This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

{York Stenographic Services, Inc.}

RPTS MEYERS

HIF141.000

``CYBER THREATS AND SECURITY SOLUTIONS''

TUESDAY, MAY 21, 2013

House of Representatives,

Committee on Energy and Commerce

Washington, D.C.

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,

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 of our witnesses' thoughtful answers to our questions this morning.

[The prepared statement of Mrs. Blackburn follows:]

********** COMMITTEE INSERT **********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

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.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

[The prepared statement of Mr. Waxman follows:]

********** COMMITTEE INSERT **********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

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

} Mr. {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, and 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,

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 work mark the

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

forward to answering any questions you may have.

[The prepared statement of Mr. Gallagher follows:]

********** INSERT 1 **********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

Mrs. {Blackburn.} Thank you. The gentleman yields back, ran a little bit over time there but that is okay. 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?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 that we would 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?

Mr. {Gallagher.} So the Executive Order serves to basically align roles and responsibilities across the

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 be come 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {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?

Mr. {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?

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. {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 protect 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

gap in authority, does it?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {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?

Mr. {Gallagher.} Yes, they already are.

Mr. {Walden.} And obviously, flexibility is critical in engaging the private sector to respond to the very rapid

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {Gallagher.} So I think the tension between, you know, 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

Mr. {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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

Mr. {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.

Mr. {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.

Mr. {Gallagher.} Yes.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

Mr. {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.

Mr. {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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. {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.

Mr. {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?

Mr. {Gallagher.} I would certainly anticipate this will

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Rogers, you are recognized, and you waive. Okay. 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.

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

you consider to be critical infrastructure, number one?

Mr. {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, you know, 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.

Mr. {Gallagher.} So I think from our view, you know, 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. {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?

Mr. {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.

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

Dr. {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?

Mr. {Gallagher.} So while remembering, in the United

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

States, NIST does not write the standards. So 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.

Dr. {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?

Mr. {Gallagher.} That is correct. We think of

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

Dr. {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?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

help facilitate, provide some clarity, particularly in this area.

Dr. {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?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 quite muscular, 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

determine adherence to the framework, and will they take into consideration the sensitive information that different companies and plants may provide?

Mr. {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 shows them the pros and cons of these different models, but what it allows is, 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {Gallagher.} Not to me, but you are not the first

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {Gallagher.} So in my experience, what I have learned in this where 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 in this case protect those sectors. On the other hand, you don't want it 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

you are developing at NIST. What types of incentives are you talking about?

Mr. {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 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 to 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 know, you have got an agreement. You know that there is 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?

Mr. {Gallagher.} At this time NIST does not but what I can share with you is some 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

of what we are talking about here.

Mr. {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, and 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?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 practice 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?

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mr. {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 performance. 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?

Mr. {Gallagher.} Yes.

Mr. {McNerney.} It would be hard not to because--

Mr. {Gallagher.} I would hope they do, actually. One

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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, and 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, that becomes really 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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {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, and in that, 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 appropriate 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 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?

Mr. {Gallagher.} So what we are seeing in the RFI process includes a broad range of incentives. Some would

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {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, you know, for somebody who has made that decision, can they get the appropriate education and workforce-specific training where they can contribute by the

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.} Okay. 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?

Mr. {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 baseline that is 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.} Okay. That is good.

Mr. {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.} Okay. 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?

Mr. {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-

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

performing sectors, put their practices on the table as best practices for consideration under the framework.

Ms. {Matsui.} Okay. 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?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

are operating that equipment or holding my data or running my applications. 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 straightforward 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.} Okay. 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

Mr. {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?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {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 industry 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.

Mr. {Gallagher.} One of the great things we don't have to worry about here is the companies not being behind this.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 was 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {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 that 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 enables 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, and in

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 related to information sharing in the sense that that 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 and 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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {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?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 don't have challenges, and what are the challenges that this framework faces and what are some of the challenges that NIST faces?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

Mr. {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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

^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 CHIE 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

} 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 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-sharing 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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,

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

[The prepared statement of Mr. McCurdy follows:]

********** INSERT 2 **********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

Mrs. {Blackburn.} Thank you.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

^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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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:]

********** INSERT 3 **********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mrs. {Blackburn.} Thank you, Mr. McConnell.

Ambassador Woolsey, you are recognized for 5 minutes.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

^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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 4 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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:]

********** INSERT 4 **********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mrs. {Blackburn.} And thank you.

Dr. Papay for 5 minutes.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

^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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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. 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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:]

********** INSERT 5 **********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mrs. {Blackburn.} Thank you, Dr. Papay.

Dr. Schneck, you are recognized for 5 minutes.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

^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 February of 2011

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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,

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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:]

********** INSERT 6 **********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mrs. {Blackburn.} Thank you.

Mr. Blauner for 5 minutes.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

^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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 s top priority for banks and other financial services companies. We have invested an

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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:]

********** INSERT 7 **********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mrs. {Blackburn.} We thank you.

Mr. Highley, you are recognized for 5 minutes.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

^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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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:]

********** INSERT 8 **********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Mrs. {Blackburn.} Thank you.

Mr. Mayer.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

^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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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,

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 it 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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:]

********** INSERT 9 **********

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

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.} Okay. 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.} Okay. 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.} Okay. 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? Okay. 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

should inform a lot in this process.

Mrs. {Blackburn.} Okay. So you kind of match up with Mr. Mayer on the concerns?

Mr. {McCurdy.} Yes.

Mrs. {Blackburn.} Okay. 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.} Okay. 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.} Okay. 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.} Okay. 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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 f 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 toto 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 okay. 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

want to be able to share more with the community without fearing we will get hurt.

Mr. {McNerney.} Okay. 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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, an 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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,

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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?

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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. Obviously, the greater the footprint, the different customers that are

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 if 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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,

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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 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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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, the 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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,

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

and in his whole discussion we have talked about launching south. Who else gets affected? 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 okay 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

only affect 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

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

[Whereupon, at 1:24 p.m., the Subcommittee was adjourned.]