybersecurity" is available here: http://csrc.nist.gov/cyberframework/rfi_comments/040813_fsscc.pdf.

Collaboratively, through the FSSCC, ABA is committed to working with NIST in formulating and implementing this Framework and offers the following recommendations to improve cybersecurity to meet our mutual goals:

- **Develop sector-specific frameworks for protecting critical infrastructure.** Instituting a centralized Cybersecurity Framework would not be effective in recognizing the unique nature of and levels of protection within each critical sector. We strongly recommend that each Sector Coordinating Council take the lead in developing a framework that is specific to that sector so that critical infrastructure can be identified in a manner that is repeatable, transparent, and predictable.
- **Leverage primary regulatory authorities.** Any Cybersecurity Framework should ensure that each sector's primary regulatory authorities remain independent as the overseer and enforcement body for the critical sectors they regulate. This is necessary to ensure that the business continuity, resiliency, and critical infrastructure protection regulations that primary regulators enforce form the basis of any critical infrastructure protection standards imposed on that sector.
- **Leverage existing audit and examination processes and, encourage complementary, not redundant audit requirements when building voluntary cybersecurity practices.** Any Cybersecurity Framework should recognize that financial sector critical infrastructure firms already undergo extensive audits both internally and by third parties, of existing cybersecurity standards. We have, and continue to recommend, that any voluntary practices be consistent with existing financial sector regulatory requirements. In particular, implementation of the Framework should not require additional third party audits in order for a company to be eligible for any incentives where existing audit and regulatory examinations are already in place.
- **Create incentives that are tailored to address specific market gaps.** To the extent that adoption of a Framework may be induced through incentives, such incentives should be tailored to address specific gaps within the market or provide benefits to a sector (or a portion thereof). To be effective they must be compelling enough to affect corporate investment behavior and be adaptable across sectors and business functions, allowing for a menu of incentives and not mandating a one size fits all approach. In addition, the

implementation of the Framework must provide benefits to firms that adopt it by reducing their compliance costs and minimizing the risk of legal action based on its application.[4]

Using the financial services sector as an example, it is widely acknowledged that the sector's existing regulatory requirements will ***exceed*** the baseline cybersecurity standards that NIST will ultimately recommend for the Framework. If the primary federal financial regulatory agencies come to this determination, as the Executive Order specifies, how can that determination be leveraged as part of or in lieu of a separate certification process? ***To not leverage the existing regulatory process as part of the certification process risks the development of a compliance exercise rather than a process that actually enhances cybersecurity for the organization.***

III. Timely Cross-Sector Information Sharing Throughout the Public-Private Partnership is Key to Cybersecurity Protection

As I have outlined, the financial services sector currently shares a significant level of threat data between institutions and across the sector through the FS-ISAC. We believe that existing information sharing and analysis mechanisms, such as those provided by the FS-ISAC, play a vital role in incident response coordination, information sharing and other operational activities for the financial services sector. Improving and encouraging information sharing is central to protecting the financial services sector and the nation.

A key factor in the success of information sharing in the financial services sector is trust. And trust takes time to develop. The ABA, FS-ISAC and FSSCC have worked hard to facilitate development of trust between its members, with other organizations in the financial services sector, with other sectors, and with government organizations such as law enforcement, regulators, and intelligence agencies for over a decade. Trust cannot be legislated, trust must be earned and we cannot afford to do anything that damages the levels of trust that have already been established.

It is of utmost importance to increase the volume, timeliness, and quality of threat information shared by U.S. law enforcement and intelligence agencies with private sector entities so that they may better protect themselves against cyber threats. We also support the intention of CISPA and the Executive Order to improve information sharing between the public and private sectors, and

[4] The FSSCC Comment Letter in response to the Department of Commerce's Notice of Inquiry: Incentives to Adopt Improved Cybersecurity Practices, is available here: http://www.ntia.doc.gov/files/ntia/fssec_response_-_doc_noi.pdf.

especially the ability to more rapidly disseminate classified reports to entities authorized to receive them. We need our Government partners to expedite the processing of security clearances, and to declassify and more broadly disseminate threat information critical to enhancing our nation's ability to protect itself from cyber threats.

In June 2011, the FS-ISAC became the third ISAC to participate in the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC). FS-ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, attend daily briefs and meetings to share information on threats and vulnerabilities. The presence at the NCCIC has greatly enhanced situational awareness and information sharing between the financial services sector and the government.

Again, ABA commends the House for passing the Cyber Intelligence Sharing and Protection Act. The timely, voluntary sharing of threat information is critical to the government and the private sector in developing and deploying protective measures and countermeasures against malicious cyber activity. While the cyber threat data that is shared by the financial services sector is machine language and not attributable to an individual, the provisions in the bill concerning liability protections for the sharing of information are extremely important and transcend our sector. This legislation provides important clarifications that will help facilitate increased cyber intelligence information sharing between the private and public sectors. We hope that this important piece of legislation will be signed into law.

IV. Foundational Work Needs to be Done to Support our Shared Goal of Enhanced Cybersecurity

Protecting our nation's critical infrastructure, including the Financial Services Sector, from the rapidly evolving cyber threat requires the ongoing development of technical capabilities and skilled resources which do not exist today.

The development of technical capabilities relies on a robust program of Research and Development (R&D) that can quickly yield new commercial products that can be leveraged to protect individual firms as well as critical shared infrastructure. To support this goal the FSSCC has published an "R&D Agenda" to help guide research sponsored by governmental agencies as well as universities and the private sector.

Beyond technical capabilities, another critical success factor is the availability of skilled resources. Simply put, demand for those resources outstrips supply today. In order to successfully meet the challenges posed, a coordinated effort is required to develop a skilled workforce that is up to the task of defending our nation and the Financial Services Sector from today's and tomorrow's cyber threats.

V. Conclusion

Cybersecurity is a top priority for banks and other financial services companies. We have invested an enormous amount of time, energy and resources to put in place the highest level of security among critical sectors, and we are subject to stringent regulatory requirements. We look forward to continuing to work with Congress and the Administration toward our mutual goal of protecting our nation's critical infrastructure.

Appendix One

Financial Services Sector Coordinating Council Membership

The Financial Services Sector Coordinating Council (FSSCC) fosters and facilitates financial services sector-wide activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security. The Council was created in June 2002 by the private sector, with recognition from the U.S. Treasury, to coordinate critical infrastructure and homeland security activities in the financial services industry.

Associations	Operators	Utilities and Exchanges
American Bankers Association	Allstate	BATS Exchange
American Council Life Insurers	Bank of America	CLS Services
American Insurance Association	BNY Mellon	CME Group
ASIS International	Citi	Direct Edge
BAI	Equifax	DTCC
	Fannie Mae	Intercontinental Exchange
BITS	Fidelity Investments	International Securities Exchange
ChicagoFIRST	Freddie Mac	NASDAQ
Consumer Bankers Associations	Goldman Sachs	National Stock Exchange
Credit Union National Association	JPMorgan Chase	NYSE Euronext
Financial Information Forum	MasterCard	Omgeo
FS-ISAC	Morgan Stanley	Options Clearing Corporation
Futures Industry Association	Navy Federal	The Clearing House
Independent Community Bankers Association	Northern Trust	
Investment Company Institute	PayPal	
	RBS	
Managed Funds Association	Sallie Mae	
NACHA	State Farm	
National Association of Federal Credit Unions	State Street	
National Armored Car Association	SunTrust	
National Futures Association		
SIFMA	Visa	
	Wells Fargo	

Mrs. BLACKBURN. We thank you.
Mr. Highley, you are recognized for 5 minutes.

STATEMENT OF DUANE HIGHLEY

Mr. HIGHLEY. Thank you, Madam Chair, Ranking Member and members of the committee. Thank you for the invitation to testify today regarding the electric power sector's work on cybersecurity. I serve as President and CEO of Arkansas Electric Cooperative, which is a nonprofit power supply system serving 17 distribution systems who in turn serve about 1 million Arkansans.

Like other cooperative managers, I report to a democratically elected board representing the customers I serve. Cooperatives work for the members we serve, and that keeps us focused solely on their needs. The electric cooperatives of Arkansas are members of the National Rural Electric Cooperative Association, a service organization for over 900 nonprofit electric utilities serving over 42 million people in 47 states.

Today I am offering testimony on behalf of the Arkansas cooperatives and the NRECA, but I am also sharing information from an overall industry perspective based on my work with the NERC Electric Subsector Coordinating Council and the National Infrastructure Advisory Council.

Whether cooperative, investor-owned or public power, electric providers agree on the need for robust and rapid recovery from natural disasters, physical attacks and cyber attacks. I think I can summarize my testimony in two statements, each 10 words or less. First, NERC has it covered; please don't mess it up. Second, we need to talk.

Now, on the first subject, we appreciate the Energy and Commerce Committee's engagement on this topic. You played a large role in the discussions that led to the creation of the North American Electric Reliability Corporation, or NERC, and its standards regime. Under that regime, the Federal Energy Regulatory Commission can order NERC today without any additional legislation, FERC can order NERC to develop mandatory, enforceable standards on any topic. NERC has developed a number of standards for cybersecurity in electric power systems, and can and does enforce these standards through audits, inspections, and fines. The standards are developed in a collaborative process with all stakeholders, which has resulted in enforceable standards that have improved the reliability of the North American electric grid.

To my knowledge, the electric power sector is the only critical infrastructure sector with such a robust regulatory framework, and I believe that this framework can serve as a model for the other critical infrastructures. The grid is an extremely complex machine, and changes to the way it operates must be carefully coordinated with all stakeholders or reliability will suffer. The NERC standard-setting process provides a platform to vet all potential impacts with input from those who understand the grid the best. Regulations issued without consideration of these impacts run the risk of reducing grid resiliency rather than enhancing it. We have already developed a method that has been proven to work, so in summary, NERC has it covered. Please don't mess it up.

On the second topic, we need to talk, we are glad to see the Executive order's emphasis on information sharing. We have recently begun a top-level dialog between utility CEOs and government, as recommended by the National Infrastructure Advisory Council. We very much appreciate the leadership shown by many members of this committee in developing CISPA and getting it passed overwhelmingly in the House.

This year we have seen some progress in getting security clearances for key personnel in our industry. It is hard to have a partnership when one party can't tell the other what is going on, and our staff must be able to conduct honest conversations with government representatives about the threat environment. While relationships have developed over time, and we do receive useful information through mechanisms such as the ES–ISAC, we still know of instances where government is slow to share information or has developed plans for our industry's response to cyber events but yet has been classified as top secret. So we welcome the continued dialog and hope that the Senate will join in crafting mechanisms and law that will ensure our owners and operators get timely, actionable information. In summary, we need to talk.

Other witnesses have raised the issue of electromagnetic pulse. Utilities can do a lot, but we cannot defend against nuclear strikes from enemy nations or other terrorist organizations. Electromagnetic pulse and its related geomagnetic disturbance from solar storms are very real threats, and FERC has just issued a rule directing NERC to develop standards on geomagnetic disturbances within the next 6 months for phase I and 18 months for phase II, so action is being taken. Experts outside the utility sector often recommended untested technical solutions that really should require detailed analysis and studies before installation to ensure that grid reliability is not harmed. Some even propose technology-specific solutions that could greatly reduce the ability for utilities to use other useful products and solutions. As I said before, the grid is very complex and one-size-fits-all fixes are generally not appropriate and may actually reduce grid reliability. That is why we support the continuance of the NERC standard-setting process. It brings together all stakeholders, including government and industry experts, to design practicable, buildable and cost-effective solutions.

Thank you for the opportunity to testify.

[The prepared statement of Mr. Highley follows:]

National Rural Electric Cooperative Association

A Touchstone Energy® Cooperative

Testimony of Mr. Duane D. Highley

President and CEO of the Electric Cooperatives of Arkansas

to the Committee on Energy and Commerce

U.S. House of Representatives

May 21, 2013

Introduction

Mr. Chairman, Mr. Ranking Member, and all members of the Committee, thank you for inviting me to testify today on the electric power sector's involvement with the ongoing implementation of the Administration's Cybersecurity Executive Order.

The National Rural Electric Cooperative Association (NRECA) is the national service organization dedicated to representing the national interests of cooperative electric utilities and the consumers they serve. NRECA is the national service organization for more than 900 not-for-profit rural electric utilities that provide electric energy to over 42 million people in 47 states or 12 percent of electric customers. Electric cooperative service territory makes up 75 percent of the nation's land mass. Kilowatt-hour sales by rural electric cooperatives account for approximately 11 percent of all electric energy sold in the United States. NRECA members generate approximately 50 percent of the electric energy they sell and purchase the remaining 50 percent.

NRECA members are not-for profit, consumer-owned distribution cooperatives. NRECA's members also include 67 generation and transmission ("G&T") cooperatives, which generate and transmit power to 668 of the 838 distribution cooperatives across the nation. The G&Ts are owned by the distribution cooperatives they serve. The remaining distribution cooperatives receive power directly from other generation sources within the electric utility sector. Both distribution and G&T cooperatives were formed to provide reliable electric service to their owner-members at the lowest reasonable cost.

Because we are owned by the members we serve, distribution cooperatives and G&Ts reflect the values of our membership, and are uniquely focused on providing reliable energy at the lowest reasonable cost. We have to answer to our owners and justify every bit of our expenses to them. There is never any debate as to whether a proposed project will benefit our shareholders or our customers because they are one and the same.

Arkansas Electric Cooperative Corporation (AECC) was created in 1949 and provides power for the more than 500,000 farms, homes and businesses served by our 17 distribution electric cooperative owners. AECC relies on a diverse generation mix, including hydropower, natural gas, coal, and renewables, to serve its members.

Electric cooperatives are dedicated to protecting and securing our electric system assets. We are guided by our obligation to serve and the fact that our consumers are our owners. The Rural Utilities Service (RUS) has long required each electric cooperative borrower to adhere to rigorous construction standards. Beginning in October 2004, RUS Electric System Emergency Restoration Plan (ERP) regulations in 7 CFR Part 1730 required each borrower to perform a vulnerability and risk assessment and to develop emergency recovery plans for physical and cyber incidents. In addition, borrowers are also required to annually exercise their ERP.

Electric cooperatives take cybersecurity risks very seriously and work diligently to understand, mitigate and respond to cyber events. NRECA supports them by working with policymakers and stakeholders to strengthen the public-private partnerships that are an essential component of grid protection. NRECA's Cooperative Research Network (CRN) has been extremely proactive in developing cybersecurity tools targeting distribution utilities (but

applicable to utilities of all sizes) which typically are not subject to NERC standards compliance because their operations do not impact the Bulk Electric System (BES). Since electric cooperatives are at the forefront of smart grid deployment, our members are very much aware of the need to comprehensively address the security of any new telecommunications-enabled devices. As part of its fulfillment of a $68 million smart grid demonstration program under the American Reinvestment and Recovery Act, CRN developed cybersecurity plans for the 23 participating electric cooperatives. That effort led to the development of a tool that compiles thousands of pages of industry and government guidance on cybersecurity into a digestible, deployable plan. It is publicly available at http://www.nreca.coop/bestbets/cybersecurity and anecdotal evidence tells us it is in use at many utilities, including some outside the cooperative network. CRN now leads training open to all segments of the industry on the plan and cybersecurity best practices.

NERC Cybersecurity Mandatory Standards

Electric power sector representatives have participated in each stage of the evolution of the North American Electric Reliability Corporation (NERC), including helping develop Energy Policy Act of 2005 (EPAct '05) amendments to the Federal Power Act which enabled NERC to receive FERC's approval as the Electric Reliability Organization (ERO) in 2006. We appreciate the support and leadership of many members of the Energy and Commerce Committee who contributed to EPAct's reliability provisions. Nearly eight years later, the legislation is working, and should provide a model for other Critical Infrastructure sectors as they work through Executive Order implementation. NERC collaborates with the electric power sector to develop mandatory, enforceable reliability standards that apply to users, owners and operators of the BES.

The NERC reliability standards, 116 in all, include nine devoted to cybersecurity, known as the Critical Infrastructure Protection, or CIP, standards. Electric power sector entities which own or operate BES assets are required to adhere to one or more of the NERC CIP standards. In order to comply, utilities have made significant investments in strategic plans, consultants, hardware, software, training, and teams of full-time employees to ensure compliance and create a culture of security.

The CIP standards and the Nuclear Regulatory Commission (NRC) cybersecurity standards are the only mandatory and enforceable cybersecurity standards in place across the vast array of US critical infrastructures. When covered entities are found to have violated the CIP standards, they can be subjected to fines as high as one million dollars per day per violation. Sizable fines have been levied when entities have been found in violation.

Today, hundreds of electric power sector technical experts are routinely deployed in NERC teams working on the continual process of writing and improving the already-extensive body of NERC reliability standards, including cyber security standards. On January 31, 2013, NERC filed its CIP Version 5 standards with FERC for approval. NERC and the industry are continuing to address FERC directives, National Institute of Standards and Technology (NIST) standards, and other best practices to make sure that the standards evolve with improvements in technology and the ever-changing risks. CIP Version 5 is a comprehensive approach; it addresses all of FERC's directives and implements key elements of NIST cybersecurity

guidelines. On April 18, 2013, FERC issued a Notice of Proposed Rulemaking in which it proposed to approve CIP Version 5.

Given the constantly evolving landscape of cyber risks, the industry recognizes that not every threat or vulnerability can or should be addressed in a standard. To keep up with emerging threats, the industry participates in the Electric Sector-Information Sharing and Analysis Center (ES-ISAC), which is operated by NERC. The ES-ISAC promptly disseminates threat indicators, analyses and warnings from a variety of private sector and government resources to assist electric sector participants in taking protective action. The information is handled confidentially, distributed through NERC's secure portal directly to asset owners and operators.

Perspectives on Executive Order Implementation

Overview of Framework and Potential Intersection with NERC Standards

The electric power sector appreciates the Administration's engagement on cybersecurity as a national security imperative and agrees with the Executive Order's directive that the Cybersecurity Framework "shall provide a prioritized, flexible, repeatable, and performance-based and cost- effective approach." Sec. 7(b). To that end, we believe that the framework must:

(1) Be high-level and flexible, to ensure that the Cybersecurity Framework can be adapted to each of the Nation's diverse critical infrastructure sectors, without unintended consequences;

(2) Build upon each sector's existing processes, standards and guidance, including the sector-specific regulatory standards which already exist in the electric and nuclear industries;[1]

(3) Avoid time-consuming and unnecessary duplication of efforts;[2]

(4) Preserve and build upon existing public-private partnerships;[3] and

(5) Be risk-based and cost-effective.

Among the existing government-industry partnerships we believe NIST should be aware of as it seeks to craft a Framework is the innovative and cooperative approach the electric power sector and the federal government are now pursuing. With both sides committing their expertise and leadership to keep the electric grid as secure and resilient as possible, the sector is working to improve coordination with the government at the most senior levels.

Specifically, a group of CEOs from the investor-owned, public power and cooperative segments of the electric power sector have engaged in what we hope will become an ongoing partnership with senior officials throughout the government, including the White House National

[1] This is consistent with Section 7 of the Executive Order, which directs that the Cybersecurity Framework incorporate existing consensus-based standards and industry best practices to the fullest extent possible.
[2] This is consistent with Sec. 10(c) of the Executive Order which requires agencies to report on duplicative, conflicting or excessively burdensome cybersecurity requirements.
[3] See generally Section 8 of the Executive Order.

Security Staff, Department of Energy (DOE), and Department of Homeland Security (DHS) leadership. This collaboration has resulted in classified briefings to inform senior industry executives of some threats facing the electric grid, as well as a commitment from government representatives to improve the flow of information between the government and industry. Other initiatives for this government-industry partnership include addressing legal, technical, and procedural hurdles associated with the deployment of proprietary government technology on utility networks to improve real-time situational awareness, and a directive to identify roles and responsibilities that will expedite response and recovery should a major power disruption occur.

I would like to emphasize that neither the Executive Order process nor its resulting Framework should be considered a substitute for, or a competitor with, the mandatory standards approved by independent regulatory agencies such as FERC and the NRC. Moreover, any framework must not undermine the existing NERC standards development process, which develops standards that can operate across the North American grid and helps to assure cybersecurity on an international basis. These mandatory standards address public policy objectives that are unique to the electric and nuclear sectors. The Framework should be focused on a much broader task, leveraging the federal government's capabilities and expertise with that of the nation's private sector critical infrastructure owners and operators, to ensure cybersecurity protection and resiliency through rapid sharing and adoption of voluntary standards, guidelines and best practices and close cooperation with our federal government partners.

The Critical Need for Information Sharing and Security Clearances

Information sharing must be a critical component of the Executive Order conversations and eventual Framework. The electric power sector appreciates the support of many members of the Energy and Commerce Committee for H.R. 624, the Cybersecurity Intelligence Sharing and Protection Act. The risks and potential impacts are very different for public-facing elements of a utility's Internet-connected business systems, versus their industrial control systems, which typically are not Internet-connected, or if they are, they are protected with more aggressive security schemes. Given that millions of attempted cyber-attacks occur daily on our public facing sites, utilities will need to rely upon assistance from governmental authorities, particularly in the form of helping to identify threats as well as threat trends.

Much of the information needed to fully understand the nature of the cyber threats faced by our industry is classified at a level that is unavailable to our organizations. The DHS Private Sector Clearance Program (PSCP) has helped key electric utility staff obtain security clearances, which allow them access to basic information about such threats. However, a recent shutdown of the PSCP created a substantial backlog in the processing of clearance applications, and hampered the industry's access to important information. Processing of these applications has now resumed and our hope is that we can continue to expand our ability to access needed information.

In addition to expanding the number of utility personnel with clearances, it is critical that government agencies regularly share clear, actionable information with industry personnel in cleared briefings. Our industry is staffed by dedicated, qualified employees who can be counted on to take the steps necessary to protect our systems – if they understand the nature of the threat against them. There is also a need for a limited number of electric industry personnel to obtain

higher-level clearances than provided by the PSCP, which would allow these individuals to help the government analyze threat information and provide context for the intelligence community.

Effective information sharing should take the form of a timely and efficient mechanism to pass along threat data, warnings, and trend information. Examples of the kinds of information that would be useful to share include: signatures of known viruses and malware; points of origination for known threat actors; known behavioral techniques of anonymous threats such as "Advanced Persistent Threats" (APT); information regarding potential vectors for introduction of cyber threats, such as counterfeit parts and software; and the sharing of best practices or policies to combat or defeat emerging threats and vulnerabilities.

Many federal stakeholders refer to the existing Defense Industrial Base information sharing pilot program as a potential model for the Framework. That program has certainly enjoyed some successes, but there are lessons to be learned there and a careful review of its effectiveness will be critical to ensuring that taxpayer funds are not spent on unnecessarily duplicative or marginally-effective programs.

Liability Protections

Liability protections will also need to be woven into the Framework. Even if current authority does not allow the Administration to extend liability protections, a full discussion of the need for liability protections must be a central part of the Framework discussion so that Congress can fully examine this complex but uniquely important aspect of cybersecurity policy.

Utilities already do their utmost to protect personally identifiable information (PII), but at the same time realize there could be a compelling need to share information that could accidentally include PII. The potential civil liability for the sharing of such information is a significant deterrent, and so we encourage the development of mechanisms that would protect Critical Infrastructure entities from such claims. We also encourage the use of liability protection in the form of shields that protect an entity from claims that it should have acted upon information received. Even with the filtering that is likely to be performed by the government to help narrow the types of information shared to only the most useful, it is still likely to be a monumental task for electric utility employees to determine what information is relevant and actionable. Utility employees should not have to be concerned that despite their best efforts to filter through the shared information, certain actions may or may not be taken that could lead to a cyber-event. Only a liability shield can resolve those concerns.

One mechanism for attaching affirmative legal defenses to the Framework is already in place and in use. DHS administers the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, or the "SAFETY Act". The SAFETY Act, which was passed into law as part of the Homeland Security Act of 2002 (the law authorizing the creation of DHS), is intended to offer affirmative legal defenses to companies that sell or otherwise deploy security technologies (which includes products, services, policies, and procedures) designed to deter, defeat, respond to, mitigate, or otherwise combat security threats. The SAFETY Act offers two types of liability protection. The first type of protection is known as "Designation", which sets a specific cap on damages that may be awarded in litigation following an attack, along with a

prohibition on punitive damages and pre-judgment interest, as well as a requirement that SAFETY Act-related claims may only be brought in Federal courts. Under Designation, the cap on damages is equal to an amount of insurance that the "seller" of the SAFETY Act-approved technology or service must carry as a condition of the award.

The second layer of protection under the SAFETY Act is referred to as "Certification". A Certification award provides the same protections as a Designation, as well as a presumption of immunity from claims arising out of or related to the use of the SAFETY Act-approved technology or service. The protections of the SAFETY Act can be negated with a demonstration that the applicant committed fraud or willful misconduct in the submission of the SAFETY Act application to DHS.

Conclusion

In closing, I thank you again for inviting me to testify. I hope that our extensive experience in responding to and recovering from unexpected events can serve as a model that informs the Framework for all critical infrastructure sectors.

Mrs. BLACKBURN. Thank you.
Mr. Mayer.

STATEMENT OF ROBERT MAYER

Mr. MAYER. Thank you, Chairman Blackburn and members of the committee for giving me the opportunity to appear before you today. My name is Robert Mayer, and I serve as Vice President of Industry and State Affairs at the United States Telecom Association. I have had the privilege in the past of sharing the communications sector coordinating council through which the Department of Homeland Security works to coordinate the infrastructure protection activities of our industry sector with those of the federal, state, local, territorial and tribal governments. Currently, I chair our sector coordinating council's cybersecurity committee.

USTelecom member companies, indeed, our entire sector, including wireless and cable broadband providers, stand on the front lines of cybersecurity. Protecting our networks and our customers from cyber threats is our highest priority and requires our members to innovate literally every single day to meet the challenges posed by increasingly sophisticated adversaries.

In our industry's view, the single most important policy step that can be taken to combat this scourge is giving appropriately cleared personnel in our companies access to real-time actionable cyber threat information. USTelecom supported passage of the Cyber Intelligence Sharing and Protection Act, or CISPA, because voluntary, real-time sharing of threat information will provide both the private sector and the government with the essential tools needed to address malicious cyber activity. We especially appreciate the effort to balance the many factors necessary to gain overwhelming bipartisan passage of CISPA, including providing necessary liability protections while at the same time ensuring appropriate safeguards for privacy and civil liberties. We commend and thank Chairman Mike Rogers, Ranking Member Dutch Ruppersberger, the authors of several helpful Floor amendments, as well as all of those who voted for the bill.

Turning to the President's February 12th Executive order, we are pleased that the Order reaffirms the importance of the public-private partnership in assessing and combating threats and that it envisions a voluntary and collaborative framework for achieving its goals. USTelecom believes that the government can encourage private sector acceptance and adoption of that framework by ensuring, among other things, that it remains a true partnership among all parties at all levels with the flexibility that rapidly changing technological threats require and with strong legal protections and incentives for participation.

I want to express our industry's hope and optimism that the process of implementing the Executive order will turn out well and will lead to widespread acceptance and adoption. We have been working constructively to date with NIST, DHS and the FCC, and hope those good relationships will continue. But do we want to bring to the committee's attention Sections 9 and 10 of the Order, because the manner in which they are ultimately interpreted and implemented may spell the difference between the success and failure of this effort.

Section 9 relates to the identification of critical infrastructure "at greatest risk." Overly expansive designations of critical infrastructure may harm innovation by leading to predictability and stagnation. Conversely, Section 9 may preemptively exempt a major portion of the Internet ecosystem from even being considered as critical infrastructure, a similarly problematic starting point for effective cybersecurity strategy. We are watching the implementation of Section 9 closely.

Section 10 requires federal agencies to review the preliminary framework and determine whether their own current cybersecurity regulatory requirements are sufficient. While this section contains language that would encourage agencies to reduce ineffective regulation, it arguably also serves as a hunting license to regulate, the very thing that would undermine the purported goal of the Order: a partnership with government to make its citizens safer. We do not believe that regulatory proceedings are compatible with addressing cybersecurity threats which emerge and evolve at lightning speeds.

Likewise, with respect to the agency most closely associated with our industry, the Federal Communications Commission, we appreciate and value the contributions it makes to the areas of public safety and emergency communications, including the work of the Communications Security, Reliability and Interoperability Council, or CSRIC, in which we participate. A voluntary and consensus-driven approach, as contrasted with a regulatory approach, is what has made the CSRIC process productive and worthwhile.

In closing, thank you for holding this timely hearing. We are of course on guard against the kind of potential regulatory overreach that would slow our response to cyber attacks or result in static, Maginot Line-type defenses that our opponents will easily bypass. Implemented prudently, however, the Executive order may enhance our ability to respond to cyber threats and represent the triumph of government-private sector cooperation. Thank you.

[The prepared statement of Mr. Mayer follows:]

Summary of
Testimony of Robert Mayer
Vice President, Industry and State Affairs
United States Telecom Association
"Cyber Threats and Security Solutions"

USTelecom represents innovative broadband companies ranging from some of the smallest rural telecoms in the nation to some of the largest companies in the U.S. economy. Its member companies and the entire communications sector stand on the front lines of cybersecurity, defending our country daily from cyber-attacks launched by state-sponsored and non-state actors. This requires our members literally to innovate every single day in order to meet the challenges posed by increasingly sophisticated adversaries.

The single most important step that can be taken to combat this worldwide scourge is giving our companies' security personnel access to real-time, actionable cyber threat information. USTelecom supported the Cyber Intelligence Sharing and Protection Act (CISPA) because it squarely addresses the dual challenges faced by broadband providers dealing with this issue: on one hand, the risks posed by cyber threats themselves, and, on the other hand, the uncertainties and potential legal costs and exposure associated with existing laws when applied to cyber-threat monitoring and response efforts utilized to protect our networks. While safeguards for privacy and civil liberties have been incorporated into CISPA together with other protections, the current legal framework concerning collection, use, and sharing of information is a major cybersecurity challenge facing our nation.

Executive Order 13636 and the accompanying Presidential Policy Directive 21 reaffirm the importance of public-private partnerships in assessing and combatting cyber threats. Our industry is hopeful and optimistic that the processes laid out there will turn out well and will lead to widespread acceptance and adoption. We have been working constructively to date with NIST, DHS, and the FCC. But ultimately the interpretation and implementation of sections 9 and 10 of the Order, and the accompanying PPD-21, may spell the difference between the success and failure of this effort.

Section 9 relates to the identification of critical infrastructure "at greatest risk." Risk designations that are either overly expansive or preemptively underinclusive may undermine many of the elements of a successful framework.

Section 10 of the Order requires federal agencies to review the preliminary framework and determine whether their own current cybersecurity regulatory requirements are sufficient. While the section contains language that would encourage agencies to reduce ineffective regulation, it arguably also serves as a hunting license to regulate, the very thing that would undermine the purported goal of the Order – a partnership with government to make its citizens safer.

Implemented prudently, the Executive Order and PPD-21 will be a triumph of government-private sector cooperation that will enhance our ability to respond to cyber threats. However, we must be on continuous guard against the kind of potential regulatory overreach that would slow our response to cyber-attacks or result in static "Maginot Line" type defenses that our opponents will easily bypass.

Testimony of
Robert Mayer
Vice President, Industry and State Affairs
United States Telecom Association
before the
House Committee on Energy and Commerce
"Cyber Threats and Security Solutions"
May 21, 2013

Chairman Upton, Ranking Member Waxman, Members of the Committee, thank you for giving me the opportunity to appear before you today to present the views of our industry on the cybersecurity threats facing our nation and the possible security solutions. It is both timely and appropriate that this committee, with its jurisdiction covering a range of sectors impacted by this burgeoning threat, take the time to review this issue.

My name is Robert Mayer, and I serve as Vice President of Industry and State Affairs at the United States Telecom Association (USTelecom). I am the past chair of the Communications Sector Coordinating Council (CSCC), one of the current 16 sectors under the Critical Infrastructure Partnership Advisory Council (CIPAC), through which the Department of Homeland Security (DHS) endeavors to facilitate coordination between federal infrastructure protection programs and the infrastructure protection activities of the private sector and of state, local, territorial, and tribal governments. Currently, I am the Chair of the CSCC's Cybersecurity Committee and serve as a senior member on the Cyber Unified Coordination Group under the National Cyber Incident Response Plan.

USTelecom represents innovative broadband companies ranging from some of the smallest rural telecoms in the nation to some of the largest companies in the U.S. economy. Our members offer a wide range of advanced broadband services, including voice, Internet access, video and

data on both a fixed and mobile basis. The customers that rely on our networks include consumers, businesses large and small, and government entities at the local, state, and federal levels. Protecting these networks and our customers from cybersecurity threats is our highest priority.

Our member companies – indeed, the entire communications sector, including wireless and cable broadband providers – stand on the front lines of cybersecurity, defending our country every day from cyber-attacks launched by state-sponsored and non-state actors. These attacks range from interruptions that constitute mere nuisances, which are easily interdicted and remediated, to potentially catastrophic events that threaten to cripple our economy and jeopardize our security. Our companies have taken significant steps to protect the integrity of our networks and the security and privacy of our customers. This requires us literally to innovate every single day in order to meet the challenges posed by increasingly sophisticated adversaries.

The Essential Keys – Information Sharing and Liability Protection

In response to the dramatic increase in cybersecurity threats, our industry has been working with Congress and the Administration over the past two years to enhance both the government's and the private sector's cybersecurity posture. The single most important step that can be taken to combat this scourge is giving our companies' security personnel access to real-time, actionable cyber threat information. To that end, USTelecom supported passage of H.R. 624, the Cyber Intelligence Sharing and Protection Act (CISPA), as well as its predecessor legislation in the 112th Congress, because the voluntary and real-time sharing of such threat information will provide both the private sector and the government with the essential tools they need, in a timely

and useful manner, to detect, deter, and respond to malicious cyber activity. We commend the authors of that legislation, Representative Mike Rogers (R-MI), a member of this committee and Chairman of the House Intelligence Committee, and the Intelligence Committee's Ranking Member, Representative Dutch Ruppersberger (D-MD), as well as all who voted for it.

CISPA is important because it is the first bipartisan legislation to pass either House of Congress that squarely addresses the dual challenges faced by broadband providers dealing with this issue today: on one hand, the risks posed by cyber threats themselves and, on the other hand, the uncertainties and potential legal costs and exposure associated with existing laws when applied to cyber-threat monitoring and response efforts that are utilized to protect our networks in a variety of circumstances. The current legal framework concerning the collection, use, and sharing of information remains a substantial barrier to effective communication between and among all relevant public and private stakeholders. Broadband providers believe this continuing legal uncertainty, and its effect in limiting the sharing and use of relevant information about cyber threats, stands as a major cybersecurity challenge facing our nation.

As we meet here today to discuss cyber threats and security solutions, we cannot emphasize enough that the most important role government can play in encouraging efforts to detect and deter cyber threats is to remove that uncertainty and to establish conclusively that cyber threat monitoring and the ability to deploy active defenses are not merely lawful but encouraged. While the President's Executive Order on cybersecurity has been described as a "down payment" on future government legislation to secure U.S. critical infrastructure and networks, the simple inability of private sector stakeholders to share information with each other or with appropriate

federal agencies, and to act quickly on that information, without fear of being sued, regulated, or held criminally liable must urgently be addressed.

We were heartened by the strong bipartisan support CISPA received in the House – a real recognition of the careful and thoughtful way in which Representatives Rogers and Ruppersberger worked tirelessly to balance the many important factors involved in developing an effective approach to this issue. Those factors include the critical need for increased real-time sharing of information, and particularly classified information, between government and private sector parties, the necessity of providing liability protections if sharing between and among government and private sector parties is truly to occur in real time and defensive actions are to be taken, ensuring that the appropriate agencies of government play appropriate roles in the process, and the importance of providing safeguards for protecting privacy and civil liberties.

The legislation's limitations on the use of shared information for cybersecurity purposes, the enhanced roles given to the civilian Department of Homeland Security and its Inspector General, and the assurance that companies cannot use shared information as a loophole for consumer marketing are just a few examples of the way in which CISPA's authors endeavored to strike an appropriate balance between our security and our liberty. But the most important principle enshrined in the bill is its recognition that neither private sector companies nor the federal government can or will share cyber threat information with each other in real time – *in other words, in time to avert the real threat at hand* – so long as they remain exposed to the potential threat of class actions, criminal prosecutions, administrative enforcement proceedings, regulatory rulemakings, or other similar legal liabilities. We look forward to continuing to work with the bill's authors and with the Senate to strengthen the bill and hope that, driven by the impressive

bipartisan majority that approved it in the House, it will form the basis for legislation the President will sign this year.

Cybersecurity Executive Order – The Broad Outlines

On February 12, 2013, the White House released its long-awaited Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," establishing a process for the adoption of cybersecurity standards under what it termed a voluntary and collaborative framework.* The Order aims to facilitate national cybersecurity policy goals by directing federal agencies to reduce duplicative and excessively burdensome cybersecurity requirements. We are pleased that the Order reaffirms the importance of public-private partnerships in assessing and combatting threats, a strategy we believe is highly effective.

The Order directs the federal government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that they may better defend against cyber threats. It mandates the rapid dissemination of such reports to private sector partners; expands the Enhanced Cybersecurity Services program to all critical infrastructure sectors; and expands and expedites the processing of security clearances to certain personnel employed by critical infrastructure owners and operators.

* The Executive Order was issued concurrently with a "Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience," also known as PPD-21, which sets forth the roles and responsibilities of federal departments and agencies in "advanc[ing] a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure." PPD-21 identifies the 16 critical infrastructure sectors mentioned above and the Sector-Specific Agency (SSA) "responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of [each] sector." The Communications Sector is one such designated sector, and DHS is our sector's designated SSA. PPD-21 supersedes Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, issued December 17, 2003.

The Order also calls on the federal government to develop a voluntary cybersecurity framework within one year through a public review and comment process. The framework will include standards and procedures to address cyber risks and will be reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, and operational feedback from owners and operators of critical infrastructure.

A voluntary program will also be established to encourage adoption of the cybersecurity framework by owners and operators of critical infrastructure and any other interested entities, and the federal government will develop a set of incentives to promote adoption of the framework. Sector-specific agencies will report annually to the President on the extent to which owners and operators are participating.

Elements of a Successful Cybersecurity Framework

On April 3rd, the National Institute of Standards and Technology (NIST) convened a workshop to gather stakeholder input on how to develop the framework for improving critical infrastructure cybersecurity. The day-long event marked the official launch of the process described in the Executive Order, and USTelecom has offered detailed comments on both the development of the framework as well as on possible incentives to promote its adoption. Some core principles we provided NIST, as well as others on which only Congress has the power to act, include:

- Promote a true public-private partnership – The framework should promote the use of a true public-private partnership model. Such models have an established, successful history in the telecommunications sector and are ideally suited for the cybersecurity framework. Government and private stakeholders can accomplish more working through a collaborative and cooperative effort where each side brings complementary competencies, resources, and

capabilities. For example, private stakeholders have valuable entrepreneurial and innovative insights that are of tremendous value to the cybersecurity effort. Additionally, these stakeholders have important insights into cybersecurity approaches that can or cannot work in a competitive marketplace. For its part, the federal government has vast resources in the form of extensive expertise, access to critical resources, and a diverse and substantial user base.

- Encourage information sharing – The framework should incorporate the Executive Order guidance that directs the federal government to increase the timeliness and quality of information provided about cyber threat information. However, as mentioned earlier, the current legal framework concerning information sharing poses a substantial barrier to two-way communications, one that must be addressed by Congress.
- Preserve innovation – Broadband providers are literally innovating every day in order to combat increasingly sophisticated cyber-attacks. Government should ensure that the framework does not hinder the ability of private industry stakeholders to innovate in the marketplace – for instance, by imposing costly mandates coupled with a lack of viable incentives. Mandated practices and rules will undermine cybersecurity efforts by leading to uniformity and predictability, thereby making it easier for cybercriminals to prey on consumers and businesses. In addition, with speed-of-response to cyber emergencies often measured in seconds, not hours or days, providers must be able to take decisive action without regulatory second-guessing or the need for a lengthy review and approval process.
- Develop flexible and non-prescriptive approaches – The framework won't succeed if it's based on a "one size fits all" approach. Because of the continuously evolving nature of cyber threats, industry must have the flexibility to respond quickly and efficiently. And given the importance of cybersecurity to maintaining a strong relationship with our customers, our

industry is continuously revising and updating existing cyber standards to ensure the highest levels of safety. Standards, norms, and best practices can help address current threats, but innovation is needed to guard against future unknown threats. We believe any effort to transform voluntary best practices derived in consensus-based venues into prescriptive mandates would have a serious chilling effect on future voluntary initiatives and partnerships with the federal government.

- All players share responsibility – Any framework must acknowledge the reality that protection of critical infrastructure is a shared responsibility that cuts across all elements of cyberspace and, indeed, the economy. Exclusion of one party or group will create vulnerabilities that could expose other stakeholders to potential threats. Such a holistic approach is essential, based on the organic nature of the Internet. In this sense, the Internet has developed an organic quality insofar as it continually grows and adapts in response to newly added systems, functions, and services.
- Examine the business case for cybersecurity investments – When recommending practices, government should be mindful that some companies have business models that allow for cost-recovery of investments needed to shore up cybersecurity protection, while others do not. For the latter group, significant costs could limit the speed and scope of adoption. Therefore the framework should include effective incentives designed to promote participation. There are a number of positive incentives the federal government could consider to foster increased cybersecurity, including tax incentives to help improve cybersecurity, as well as direct funding and/or grants for cybersecurity research and development.
- Establish legal safe harbors for participation – Voluntary adoption of the cybersecurity framework by owners and operators of critical infrastructure and other interested entities will

occur fastest and most efficiently if companies are assured they can spend their limited resources on implementation rather than on lawyers to deal with compliance and litigation issues. The Administration, to the extent the law permits, and Congress, if necessary, should establish legal safe harbors that would encourage participation in the voluntary framework. One such safe harbor would be a strong liability protection regime analogous to that we've sought for information sharing. Another would be preemption of future state and local legislation and regulation. Given the inherent uncertainties surrounding future regulation at both the federal and state level, companies would clearly see in such safe harbors the benefits of adopting the framework. Moreover, such provisions would greatly assist the collaborative aspects of the framework by adding an increased element of trust and good faith between government and industry stakeholders, as well as the predictability of known business costs.

Implementation of the Order Will Determine Its Success

The implementation of the Executive Order is a complex undertaking, intended out of necessity to be carried out in a relatively short time frame. Given this situation, I want to express our industry's hope and optimism that the process laid out in the Order will turn out well and will lead to widespread acceptance and adoption not just by our sector but by all. To date, we have had an extraordinarily good working relationship with NIST, which historically and culturally has a long-standing reputation for working in strong partnership with the private sector to provide guidance on the path toward development of voluntary consensus standards.

We have also developed an effective working relationship with DHS, largely through the public-private partnership efforts of the CSCC and the Communications Information Sharing and Analysis Center (Comms ISAC). To date we have seen a good faith effort on the part of DHS to

implement the Executive Order using the public-private partnership model, which has succeeded in so many other areas of our cybersecurity work. We have had many hours of productive and constructive discussion with DHS on the issues in the Executive Order of greatest concern to us, and these discussions continue on virtually a daily basis. We are hopeful that those concerns will be reflected in DHS's final document, but the words we see on paper will be the real test of how the partnership process has worked.

In that regard, we do want to bring to the Committee's attention sections 9 and 10 of the Order, because the manner in which they are ultimately interpreted and implemented may spell the difference between the success and failure of this voluntary partnership effort.

Section 9 relates to the identification of critical infrastructure "at greatest risk." It is unclear at this juncture how encompassing it will be of our businesses and infrastructure. On one hand, overly expansive designations of critical infrastructure that lead to prescriptive solutions will undermine many of the elements of a successful framework by harming innovation and by leading to predictability and stagnation, outcomes that only make it easier for cyber adversaries to achieve their nefarious objectives. On the other hand, section 9 may preemptively exempt a major portion of the Internet ecosystem from possible inclusion as critical infrastructure. Given the interconnected nature of the Internet, the effectiveness of any cybersecurity strategy is inherently undermined when a major portion of the ecosystem is exempt from consideration even from the very start of the process.

Section 10 of the Order requires federal agencies to review the preliminary cybersecurity framework and determine whether their own current cybersecurity regulatory requirements are

sufficient. Agencies are then directed to propose prioritized, risk-based, efficient, and coordinated actions to mitigate cyber risk. Section 10 also requires that agencies consult with owners and operators of critical infrastructure, and report on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements and make recommendations to minimize or eliminate such requirements. While we are gratified the section contains language that would encourage agencies to reduce ineffective regulation, it arguably serves as a hunting license for departments to regulate, the very thing that would undermine the purported goal of the Order – a partnership with government to make its citizens safer. Indeed, these agencies are explicitly "encouraged" to go on such a hunting trip.

While section 10 does not apply to independent regulatory agencies, the accompanying PPD-21 singles out by name the one such agency most closely associated with our industry – the Federal Communications Commission - and directs that the FCC "to the extent permitted by law, is to exercise its authority and expertise to partner with DHS and the Department of State, as well as other Federal departments and agencies and SSAs as appropriate, on: (1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends."

We appreciate and value the contributions the FCC makes to the area of public safety and emergency communications, including the work of its Communications Security, Reliability and Interoperability Council (CSRIC), in which we are active participants. In the rapidly changing environment that cybersecurity presents, regulatory proceedings are incompatible with addressing new threats that can emerge and evolve at lightning speed. That is what has made the voluntary and consensus-driven approach of venues like CSRIC productive and worthwhile.

In closing, let me again thank the Committee for holding this timely hearing. Implemented prudently, Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," will be a triumph of government-private sector cooperation that will enhance our ability to respond to cyber threats in rapid and innovative ways. As it is implemented, however, we must be on continuous guard against the kind of potential regulatory overreach that would slow any response to cyber attacks or build static "Maginot Line"-type defenses that our opponents will easily bypass.

Mrs. BLACKBURN. Thank you, Mr. Mayer. I thank each of you for your testimony, and I yield myself 5 minutes for questions.

Mr. Mayer, I am going to begin with you. Let us talk for just a second about what you just mentioned, and I want to hear just a little bit more from you on why you think that the interpretation and implementation of Sections 9 and 10 of the Executive order may spell—what was your statement there?—spell the difference between success and failure of the effort. So just another couple of sentences on that?

Mr. MAYER. OK. Sure. So the vast body of the Executive order governing critical infrastructure under Section 2 is under a voluntary framework. Section 9 carves out what is determined to be critical infrastructure at greatest risk, and there is a process right now where DHS is working with industry and others to determine what is on that list of critical infrastructure. To the extent that that list becomes overly expansive, it will overcome, so to speak, the nature and usefulness from our perspective of the voluntary framework, and I think it was interesting that Secretary Gallagher mentioned as a concern that that very provision might operate to be a disincentive for folks who participate in the voluntary framework. We are going forward with the presumption that it is all going to turn out well and that the voluntary framework will dominate and that there will be——

Mrs. BLACKBURN. So the fear is overreach and uncertainty basically?

Mr. MAYER. Yes, ma'am.

Mrs. BLACKBURN. OK. Mr. Highley, I want to come to you. I will just work right down the line. Listening to Mr. Waxman, it made it sound like our electric utilities are just getting bombarded every day, and my understanding was, these attacks are really fairly rare for you all, and more often than not, it is an attack on the consumer-facing side like most businesses. So I just want to be certain, don't you already have mandatory standards that are governing how you should protect your operations?

Mr. HIGHLEY. Yes. The answer is yes. The majority of those attacks, while large in number, are the same attacks that every business receives to their Internet portal, and those are on the public-facing sides of the business. They are all stopped at the gate, and the supervisory control and data acquisition systems have mandatory enforceable standards for how you interface to those. We don't have significant problems with attacks to those today.

Mrs. BLACKBURN. OK. Let me just very quickly, a show of hands, how many of you prefer staying with standards, the voluntary standards as opposed to going to regulation? How many of you prefer standards? OK. All right. I just was curious about that. And then I would like to have one statement from each of you. As we look at the cybersecurity framework and the plans that are in place for implementation, I would like to know what your primary concern is, and Mr. McCurdy, I would like to start with you and just work down the line, and then I will yield my time.

Mr. MCCURDY. Thank you, Madam Chair. I think our primary concern is that when you are developing the risk profile and the definitions of what is critical infrastructure, that they look at existing tools that DHS has used and TSA, we work through those. We

have a lot of self-assessment tools that companies run. So that experience should inform a lot in this process.

Mrs. BLACKBURN. OK. So you kind of match up with Mr. Mayer on the concerns?

Mr. MCCURDY. Yes.

Mrs. BLACKBURN. OK. Mr. McConnell?

Mr. MCCONNELL. My primary concern is it does not have the effect of law and so therefore it cannot grant liability protection as an incentive to industry to comply with these standards.

Mrs. BLACKBURN. OK. Ambassador?

Mr. WOOLSEY. I believe that we are at war without wanting to be so, and whether it is North Korea or Iran, they believe they are at war with us. They have the hardware to do us huge damage in various ways but particularly through electromagnetic pulse, and trying to defend against them with 3,500 generals—the utilities—each commanding essentially its own force is going to fail.

Mrs. BLACKBURN. OK. Dr. Papay?

Mr. PAPAY. Madam Chair, I think it is important for businesses to have that ability to break down barriers to sharing information. I will go along with what Dr. Schneck was saying earlier. It has got to be as easy as possible for us to share that critical cybersecurity information with each other, and the EO is getting there but we need legislation to follow it up.

Mrs. BLACKBURN. Great. Dr. Schneck?

Ms. SCHNECK. I completely agree with Dr. Papay. I will add more, and that is on the technology front, right tool for the right job. We have so many technologies as a community all over the world. I mentioned one that many people provide, a whitelisting concept. We have to have a framework that allows people to very quickly not only build on those and innovate but assign the right technology to the right job for what the attacker is doing today.

Mrs. BLACKBURN. OK. I am running over time but I want to finish the panel. Mr. Blauner?

Mr. BLAUNER. Since everyone already mentioned information sharing, to us, I would say the most critical thing is, we are already a regulated environment, which is why I didn't raise my hand earlier. We just don't need extra complexity added into that and having another agency come in and try to regulate us a second time.

Mrs. BLACKBURN. Mr. Highley?

Mr. HIGHLEY. For electric utilities, I would say don't short-circuit the existing regulatory framework we have where FERC can order NERC to write standards as needed.

Mrs. BLACKBURN. I am going to have to get you that app. Mr. Mayer?

Mr. MAYER. With the exception of Section 9 in the context of the voluntary framework, one of the primary concerns that we have and I think Representative Eshoo mentioned this, is that we can't have a one-size-fits-all solution, not only across the sectors but even within the sectors because different companies have different business models and different abilities to recover for investment and security.

Mrs. BLACKBURN. Thank you. I am way over my time. Mr. McNerney for 5 minutes.

Mr. MCNERNEY. Thank you, Madam Chair.

Mr. Woolsey, very sobering testimony. Do you think that the solution to the threat is hardware-based that you discuss in EMP threat or do you think it is software-based? I mean, there must be some way to protect the critical components from EMP.

Mr. WOOLSEY. There are various things. The surge arrestors can help with one part of it, Faraday boxes for other components. There are a number of things that can be done. They overlap, some of them, with traditional cyber defenses; surge arrestors are one example. Others do not. What will fail, I think, disastrously is for 3,500 utilities each voluntarily going off on its own because they don't want to be regulated trying to figure out what to do about electromagnetic pulse. They will lose. Anybody who is facing an enemy who is commanded by somebody as shrewd as the senior leadership in Iran or, I am afraid, probably also North Korea, who is focused on defeating us, anybody who is facing an enemy like that with 3,500 generals all going off in different directions will lose. We will lose.

Mr. MCNERNEY. So you mentioned that some of the hardware that we need is actually going to help provide protection at the cyber level as well, so I appreciate that comment.

Now, Mr. Highley was talking about the NERC process providing sufficient protection and us not messing it up. Do you agree with that perspective?

Mr. WOOLSEY. Well, the first order after 9/11 that came out of NERC in response to a query, as I understand it, or a direction from FERC in total took 44 months, I believe. That is—World War II took 3 years and 8 months for us. So if response to one part of one problem is timely and useful when it comes within the time that we went from Pearl Harbor to accepting Japan's surrender, then OK. But I think that standard for promptness and effectiveness of response in circumstances in which you are dealing with an enemy is nuts. It is nuts to suggest that that will be effective against an enemy, against solar-based electromagnetic pulses. If we are lucky, maybe it will work.

Mr. MCNERNEY. Thank you. Ms. Schneck, you mentioned the issue of legal liability and protection on that issue, but that is a huge gift to a company to be given legal liability protection. What would you be willing to give back in terms of first of all protection to get that kind of legal liability protection yourself?

Ms. SCHNECK. So to clarify, we would want the protection. We work very hard in analytics, as does our community, all the different companies.

Mr. MCNERNEY. Right. You want legal liability protection but personal information—I mean, what would you be willing to trade to get that kind of gift from the federal government?

Ms. SCHNECK. To also clarify, we don't ever share personal information. That is not what we do. We share cyber indicators. A good example is the address of a machine that is sending something bad to, say, 30,000 different places or feeding that information to 30,000 different machines to form a botnet. Our understanding is that a certain link goes to a site that will feed you code to hook you up to steal your intellectual property. That is the kind of information we want to share between machines, and between humans,

we want to be able to say things like, if you are looking at a weather map, I see danger there, or I see the same type of attack because we protect such a wide part of the globe. If we see the same type of event happening to some in the same sector, we want to be able to tell that to the whole sector. We want to act in good faith, which we do today. We certainly applaud CISPA and the work there. We want to be able to share more with the community without fearing we will get hurt.

Mr. MCNERNEY. OK. I am going to ask a question similar to what the chairwoman asked. If NIST develops performance-based standards—and anyone can answer this—how would industry cooperate in terms of implementing or compelling those standards to be enforced?

Mr. MCCONNELL. If you are going to grant industry liability protection, you are going to have to have some audit that will allow you to determine to verify that they had met the standards. The way I think about this issue is, the set of standards are established, businesses comply with those standards, and then if there is a breach, they would have liability protection against the fact of a cyber breach.

Mr. MCNERNEY. Thank you. I will yield back.

Mrs. BLACKBURN. Thank you. Chairman Walden for 5 minutes of questioning.

Mr. WALDEN. Thank you very much, Madam Chair.

Mr. Mayer and Ms. Schneck, Dr. Gallagher has emphasized that the Executive order framework would remain voluntary. Are you confident it will? Mr. Mayer, do you want to go first?

Mr. MAYER. I am confident that NIST in its current work has every intention of developing a voluntary framework, and in fact, it is their mandate as an organization to do that.

Mr. WALDEN. And you are confident it will stay voluntary? I know nobody can really predict the future well but——

Mr. MAYER. The concern or the caution is around what happens after framework is developed and when it moves toward sector-specific available. When you combine that with the list that we still do not have settled, it can morph into something that, as I've indicated before, takes on a different quality, and that would be problematic. But we are—from every indication in talking with all of the key federal entities, right now we are quite sanguine that it is going to be a voluntary process.

Mr. WALDEN. Dr. Schneck?

Ms. SCHNECK. So thank you. We are very participatory in the framework process as well. We have yet to fully finish studying the Executive order as a whole, but at present we are very supportive of the framework of the voluntary focus of the idea that all different technologies could be explored, innovation could be made more rapid. More cybersecurity jobs could come as a result of that. Believing it would make us more secure, we work in very close partnership with NIST. We have just signed an MOU with their cybersecurity center to foster that innovation even faster as have many other companies. So at present, it does look optimistic and we have been very supportive of that.

Mr. WALDEN. And again in your testimony, Dr. Schneck, you highlight your security-connected products as comprehensive. Do

you believe that the Executive order's approach to cybersecurity is comprehensive?

Ms. SCHNECK. I think that remains to be seen. We are in the early stages. So far we have been working, again, in partnership with NIST. A full response to the RFI focused a lot on this need for private sector innovation to drive where security can go because that adversary is so fast, the only way to be out front ahead of those that wish to do us harm is to band together, and I think thus far—again, we are not finished studying the full effects of the EO.

Mr. WALDEN. All right. Mr. Highley, you are here representing some of the electrical co-ops, right?

Mr. HIGHLEY. Yes.

Mr. WALDEN. Mr. Woolsey, who has extraordinary service in the government, has indicated, if I am hearing him right, that he has deep concerns about a more voluntary structure with so many utilities and power suppliers. Can you comment on his comments relative to FERC and the ability to enforce and your organizations and others that you are representing today, ability to protect the grid?

Mr. HIGHLEY. So on behalf of the trade association, the National Rural Electric Cooperative Association, they are engaged in discussions with NIST and with FERC and NERC on the regulation to protect us from these issues. I agree, it is a very serious concern. What we want to do is see that work through a deliberate process that involves all the stakeholders. That is why we support the NERC process. I also agree with Mr. Woolsey that the process has been very slow in the past and we are taking actions to improve the speed at which that can move, and I think you saw in the recent FERC order, they are asking for the geomagnetic disturbance actions to be taken within 6 months. So we are trying to accelerate that process in order to get actionable, enforceable standards that utilities will meet.

Mr. WALDEN. All right. And Mr. Mayer, again, what sort of industry best practices are most effective from your experience in combating cyber threats and how can such practices be identified, incorporated and encouraged under the Executive order?

Mr. MAYER. So I think clearly I am biased, but I would say that the communications sector is a leading sector in terms of advanced cybersecurity capabilities. Not only do we have to protect our networks because that is an ongoing business against attacks, but we have to protect our customers, and many of those customers are some of the largest corporations in the United States and some of the largest government agencies. So we have over the years invested significant amounts of money and capabilities into innovating and developing all sorts of preventative response, mitigation, technologies, tools, practices. The interesting thing also is that many of our companies compete in this space for services, so it is a very active market that encourages innovation and then encourages further investment, and you know, we are in constant conversations either through the council or other mechanisms, some business-to-business mechanisms, in which we talk about these capabilities, and we will bring these capabilities to discussions at NIST at these workshops and demonstrate some of the things that

we do, and much of the work that we have done in developing best practices, for example, at the FCC through CSRIC.

Mr. WALDEN. Thank you, and thanks for your generosity on the time.

Mrs. BLACKBURN. Absolutely. Mr. Waxman for 5 minutes.

Mr. WAXMAN. Thank you very much, Madam Chair. We are talking about cybersecurity for a range of critical infrastructure sectors, but I want to focus on the electric grid, as I did earlier, because it is the foundation for every one of these sectors. Protecting the grid from cyber attacks and other threats is essential to our economy.

Ambassador Woolsey, you touched on some of these issues but I want to bring them out for the record. It is not just our civilian infrastructure that depends on the grid. What about our national security installations? Aren't they also largely dependent on the electric grid?

Mr. WOOLSEY. Absolutely, Congressman Waxman. To the best of my knowledge, there is one military base in the United States, China Lake, which has its own water steam system, has a geyser underneath it, essentially, and it sends electricity to Los Angeles when it doesn't need it itself. Everybody else is on the grid. So if the grid goes down, soldiers and sailors are as hungry as everybody else.

Mr. WAXMAN. Thank you very much. We only have a limited time so I want to get some more points in here. The problem is that the Federal Energy Regulatory Commission, what we call FERC, lacks authority to ensure that the grid is protected. The industry-controlled North American Electric Reliability Corporation, or NERC, issues the cyber and physical security standards for the grid. Now, NERC operates by a consensus. Standards have to be approved by a supermajority vote of the utilities. It takes them years to develop a standard. The most recent version of NERC's critical infrastructure protection standards took 43 months to develop and they are still not in effect, and these standards do not include measures to address specific viruses or cyber threats. Once NERC submits a standard, FERC cannot directly fix an inadequate standard. So the process will start all over again.

Mr. Ambassador, what do you think of NERC's track record on grid security threats? Is this the right regulatory model for national security issues?

Mr. WOOLSEY. I don't believe it is the right model, Congressman, and I think NERC's record on security against the kinds of sophisticated threats we face today in traditional cyber and electromagnetic pulse is virtually nonexistent.

Mr. WAXMAN. In 2010, Fred Upton, now a chair, and Ed Markey, soon to be Senator from Massachusetts, had a bipartisan grid security bill. It would have provided FERC with the authority it needs to improve the security of the electric grid. This committee passed that bill by a vote of 47 to nothing. The House passed the bill by voice vote. Members viewed it a national security issue.

Ambassador Woolsey, in April of 2010, you and several other prominent national security experts, former national security advisors and Secretaries of Defense and Homeland Security wrote to the committee to strongly endorse the bipartisan GRID Act. Do you

still think that FERC needs additional authority to protect the electric grid against threats and vulnerabilities?

Mr. WOOLSEY. Yes, I do, absolutely.

Mr. WAXMAN. The GRID Act also provided FERC with authority to address the threat posed by electromagnetic pulses. How worried should the committee be about this threat for which there is no mandatory standard?

Mr. WOOLSEY. I think the committee should be quite concerned and all Americans should. It is an extremely dangerous situation we are in now, and we are where we were yesterday.

Mr. WAXMAN. Well, I thank you for your testimony and your answers to my questions. I just wanted to make it very, very clear because you and I see this issue in the same way. We have got to rely on clear regulatory authority to get this job done.

Mr. WOOLSEY. Thank you, Congressman. I think that NERC could deal adequately with squirrels and tree branches, which is what the main problem is for a lot of electricity maintenance regular delivery, but North Korea and Iran, I think, are quite beyond their competence.

Mr. WAXMAN. Thank you for your answers and thank you for your service. I yield back the time.

Mrs. BLACKBURN. The gentleman yields back. Mr. Latta for 5 minutes.

Mr. LATTA. Thank you, Madam Chair, and again, thanks very much to this panel for your very instructive information that we have received this morning and this afternoon.

You know, as I was sitting here thinking that there is a lot of folks, I would say a great majority of Americans, don't understand the threat that we are under and how important it is that we come to real grips in this country of the cybersecurity that we have to have to protect ourselves, and if I could just start with Mr. Papay. In your testimony, you talk about Northrop Grumman's focus on internal cybersecurity awareness training as part of your internal protection efforts and your cyber academy. Can you share a few points about what kind of training that people go through when they are at that?

Mr. PAPAY. Yes, sir. Thank you for the question. It is a voluntary participation within the company for everybody to sign up for at least a lower level of cybersecurity awareness training to understand where the threats are coming from and what they can do as an employee of the company to combat those because, really, all of my 70,000 employees in the company are really my first line of defense against incoming cyber threats that they might get in their email or through a malicious Web link. So above the basic cybersecurity awareness, it moves on up the pyramid, as we call our cyber academy pyramid, to really get to those certifications where somebody wants to go off and advance their knowledge of cyber and move it on up all the way up through penetration testing and forensics and secure coding to where we have really got a set of experts within the company because cybersecurity for us is not just about the defense of our company but it is also the primary business that we are in. So that is our cyber academy in a nutshell, sir.

Mr. LATTA. Thank you.

Mr. McConnell, if I could ask you a quick question, and I really appreciate your knowledge of the severity of the cyber threats that face our Nation. Do you have any estimates as to what the economic espionage costs are to this country every year?

Mr. MCCONNELL. There is a huge debate about that issue now. The community struggled with a National Intelligence estimate, and they could not agree. I personally would put it in the cost of billions of dollars and millions of jobs, and that is based on my best guess at looking at all the information over the past 20 years, billions of dollars and millions of jobs every year.

Mr. LATTA. Well, and one of the things again, like I said, I have had a couple of informational meetings with the FBI in my district. We are doing one again next week. How do we get this information out? You know, a lot of the larger companies out there are worried about the cybersecurity and it is getting the folks back home in the smaller companies to say, you know what, this could affect us because we might be the largest part of the chain, the weakest link that they get into and move up from there. But, you know, have you in your experience talked with individuals out there, companies out there that might be smaller in nature and expressed to them how serious cybersecurity is for them?

Mr. MCCONNELL. The answer is yes, quite a bit, but let me make a point with regard to sharing the information. The rules that we have were created in World War II and they served us well in the Cold War, and both Ambassador Woolsey and I have had the position of being responsible for protecting sources and methods of the U.S. intelligence community. The rules are in place. That community will not change, will not share unless the rules change so they can share information with the private sector. I have observed this over a long career, and the rules must change. Therefore, we have a process for flowing information to corporate America. The point is, why do we collect this information, why do we analyze it? It is to protect the Nation. So we have to then have a forcing function to cause a bureaucratic organization that will not comply with that process of sharing information unless they are compelled to do so.

Mr. LATTA. Thank you. And also, Mr. Mayer, if I could just briefly, I am running out of time here. Again, I thank you for being here today. You know, in your testimony you highlight the number of your member companies, the entire communications industry on the front of cybersecurity, and when you are looking at the overall picture, given that USTelecom represents a large range of companies from small rural providers to some of the largest in the country, what would be the effect of labeling some of these businesses and networks as critical infrastructure?

Mr. MAYER. I didn't hear the last part, sir.

Mr. LATTA. What would be the effect of labeling these businesses and networks as critical infrastructure?

Mr. MAYER. Well, there are criteria that are being established to define what critical infrastructure is under Section 9. Under Section 2, it is vague, and I think there is an assumption that the broad sector is determined to be critical infrastructure under that element. So the question becomes, to what extent can different companies of different sizes have incidents that result in catastrophic situations, and the truth is, not very substantially. Obvi-

ously, the greater the footprint, the different customers that are served, the concentration of facilities in an area, all will make a difference. But for purposes of the voluntary framework under Section 2, the entire sector is captured as critical infrastructure.

Mr. LATTA. Thank you. Madam Chair, my time is expired and I yield back.

Mrs. BLACKBURN. The gentleman yields back. Ms. Eshoo for 5 minutes.

Ms. ESHOO. Thank you, Madam Chair. I want to thank the entire panel. This is a panel with enormous depth and breadth of expertise, and a special welcome to our former colleague, Dave McCurdy, who served as the chairman of the House Intelligence Committee, to Admiral McConnell, who served our Nation as a Director of National Intelligence, and to Ambassador Woolsey, who served as the Director of the CIA. With your collective presence, but most especially from this end of the table, this is a confirmation that this is a national security issue, period. It is a national security issue. It is not an "and" or an "or." We can't be squishy about it. I mean, we really have to put the pedal to the metal, and I know that probably all of you and just about all of us have been asked to give speeches on cyber attacks and cybersecurity over the last several years.

These attacks are really the new normal. They are the new normal, and I don't think there is any question about that. I don't know what day I pick up the newspaper that there isn't some article about who is doing what to our country. So it is a question about how we are going to handle this. Now, what is very interesting to me today is our grid, and I want to go to Ambassador Woolsey, and I heard Dr. Gallagher from NIST talking about a lot of voluntary cooperative measures, and I think there is a place for it, but I have to tell you from what I think we are all experiencing, I don't think our national grid should be left up to that. So can you just spend a moment—and I have a couple of other questions if I have time—but I think when there is only one defense operation in our Nation that can rely on its own energy so that this doesn't occur to them, I think we are leaving ourselves absolutely wide open. I mean, it is like here we are, come get us.

Mr. WOOLSEY. Congresswoman, I completely agree with you. I have been very concerned and speaking and writing about this issue for some years. I think that the problem is that our grid grew up in the beginning of the late 19th century and it is still growing, but mainly in the 20th century. During the period of time in which the only time we had to worry about security inside the country at all was really right after Pearl Harbor with Japanese and German submarines off the coast. Yes, in the Cold War, we and the Soviets deterred one another but generally speaking, the only time Americans were really worried somebody might be coming ashore, might go after, you know, a utility or something like that was from 1941 to around 1946. I think that that mentality has meant that we have put together an electric grid that is designed for openness, for ease of access, for being cheap, providing electricity as cheaply as possible, and without a single thought being given to security except for nuclear power plants, and even the nuclear power plants, most of the time their transformers are outside the fence, even

though the plant itself may have great guards and so forth, and——

Ms. ESHOO. Do you believe, if I might, I would appreciate this, and we are going to have a working group and I think that I would like to have you come back to be instructive to us, but do you think that this deserves a different kind of set of approaches because it is what it is? And, you know, God forbid that this goes down, we are cooked.

Mr. WOOLSEY. Technology has caught up with us. At the same time we were doing the Y2K fixes in the late 1990s, the Web was coming heavily into use and everybody decided hey, what could go wrong if we put the control systems for the electric grid on the Web and the SCADA systems, some of them, Supervisory Control and Data Acquisition systems. So you have a situation now where our control systems for our electricity are open to hackers. That wasn't the case some years ago. So we have not only ignored security, we have done really, really dumb things without thinking about security, and we are now faced with a situation with the grid in which we have to make some very substantial changes very quickly because of really serious dangers, and a lot of people want to put the blinders on and say gee, that is tough, we don't want to deal with that. I am delighted to help in any way I can.

Ms. ESHOO. Well, I think it gets into a debate of whether the government should regulate or not in this area. That is really where the rub comes. But I think that we really have to scrub this with the seriousness that needs to be brought to it because this is an enormous vulnerability for our country. It is a very serious one, and I appreciate your work. I have so many questions that I want to ask. I wish I were the only one here and could just go on and on, but I will submit my questions to you, and thank you to all of you for testifying, and for those of you that spent considerable time serving our government, thank you.

Mrs. BLACKBURN. The gentlelady yields back. Mr. Lance, you are recognized for 5 minutes.

Mr. LANCE. Thank you, Madam Chair, and it is an honor to meet all of you, and this is certainly among the most distinguished panels I have heard as a member of the committee.

Regarding cybersecurity, I usually think of challenges from China and Iran and from Russia, and to the distinguished members of the panel, and I would start with you, Ambassador Woolsey, and also Admiral McConnell, I have heard several times this morning North Korea. Might you go into a little more detail regarding your belief in the threat from North Korea?

Mr. WOOLSEY. Yes, Congressman, not particularly cyber, although they do some cyber attacking. Mike would know more about that than I. The problem is that one way to launch an electromagnetic pulse attack against the United States, and this is, by the way, in my op-ed in the Wall Street Journal this morning too, is to use what is called a fractional orbital bombardment system, FOBS, which was invented by the Soviets. It is essentially a way to bypass all of our defenses by launching a satellite into orbit, usually relatively low Earth orbit, and launching it toward the south because our detection systems, our radars and so forth, are focused north, and the one North Korean satellite and the two, or

now three, I think, Iranian satellites have all been launched toward the south and they have all been launched at an altitude to have an orbit over us that would be pretty optimal with respect to the detonation of a nuclear weapon and the creation of an electromagnetic pulse. All you really need for that is a nuclear weapon. You can make it more effective with more gamma rays if you design it that way. It does not have to have a high yield. It can be two, three, four, five kilotons, it doesn't matter. It is not the blast that matters, it is the generation of the gamma rays from space. If that is done, it is a relatively simple task. You don't need heat shields. You don't need accuracy. You are not trying to hit anything on the ground. You are just detonating up there at several hundred kilometers. And that means that that type of capability could be in the hands of the North Koreans, and as the President said a few months ago, even within this year, in the hands of the Iranians.

Now, that is a very different situation than their having to come at us to attack American bases, to engage us where our military forces are or anything like that, or even attack South Korea with American troops helping defend South Korea. To simply put a satellite into orbit at a few hundred kilometers and detonate a simple nuclear weapon is, I am afraid, not that hard if you already have the weapon and you already have the launch vehicle, the ballistic missile. So that is why I talk about North Korea as well. Iran doesn't have a nuclear weapon yet but it may well in relatively short order. So those two countries, especially since they hate us so much, or at least their governments do, and in the case of North Korea, they issue extremely strident statements about destroying the United States. Putting those things together, I take them at their word, they would like to do that, and then we have to find some way to keep them from doing it.

Former Secretary of Defense Bill Perry and current Deputy Secretary of Defense Ashton Carter in the Washington Post back in 2006 urged President Bush not to let the North Koreans test their medium-range missile, which is the same thing that had been used for the launch vehicle, but to attack their launching pad with conventional weapons if they ever hold one of these ballistic missiles out to launch. They have now done that several times, and I think Bill and Ash were right and President Bush was unwise not to follow their advice, and now we are in a situation where both countries have the launch vehicles but only one has a nuclear weapon so far.

Mr. LANCE. Thank you. Admiral McConnell, your thoughts?

Mr. MCCONNELL. On a scale of one to 10, 10 being the best, the best in the world, the Russians and Chinese are probably a seven. The Iranians are probably a four. The issue is, about 80 percent of what is out there is from the Chinese. They have a policy of economic espionage. They have 100,000 just in the military, probably another 100,000 scattered throughout, and they are after economic advantage, competitive advantage. So that is what we are facing.

I didn't mention terrorist groups. On a scale of one to 10, they are pretty low. But the Chinese and others are producing thousands of these malware attack tools. These are exploitation attack. How long is it before some extremist group who wants to change the world order gets their hands on some of these weapons and

then they go after something like a critical infrastructure, for example, the grid.

Mr. LANCE. Thank you. My time is expired. Thank you very much.

Mrs. BLACKBURN. The gentleman yields back. Mr. Doyle for 5 minutes.

Mr. DOYLE. Thank you, Madam Chair, and thank you to all our witnesses here today. It has been very interesting testimony.

Like many of my colleagues on this committee, I have been engaged in this issue for quite some time now, and there are many aspects of this debate that we have weighed in on, most specifically the importance of protecting consumer privacy, but today I want to address the ways we can successfully develop a cybersecurity framework that protects and defends our critical infrastructure while being nimble enough to adapt to new and emerging threats.

I come from Pennsylvania. We have a complex electric and telecommunications distribution network, miles and miles of new natural gas pipeline being built every day and several large nuclear power plants. So protecting our critical infrastructure in my State and across the country is of the utmost urgency.

I can see that everyone here today agrees with the urgency and the seriousness of the task, and as NIST develops its cybersecurity framework, I am hopeful that the testimony at this hearing today will be considered. A lot of that testimony deals with the need for voluntary standards that aren't prescriptive, and while I agree that codifying prescriptive standards this month that could be out of date by next month isn't the best approach. I am not convinced, however, that voluntary incentive-based standards will properly protect our critical infrastructure.

So I mentioned in Pennsylvania, we have several nuclear power plants including the Beaver Valley plant, which sits just outside my district. Now, you are all probably aware that the NRC issued its cybersecurity regulations after September 11. The regulations they developed for nuclear power plants were performance-based standards that once approved were incorporated into a plant's operating license giving it proper enforcement mechanisms.

So I would like to ask Ambassador Woolsey and Admiral McConnell, do you think it makes sense to develop performance-based cybersecurity standards for our critical infrastructure sectors?

Mr. MCCONNELL. I think performance-based standards are what we should strive for. The reason for that is they have to be dynamic. The question will be, how do you get compliance with those standards. So the argument will come down to, do you incentivize industry to allow them to get some reward for following the standards or do you compel it, so that will be the debate that Congress will have to wrestle with.

Mr. DOYLE. Ambassador?

Mr. WOOLSEY. I think that is a good idea, but the problem is, if one expects innovation to come from utilities, it is not where it is going to come from. Just former Deputy Director of the Advanced Research Projects Agency for DOE, ARPA-E, told me about 3 or 4 weeks ago that he had just done the calculation and that the 3,500 utilities in the United States spend less on research and development than the American dog food industry. I don't know what

those totals are. I haven't looked up the dog food industry's total yet. There are some fine institutions, the Edison Electric Institute and so forth, that do some R&D work, but we have not designed our system so that the electric grid demands, takes advantage of or is a mecca for security measures, and something has to drive that and drive it really hard within that framework. If one can figure out a way to use performance-based standards, yes, but if one just hopes that performance is going to be met, I don't see anything that is going to improve the current situation, which I think is really very bad.

Mr. DOYLE. Thank you, Ambassador. Dave?

Mr. MCCURDY. Congressman, thank you. I want to put something in context here, and I have dealt with this issue as well for quit some time, and part of my indoctrination or introduction to the cyber level was in your home district in Pittsburgh. I was on the board of the Software Engineering Institute at Carnegie Mellon, and there, they develop the best practices and understanding of cybersecurity, and it was their CERT, which is now the basis of the U.S. CERT, because the government, when they formed DHS after 2001, you know, used that expertise. It has evolved. In fact, as a founder of the Internet Security Alliance, I was in Tokyo on 9/11 talking to the OECD about the role of board directors and corporate leadership in raising the awareness of the importance of cybersecurity, then we called it Internet security. It has evolved. And even though we can talk about the extreme cases, and it is true, and I spent seven terms across the hall in the Armed Services Committee, which is a lot of conversation that we have gotten into, don't just assume that the worst case here is applying in the cyber arena. First of all, these attacks that occur, a number of them are repelled at the border. We have to assume that many are going to penetrate, but that is why we have also gone to other layers of defense where we have penetration, understanding, detection capability and in mitigation. That is working with this entire array of government agencies and outside contractors, et cetera, that are raising the level of protection. So I just wanted to get that on the record, Madam Chair, because I think we have perhaps gotten a little on one extreme of the severity as opposed to likelihood of occurrence and what actually happens on a daily basis.

Mr. DOYLE. Thank you, Madam Chair.

Mrs. BLACKBURN. Thank you. Dr. Olson for 5 minutes.

Mr. OLSON. I thank the chairwoman, and welcome to our witnesses, and before I ask my questions, I want to let Congressman McCurdy know that the people back home in Texas 22 have the people of Moore, Oklahoma, in our hearts and in our prayers. I know that is your old district. And Mary Fallin, my former colleague, is doing a great job. But if you all need some help, just ask. We will swim across the Red River. God bless the people of Moore, Oklahoma, and everybody impacted by those terrible tornados.

As you know, we are having an energy renaissance right here in America because of new technology: hydraulic fracturing and directional so-called horizontal drilling. The Administration just this last week said the Barnett shale play has twice the oil and gas they thought they had up there just 6 months ago. The Barnett shale play in the Dallas-Fort Worth area is still going strong. The

Permian Basin in West Texas is booming again and the Eagle Ford shale play is off the charts. With all this new energy, thousands of miles of pipelines have to be built including the Keystone XL pipeline that is actually being built right now from Port Arthur to the Port of Houston up to Cushing, Oklahoma, your home State, and with that NASA-like automation of modern pipelines, that makes them safer but obviously it opens them to cyber attacks. So I know that your membership takes these threats seriously. Could you expand on what steps the industry is taking to protect itself from cyber attacks from malicious actors who might attempt to alter the operations of pipelines themselves? What are you doing as an agency or as an association?

Mr. MCCURDY. Well, thank you, Congressman. First of all, safety is the number one priority of our sector, and there are 2.4 million miles of natural gas pipeline in this country, which is the envy of the world, and coincident with the comment I just made to Congressman Doyle, this has to start at the top, the awareness of the importance of cybersecurity. Our current chairman is the CEO of Questar in Utah. He as an engineer was working on cybersecurity issues post 9/11 and has made it very clear that during his term as chairman of AGA, this is a top concern. So we have established not only task forces working, we chair a number of coordinating committees within the framework but also in the oil and gas sector. In fact, Mr. Jibson and Questar, there is a tool that DH uses called CSAT, which is an evaluation tool that takes multiple weeks to actually run to assess your own security, and he not only had that run several times but he also had reported to his board of directors the outcomes so that they could prioritize their investments, and ultimately, it is making sure that the utility commissions that not only regulate but they also approve the rate mechanisms, rate recoveries, understand the importance. So there is a whole panoply of action that is occurring, not only at the technical level—we have technical experts meeting every day—we had FBI walk into us and talk about risks. We had DHS. We have met with DOE, met with NSA. So there is a good, you know, kind of information flow. However, the gist of this hearing is, how do you improve information exchange, and that goes from making sure that the clearances are there for industry and potential protection because of this kind of litigious society that we belong to so that there is a free flow of information and it is relevant and it is timely. When they come to us and they say here is a perceived threat, they have also identified not only the nature of the threat but also some actions that can be taken to mitigate it or defeat it. That is an important flow of information and exchange.

Mr. OLSON. In your opening comments, you said the cybersecurity framework is "headed in the right direction." So my question for you is, headed in the right direction, that is a good thing—that is not a great thing but a good thing. So my question is, what do you hope to see out of this framework and what do you not want to see out of this framework? One on each category.

Mr. MCCURDY. There was a question earlier about are they confident that NIST was going to maintain the voluntary nature, and I think NIST on its own would. We work with NIST and other organizations I have worked with, there are standards developing.

They work with industry. I think given that background and that direction, they will build a consensus and it would be a voluntary set of incentives and guidelines and the like. It is beyond that. So what happens in the Administration that says maybe that is not enough. So in the hands of NIST and the current framework, I think it is a good step.

Mr. OLSON. Thank you. I yield back the balance of my time. Thank you so much, and again, we have the people in Moore, Oklahoma, in our thoughts and prayers. God bless you, sir.

Mrs. BLACKBURN. The gentleman yields back. Mr. Griffith for 5 minutes.

Mr. GRIFFITH. Thank you, Madam Chair. This is a question for Mr. McConnell. Softbank, a Japanese company, has offered to purchase Sprint. My understanding is, the National Security Committee on Foreign Investment in the United States has a review ongoing. Do you have any concerns about placing a major infrastructure provider like Sprint, which has some security issues for our national security, under the control of Softbank?

Mr. MCCONNELL. Yes, I do. If you are in the intelligence business, as I was and some would argue still am, the one thing you would love to do is to run the infrastructure of some other country if you considered them a potential adversary. So having a foreign country own and control the telecommunications industry inside the United States, I would not be in favor of.

Mr. GRIFFITH. All right. I appreciate that.

I do want to get back to, because I found it very interesting, and I am very concerned about the electromagnetic pulse issue, but I do want to give Mr. Highley an opportunity to respond. There have been some comments that the current structure won't work. Do you agree or disagree?

Mr. HIGHLEY. I disagree.

Mr. GRIFFITH. Tell me why.

Mr. HIGHLEY. There is a item called the Electric Subsector Information Sharing and Analysis Center, which is part of NERC, and it was stated earlier that NERC can't respond quickly enough to developing threats, but the whole purpose of this center is to disseminate developing threats as soon as they are released by government or the information sharing work that is done. As soon as they can declassify a threat, whether it is physical or cyber, that is sent out to the utilities, and believe me, we respond when we get those actionable-threat updates. Recently the CFOs met with a number of Cabinet-level officials to discuss threats to the electric system, and EMP was not raised as a top priority, top concern, but I guarantee you that when we are informed of that, we will respond.

Mr. GRIFFITH. But let me say, don't you think that should be a major concern? I mean, we do have two enemies, and of course, then there are natural causes as well that might cause this problem. Don't you think it should have been discussed and shouldn't it be on the list?

Mr. HIGHLEY. Absolutely. It is of great concern.

Mr. GRIFFITH. Let me go back to you, if I might, Ambassador Woolsey, because I do find this very interesting, and in his whole discussion we have talked about launching south. Who else gets af-

fected? Because obviously it is not just going to be the United States if you release that magnetic pulse out there. If you launch south from either Iran or North Korea, what other countries are going to be impacted? I guess what I am asking also is, are they going to be impacted or can they launch it such a way that it doesn't affect them as well?

Mr. WOOLSEY. It depends on the altitude that the detonation occurs at and where it is. The lower the altitude, the less you get of at least one of the three types of electromagnetic pulse effects, because some of the effect is line of sight and others of the effects travel along the transmission lines and so forth. So it is kind of a complicated question. You are probably OK on the other side of the earth from the detonation but it would certainly be the case that if the heart of the United States was taken out of the electric grid by something like this, certainly Canada would be in very serious trouble and the like.

It would also be pretty difficult, I think, although perhaps not impossible to detonate at appropriate altitude to only affect a relatively small country. So I think a better witness on this than me is Peter Pry, who is sitting behind me, who worked on both of the electromagnetic pulse commissions.

Mr. GRIFFITH. Maybe they can steer us to some information that we can look at on that issue.

Mr. WOOLSEY. I would be glad to.

Mr. GRIFFITH. And then you made a comment earlier that it was less likely, understandable because they are our enemies but there was also the threat of the solar-based impulse. Can you explain that a little bit, and when was ht last time we had one strong enough to take out the electric grid?

Mr. WOOLSEY. The huge one was in 1859, and most of the physicists and people who study the sun and work on these things think that the big ones occur about once a century, and we are about 150 years, so we are about 50 years overdue, but these things don't occur with real regularity. There have been several since at a much lower level than the one that occurred in 1859.

Mr. GRIFFITH. Let me stop you there, because another one of my questions that I am interested in is, doesn't that also have impacts on our weather conditions, and what happened in 1859 with the weather?

Mr. WOOLSEY. I don't know that, but solar events of all different kinds including much, much smaller ones than this have substantial effects sometimes on weather and climate. But you need somebody up here who——

Mr. GRIFFITH. I understand. You go on back to what you do know. I appreciate that. And go ahead and tell me some more about what—well, I am out of time anyway. Maybe we can have this discussion another time or at a later date. I appreciate it, Madam Chair, and I yield back.

Mrs. BLACKBURN. The gentleman yields back, and I will remind all of our members that you have 10 business days to submit additional questions. Indeed, as you all can see, there will be some more questions coming your direction, and that would put the deadline for questions at June 5th. I would ask that our witnesses, as patient as you have been with us today, that you please respond

promptly to the questions where a written answer is requested, and without objection, this hearing is adjourned.

[Whereupon, at 1:24 p.m., the Subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. FRED UPTON

Today's hearing continues the Energy & Commerce Committee's oversight of a topic of great national significance—cybersecurity. The committee continues to closely monitor the cybersecurity protection and mitigation efforts of those vital sectors within the committee's jurisdiction, including oil and gas pipelines, the electric grid, nuclear energy, chemical facilities, sewer and water, and telecommunications.

As the nation becomes more reliant on digital communications technology, we also increase our exposure to cyber threats. Indeed, cyber risks to our nation's critical infrastructure have increased significantly in recent years, including multiple high-profile cyber incidents that have confirmed the steady rise in cyberattacks.

But combatting such threats requires a cybersecurity regime that provides ample flexibility to afford owners and operators of critical infrastructure the ability to protect against and respond to rapidly evolving threats. A one-size-fits-all approach to cybersecurity is ill-suited for the diverse range of critical infrastructure sectors, each of which has its own complex characteristics. Owners and operators know best how to protect their own systems, and it is nearly impossible for the speed of bureaucracy to keep pace with ever changing threats.

Undertaking certain reasonable actions in the short-term can have a marked improvement in protecting critical assets. These actions include enhanced information sharing between the federal government and the private sector, greater emphasis on public-private partnerships, and improved cross-sector collaboration. Regarding information sharing, we continue to support Intelligence Committee Chairman Rogers's legislation, which passed the House last month.

I believe that the best approach to improving cybersecurity is for existing regulators to work with industry stakeholders, and for robust information sharing between government and stakeholders. In contrast, I continue to be skeptical of continued calls for a top-down, command-and-control regulatory approach centralized at the Department of Homeland Security or any other federal agency. Along those lines, the committee will continue to monitor with great interest implementation of the President's Executive order on cybersecurity.

# # #

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225-2927
Minority (202) 225-3641

June 10, 2013

Dr. Patrick D. Gallagher
Under Secretary of Commerce for
Standards and Technology
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Dr. Gallagher:

Thank you for appearing before the Committee on Energy and Commerce on Tuesday, May 21, 2013, to testify at the hearing entitled "Cyber Threats and Security Solutions."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Monday, June 24, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Nick.Abraham@mail.house.gov and mailed to Nick Abraham, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Committee.

Sincerely,

Fred Upton
Chairman
Committee on Energy and Commerce

cc: The Honorable Henry A. Waxman, Ranking Member,
Committee on Energy and Commerce

Attachment

QFRs

House Committee on Energy and Commerce

May 21, 2013 Cyber Threats and Security Solutions Hearing

The Honorable John D. Dingell

1. **At the Committee's May 21, 2013 hearing about cybersecurity, you answered in the affirmative on my question about whether the administration should be granted additional statutory authority to address cybersecurity-related risks. Please identify with specificity what additional statutory authority you believe the Administration requires in this regard.**

Answer: The Administration's legislative priorities for the 113th Congress build upon the President's 2011 Cybersecurity Legislative Proposal and take into account two years of public and congressional discourse about how best to improve the nation's cybersecurity.

The Administration is working toward legislation that:

- Facilitates cybersecurity information sharing between the government and the private sector as well as among private sector companies. We believe that such sharing can occur in ways that protect privacy, confidentiality, and civil liberties , reinforce the appropriate roles of civilian and intelligence agencies, and include targeted liability protections while allowing the flexibility needed for firms to continue to innovate as new technologies are developed.

- Incentivizes the adoption of best practices and standards for critical infrastructure by complementing the process set forth under the Executive Order;

- Gives law enforcement the tools to fight crime in the digital age while protecting privacy, confidentiality, and civil liberties;

- Updates Federal agency network security laws, and codifies DHS' cybersecurity responsibilities; and

- Creates a National Data Breach Reporting requirement.

In each of these legislative areas, the right privacy, confidentiality, and civil liberties safeguards must be incorporated. The Administration wants to continue the dialogue with the Congress and stands ready to work with members of Congress to incorporate our core priorities to produce cybersecurity information sharing legislation that addresses these critical issues.

2. **I understand that pursuant to Homeland Security Presidential Directive- 12 (HSPD-12), NIST has finalized reliable identification guidelines for logical and physical access to federal information systems. Does NIST intend to finalize similar guidelines with respect to mobile device registration and credentials? If so, when does NIST expect to finalize such guidelines?**

Answer: NIST is developing draft guidelines for the use of the Personal Identity Verification (PIV) infrastructure to support authentication to mobile devices such as smart phones and tablets. The guidelines maximize the USG investment in the PIV infrastructure and adapt PIV credentials for these mobile devices. NIST expects to release the draft guidelines for public comment during the 4th Quarter of Fiscal Year 2013.

The Honorable Anna G. Eshoo

1. **If you could ask Congress to address one unfinished piece of business relative to cybersecurity, what would it be?**

Answer: The Administration's current legislative priorities build upon the President's 2011 Cybersecurity Legislative Proposal and subsequent public and congressional discourse about how best to improve the nation's cybersecurity. The Administration stands ready to work with members of Congress toward legislation that facilitates cybersecurity information sharing in a manner that protects privacy, confidentiality, and civil liberties, reinforces the appropriate roles of civilian and intelligence agencies, and includes targeted liability protections. Such legislation should incentivize the adoption of best practices and standards for critical infrastructure by complementing the process set forth under the Executive Order. It should also update Federal agency network security laws, codify DHS' cybersecurity responsibilities, create a National Data Breach Reporting requirement, and give law

enforcement the tools to fight crime in the digital age. In each of these legislative areas, the right privacy, confidentiality, and civil liberties safeguards must be incorporated.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

June 10, 2013

The Honorable Dave McCurdy
President and CEO
American Gas Association
400 North Capitol Street, N.W.
Washington, D.C. 20001

Dear Congressman McCurdy:

Thank you for appearing before the Committee on Energy and Commerce on Tuesday, May 21, 2013, to testify at the hearing entitled "Cyber Threats and Security Solutions."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Monday, June 24, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Nick.Abraham@mail.house.gov and mailed to Nick Abraham, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Committee.

Sincerely,

Fred Upton
Chairman
Committee on Energy and Commerce

cc: The Honorable Henry A. Waxman, Ranking Member,
Committee on Energy and Commerce

Attachment

Dave McCurdy
President and CEO
American Gas Association

House Committee on Energy & Commerce Hearing
"Cyber Threats and Security Solutions" (May 21, 2013)

Response to Additional Question for the Hearing Record

The Honorable Anna G. Eshoo: If you could ask Congress to address one unfinished piece of business relative to cybersecurity, what would it be?

The American Gas Association (AGA) believes that there is a role for cybersecurity legislation, particularly as it relates to improving public-private cybersecurity information sharing and related liability protections. Passing legislation that addresses both policy areas is of paramount concern.

To help counter cyberattacks and protect networks against future incursions, critical infrastructure, including natural gas utilities, needs government to help them identify, block and/or eliminate cyberthreats as rapidly and reliably as possible. From a functional perspective, this will require streamlining the process by which actionable threat intelligence is shared with private industry. Harnessing the cybersecurity capabilities of the government intelligence community on behalf of private sector networks will go a long way towards overall network security. The recently passed H.R. 624, *The Cyber Intelligence Sharing and Protection Act* (CISPA) provides a positive roadmap by establishing a cybersecurity partnership between critical infrastructure and the defense/intelligence community and DHS to distribute cyberthreat information, interpret and share potential threat impacts, and work with critical infrastructure to keep their networks safe. We hope that the Senate will move forward with the CISPA concept to improve our chances of getting a cybersecurity information sharing bill enacted into law.

Another avenue for legislation surrounds offering liability protection for companies with robust cybersecurity programs – standards, products, processes, etc. The Administration's recent executive order (EO) on cybersecurity underscores this need. The EO directs sector agencies, and the intelligence and law enforcement community to establish a cybersecurity information sharing partnership; tasks the National Institute of Standards and Technology with establishing a quasi-regulatory set of cybersecurity standards (a "cybersecurity framework"); and orders DHS to incentivize critical infrastructure to adhere to the NIST standards. What the EO cannot do is provide liability protections for critical infrastructure entities that make the effort to participate in a public-private cybersecurity program, regardless of whether it is created via EO or some future law.

AGA supports employing the *SAFETY Act* as an appropriate avenue for providing companies that participate in a government-private industry cybersecurity partnership with liability coverage from the impacts of cyberterrorism. *SAFETY Act* applicability in this area is plain:

- The SAFETY *Act* exists in current law, and a related office at DHS has been reviewing and approving applications for liability coverage in the event of an act of terrorism or cyber attack for over a decade. This office utilizes an existing review and approval process which would allow for immediate granting of liability protections from cyber attacks.
  - Because the *SAFETY Act* can apply to a variety of areas ranging from cybersecurity standards (cyber best practices, etc.), to procurement practices and related equipment (SCADA, software, firewalls, etc.) companies can layer their liability protection.
  - We are aware of no other existing statute that offers similar liability protections. Moreover, we do not see the need to write new law to address liability protections from cyber incidents when the *SAFETY Act* is already applicable.

This said, there are some areas where we believe the *SAFETY Act* could be a little stronger as it applies to cyber matters. First, and foremost, the statute could be expanded to make specific reference to liability protections from "cyber" events (cyber attacks, cyber terrorism, etc.) and more specific reference to coverage for cybersecurity equipment, policies, information sharing programs, and procedures. While there is coverage under the Act currently for cyber attacks, specifically identifying "cyber attacks" as a trigger for liability protections would strengthen the overall concept.

Congresswoman Eshoo, we hope that our response to your inquiry is sufficient and substantive. If you have any additional questions about our industry's cybersecurity priorities and activities, please contact Brian Caudill (bcaudill@aga.org), AGA's Senior Director of Federal Affairs at 202-824-7029.

400 N. Capitol St. NW 4th Floor, Washington, DC, 20001 P: 202-824-7029 F: 202-824-7092 E: bcaudill@aga.org www.aga.org

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

June 10, 2013

Mr. John M. McConnell
Vice Chairman
Booz Allen Hamilton
13200 Woodland Park Road
Herndon, VA 20171

Dear Mr. McConnell:

Thank you for appearing before the Committee on Energy and Commerce on Tuesday, May 21, 2013, to testify at the hearing entitled "Cyber Threats and Security Solutions."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Monday, June 24, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Nick.Abraham@mail.house.gov and mailed to Nick Abraham, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Committee.

Sincerely,

Fred Upton
Chairman
Committee on Energy and Commerce

cc: The Honorable Henry A. Waxman, Ranking Member,
Committee on Energy and Commerce

Attachment

Honorable Anna G. Eshoo

If you could ask Congress to address one unfinished piece of business relative to cybersecurity, what would it be?

Answer: Comprehensive cybersecurity legislation that provides a legal framework for the nation to effectively address, across all departments of government and the private sector, the increasing cyber threats that are directed against the country and that probably will lead to a catastrophic event(s) for the nation.

Rationale: Today the nation suffers from increasing exploitation from criminal, hacktivist, nation-state, and terrorist groups directed against government and private sector critical infrastructures and business interests. In addition, nation-states are conducting cyber economic espionage against the U.S. to obtain business plans, source code, innovation, research and development and other valuable intellectual property for competitive advantage over the country. In time, some nation state or terrorist group will use the 1000's of malware attack tools generated annually by nation states in preparation for potential cyber-war for a destructive attack against the U.S. Examples include attacks to degrade or destroy liquidity and confidence in the global banking system, electric power distribution or mass transportation. We have the capabilities to slow down or halt such exploitation or direct attacks, however, we do have the legal framework in place that allows and, in fact, requires the needed collaboration and sharing of sensitive information from government to the private sector, between private sector entities and from the private sector to government. There were many bills and amendments proposed in the Congress last year. None of them were successful in passing both Houses of the Congress for signature by the President. This failure leaves the U.S. vulnerable as we become increasing digitally dependent.

Mike McConnell

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

June 10, 2013

Ambassador R. James Woolsey
Chairman, Woolsey Partners LLC
Former Director of the
Central Intelligence Agency
P.O. Box 1434
Great Falls, VA 22066

Dear Ambassador Woolsey:

Thank you for appearing before the Committee on Energy and Commerce on Tuesday, May 21, 2013, to testify at the hearing entitled "Cyber Threats and Security Solutions."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Monday, June 24, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Nick.Abraham@mail.house.gov and mailed to Nick Abraham, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Committee.

Sincerely,

Fred Upton
Chairman
Committee on Energy and Commerce

cc: The Honorable Henry A. Waxman, Ranking Member,
Committee on Energy and Commerce

Attachment

Question from The Honorable Anna G. Eshoo

If you could ask Congress to address one unfinished piece of business relative to cybersecurity, what would it be?

Response:

Because of the extreme danger caused by our electric grid's vulnearbility to electro-magnetic pulse (EMP) and because the North Koreans have detonated 3 nuclear weapons and successfully launched a satellite, I believe that a adopting a policy of destroying any North Korean missile or launch-vehicle prior to launch is essential (see my Wall Street Journal op ed of May 20, 2013, attached). It should be noted that the North Koreans, Iranians, Russians, and Chinese all regard electro-magnetic pulse as part of their cyber arsenal.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 227–2927
Minority (202) 225–3641

June 10, 2013

Dr. Michael Papay
Vice President and
Chief Information Security Officer
Northrop Grumman Information Systems
7575 Colshire Drive
McLean, VA 22102

Dear Dr. Papay:

Thank you for appearing before the Committee on Energy and Commerce on Tuesday, May 21, 2013, to testify at the hearing entitled "Cyber Threats and Security Solutions."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Monday, June 24, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Nick.Abraham@mail.house.gov and mailed to Nick Abraham, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Committee.

Sincerely,

Fred Upton
Chairman
Committee on Energy and Commerce

cc: The Honorable Henry A. Waxman, Ranking Member,
Committee on Energy and Commerce

Attachment

House Energy & Commerce Committee Hearing:
"Cyber Threats and Security Solutions"
10:00 am, May 21, 2013

Questions for the Record
Dr. Michael Papay
Chief Information Security Officer &
Vice- President, Cybersecurity Initiatives,
Northrop Grumman

The Honorable Anna G. Eshoo

1) **With our nation's need for cybersecurity talent growing every day, what can this Committee or Congress do to expand the pipeline of highly qualified candidates for cyber jobs?**

   The need for a well-trained and qualified cyber workforce is not only critical to our national security but also our global competitiveness. I urge Congress to support programs aimed at encouraging students to pursue careers in the Science, Technology, Engineering and Mathematics (STEM) disciplines. It is essential for all cyber stakeholders across government, industry, and academia to dedicate the resources needed to building a robust high-tech cyber workforce for the future.

   According to a 2010 U.S. Department of Commerce study, the number of STEM jobs is expected to grow 17% in the next decade. I was privileged to serve on the 2012 Homeland Security Advisory Council's Task Force on CyberSkills. This Council focused on identifying far-reaching improvements that would enable the Department of Homeland Security (DHS) to recruit and retain the cybersecurity talent it needs. One of the council's recommended objectives was to radically expand the pipeline of highly qualified candidates for cyber jobs through innovative partnerships with community colleges, universities, organizers of cyber competitions, and other federal agencies. Another important effort focused on this issue is the National Initiative for Cybersecurity Education (NICE). The National Institute of Standards and Technology (NIST) is leading the NICE initiative, including more than 20 federal departments and agencies, to ensure coordination, cooperation, focus, public engagement, technology transfer and sustainability. The goal of NICE is to establish an operational, sustainable and continually improving cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security. It includes not only the federal workplace, but also civilians and students in kindergarten through post-graduate school.

   Northrop Grumman considers a well-trained cyber workforce a priority for both for our nation and our company, which is why we have sponsored the nation's first ever cybersecurity honors program at the University of Maryland-College Park. We are also focusing our educational efforts on middle and high school students as the presenting sponsor of the CyberPatriot program, which this year hosted over 1,200 teams, representing approximately 7,500 students, from all 50 states, and Department of Defense schools in Europe and the Pacific.

2) **If you could ask Congress to address one unfinished piece of business relative to cybersecurity, what would it be?**
   Cyber threats are rapidly evolving while simultaneously becoming more difficult to detect and increasingly ominous. Furthermore, cyber attackers are currently able to take advantage of siloed networks by launching similar attacks time after time. The most effective step that Congress could take

to raise the nation's overall level of cybersecurity is to facilitate and encourage companies to secure their own networks and break down the barriers to sharing cyber threat information.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

June 10, 2013

Mr. Charles Blauner
Global Head of Information Security
Citigroup, Inc.
399 Park Avenue
New York, NY 10043

Dear Mr. Blauner:

Thank you for appearing before the Committee on Energy and Commerce on Tuesday, May 21, 2013, to testify at the hearing entitled "Cyber Threats and Security Solutions."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Monday, June 24, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Nick.Abraham@mail.house.gov and mailed to Nick Abraham, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Committee.

Sincerely,

Fred Upton
Chairman
Committee on Energy and Commerce

cc: The Honorable Henry A. Waxman, Ranking Member,
Committee on Energy and Commerce

Attachment

Dear Representative Eshoo

It was my pleasure to testify, on May 21, before the House Subcommittee on Financial Institutions & Consumer Credit regarding protecting our nation from the cybersecurity threats we face. You asked, in a question subsequent to that testimony: "If you could ask Congress to address one unfinished piece of business relative to cybersecurity, what would it be?"

I believe, consistent with the attached letter from the American Bankers Association, the Financial Services Roundtable, and the Securities and Financial Markets Association to Senators Feinstein and Chambliss, that it is vitally important Congress pass legislative clarifying the ability of the public and private sector to share vital cyber threat information. As stated in the letter, while the financial services sector has done much to enhance information sharing, "This progress, however, is ultimately inadequate without Congressional action to enhance, facilitate, and protect threat information sharing across sectors and with government."

The financial sector therefore supports efforts to develop legislation that further strengthens the ability of the private sector and the Federal government to work together to develop a more effective information sharing framework to respond to cyber threats, providing liability protection while balancing the need for privacy protection. Such legislation must acknowledge and enhance existing relationships to leverage the experience of existing information sharing programs.

I would be happy to answer any further questions you may have about this important issue.

Charles Blauner
Chair – Financial Services Sector Coordinating Council

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

June 10, 2013

Mr. Duane Highley
President and CEO
Arkansas Electric Cooperative Corporation
1 Cooperative Way
Little Rock, AR 72209

Dear Mr. Highley:

Thank you for appearing before the Committee on Energy and Commerce on Tuesday, May 21, 2013, to testify at the hearing entitled "Cyber Threats and Security Solutions."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Monday, June 24, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Nick.Abraham@mail.house.gov and mailed to Nick Abraham, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Committee.

Sincerely,

Fred Upton
Chairman
Committee on Energy and Commerce

cc: The Honorable Henry A. Waxman, Ranking Member,
Committee on Energy and Commerce

Attachment

Question for the Record, in connection with May 21, 2013 full Committee hearing
Submitted by NRECA on behalf of Duane Highley

Question posed by: Rep. Anna G. Eshoo

Question: **If you could ask Congress to address one unfinished piece of business relative to cybersecurity, what would it be?**

Response:

Thank you for your question. If we could ask Congress to pick up the ball and get it into the touchdown zone on one component of cybersecurity legislation, it would be information sharing. That phrase gets over-used to the point it has lost its meaning, but still, as a representative of a privately-owned business that owns and operates critical assets in the Bulk Electric System, I can tell you that we aren't yet to the point where there is "real-time collaboration" among government and industry. We want and need to get there but it will take building trust, collaboration, many conversations, and more clearances.

The risks and potential impacts are very different for public-facing elements of a utility's Internet-connected business systems, versus their industrial control systems, which typically are not Internet-connected, or if they are, they are protected with more aggressive security schemes. Given that millions of attempted cyber-attacks occur daily on our public facing sites, utilities will need to rely upon assistance from governmental authorities, particularly in the form of helping to identify threats as well as threat trends.

Much of the information needed to fully understand the nature of the cyber threats faced by our industry is classified at a level that is unavailable to our organizations. The DHS Private Sector Clearance Program (PSCP) has helped key electric utility staff obtain security clearances, which allow them access to basic information about such threats. However, a recent shutdown of the PSCP created a substantial backlog in the processing of clearance applications, and hampered the industry's access to important information. Processing of these applications has now resumed and we hope we can continue to expand our access to needed information. We also need a limited number of electric industry personnel to obtain top-secret "SCI" clearances, which are not typically provided by the PSCP; this would help immensely in achieving "real-time collaboration."

In addition to expanding the number of utility personnel with clearances, it is critical that government agencies regularly share clear, actionable information with industry personnel in cleared briefings. Our employees can be counted on to take the steps necessary to protect our systems – if they understand the nature of the threat against them. Effective information sharing should take the form of a timely and efficient mechanism to pass along threat data, warnings, and trend information. Examples of the kinds of information we need are: signatures of known viruses and malware; points of origination for known threat actors; known behavioral techniques of anonymous threats such as "Advanced Persistent Threats" (APT); information regarding potential vectors for introduction of cyber threats, such as counterfeit parts and software; and the sharing of best practices or policies to combat or defeat emerging threats and vulnerabilities.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

June 10, 2013

Mr. Robert Mayer
Vice President for Industry
and State Affairs
United States Telecom Association
607 14th Street, N.W., Suite 400
Washington, D.C. 20005

Dear Mr. Mayer:

Thank you for appearing before the Committee on Energy and Commerce on Tuesday, May 21, 2013, to testify at the hearing entitled "Cyber Threats and Security Solutions."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Monday, June 24, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Nick.Abraham@mail.house.gov and mailed to Nick Abraham, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Committee.

Sincerely,

Fred Upton
Chairman
Committee on Energy and Commerce

cc: The Honorable Henry A. Waxman, Ranking Member,
Committee on Energy and Commerce

Attachment

The Honorable Anna G. Eshoo

1. If you could ask Congress to address one unfinished piece of business relative to cybersecurity, what would it be?

Response:

The single most important step that can be taken to enhance both the government's and the private sector's cybersecurity posture is to give our companies' security personnel access to real-time, actionable cyber threat information by amending the current legal framework concerning the collection, use, and sharing of information. The current framework remains a substantial barrier to effective communication between and among all relevant public and private stakeholders. Neither private sector companies nor the federal government can or will share cyber threat information with each other in real time – in other words, in time to avert the real threat at hand – until they are appropriately permitted by law to do so, and are protected from the potential threat of class actions, criminal prosecutions, administrative enforcement proceedings, regulatory rulemakings, or other similar legal liabilities.

USTelecom notes that addressing this critical need is urgent, and is unrelated to the recent reports and reaction to the National Security Agency's (NSA) alleged surveillance programs. There is a clear difference between what the NSA is reported to have done and the critical need of our industry for a voluntary process that will allow our companies to protect our networks and customers from cyber attacks – including malware, viruses, denial of service attacks, exfiltration of intellectual property, and other threats – through the ability to share information in real time or near-real time among other companies, and with appropriate government agencies. Thus, regardless of whether Congress chooses to amend the Patriot Act or the Foreign Intelligence Surveillance Act (FISA) in response to the NSA programs currently under review, the fact remains that cybersecurity information-sharing legislation that provides necessary liability protections while also containing appropriate privacy and civil liberties provisions should be passed by Congress as soon as possible.