OVERSIGHT OF EXECUTIVE ORDER 13636 AND DEVELOPMENT OF THE CYBERSECURITY FRAMEWORK

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

JULY 18, 2013

Serial No. 113–27

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

86–034 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan, *Vice Chair*
PATRICK MEEHAN, Pennsylvania
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
JASON CHAFFETZ, Utah
STEVEN M. PALAZZO, Mississippi
LOU BARLETTA, Pennsylvania
CHRIS STEWART, Utah
RICHARD HUDSON, North Carolina
STEVE DAINES, Montana
SUSAN W. BROOKS, Indiana
SCOTT PERRY, Pennsylvania
MARK SANFORD, South Carolina
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
YVETTE D. CLARKE, New York
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
RON BARBER, Arizona
DONDALD M. PAYNE, JR., New Jersey
BETO O'ROURKE, Texas
TULSI GABBARD, Hawaii
FILEMON VELA, Texas
STEVEN A. HORSFORD, Nevada
ERIC SWALWELL, California

GREG HILL, *Chief of Staff*
MICHAEL GEFFROY, *Deputy Chief of Staff/Chief Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

PATRICK MEEHAN, Pennsylvania, *Chairman*

MIKE ROGERS, Alabama
TOM MARINO, Pennsylvania
JASON CHAFFETZ, Utah
STEVE DAINES, Montana
SCOTT PERRY, Pennsylvania
MICHAEL T. MCCAUL, Texas *(ex officio)*
YVETTE D. CLARKE, New York
WILLIAM R. KEATING, Massachusetts
FILEMON VELA, Texas
STEVEN A. HORSFORD, Nevada
BENNIE G. THOMPSON, Mississippi *(ex officio)*

ALEX MANNING, *Subcommittee Staff Director*
DENNIS TERRY, *Subcommittee Clerk*

CONTENTS

OVERSIGHT OF EXECUTIVE ORDER 13636 AND DEVELOPMENT OF THE CYBERSECURITY FRAMEWORK

Thursday, July 18, 2013

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES,
Washington, DC.

The subcommittee met, pursuant to call, at 10:05 a.m., in Room 311, Cannon House Office Building, Hon. Patrick Meehan [Chairman of the subcommittee] presiding.

Present: Representatives Meehan, Marino, Clarke, Keating, and Vela.

Mr. MEEHAN. The Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order.

Subcommittee is meeting today to examine the implementation of Executive Order 13636 and the administration's cybersecurity framework, and I recognize myself now for an opening statement.

I would like to welcome everybody to today's hearing, which continues our subcommittee's efforts to provide oversight over the President's Cybersecurity Executive Order 13636. The focus of the Executive Order is to provide protection for our Nation's critical infrastructure sectors from cyber threats. These sectors include our energy and nuclear facilities, our Nation's transportation systems, our defense industrial base, and financial services, among others.

Today we will focus on the cybersecurity framework, under which the National Institute for Standards and Technology or NIST, as it is often referred to, has the responsibility of working with stakeholders to develop.

The framework is expected to be completed and released by October 30. On July 1, NIST released an outline of that framework, which will be the basis of the committee's questioning today.

So far NIST has held three workshops to gather input from industry, academia, other stakeholders, and a fourth is expected in September, I believe, in Dallas, Texes.

I believe that the outline of NIST's framework provides an important step to increasing our Nation's awareness and ability to protect our networks from crippling cyber attacks.

In fact, I believe that the three are many mature actors in both Government and the private sector working in great coordination

currently—including those at the Department of Homeland Security—to shield our systems from cyber threats.

It is, however, those outliers—the ones without the awareness, those with insufficient resources—who can present immense vulnerabilities to entire networks.

It is this concern that our subcommittee seems to have allayed. We must find answers to the question of: How do we incentivize participation without creating counterproductive, onerous standards and regulations?

Adopting the NIST framework would result in a positive exercise for owners and operators of critical infrastructure. However, I have concerns that a self-assessment may not be sufficient to incentivize action to bolster cyber defenses in all cases.

Our committee has held over 200 meetings with stakeholders and one of the common themes emanating from the discussions is that they are only as strong as their weakest links. I believe an analysis of the incentives included in this framework is in order.

I look forward to hearing from the panel today on ways we can assist both the public and private sector to increase their hygiene with limited resources.

Providing incentives for organizations to share information and best practices is further complicated by the absence of liability protections. In the Executive Order, our goal should be to encourage that information sharing, and I have questions about the ability of regulators to reform use—require use of the framework, turning this into burdensome check-the-box rules and regulations.

Ultimately, I believe it is the consensus of the committee that Congress must pass legislation in order to address many of these outstanding issues.

Existing structures within DHS must be authorized by Congress to continue functioning. Liability protections, information-sharing provisions, and industry-led incentives can only be fully enacted by statute, not exclusively by Presidential Directive.

I look forward to working with the committee, with our panel, and DHS to craft legislation that will address these issues.

I thank the panel for their participation today, and I look forward to hearing from your testimony.

[The information follows:]

DHS Incentives Study: Preliminary Analysis and Findings

Executive Order 13636 on Improving Critical Infrastructure Cybersecurity

Tony Cheesebrough
Chief Economist
Integrated Task Force

May 21, 2013

Homeland Security

Cybersecurity Incentives Study

- Though the EO requires separate studies from DHS, Treasury, and Commerce, the DHS Integrated Task Force (ITF) has been working collaboratively with these partners to share data, research, and analysis to produce its study
- The White House Council of Economic Advisors, Treasury Tax Policy and Insurance Policy Offices, and Homeland Security Studies and Analysis Institute each provided focused secondary research support
- The Department of Commerce has also made available its Notice of Inquiry (NOI) responses

Final List of Incentives Considered

Initial Incentive Category		Final Incentive Category
1 Expedited Security Clearance Process	→	Remove due to existing DHS efforts
2 Grants		No Change
3 Include Cybersecurity in Rate Base	→	"Include Cybersecurity in Rate Base for Price-Regulated Industries"
4 Information Sharing	→	Remove due to EO Section 4
5 Insurance	→	Remove as independent category and include in Cyber SECURITY Act
6 Liability Considerations and Legal Benefits	→	Remove as independent category and include in Cyber SECURITY Act
7 New Regulation/ Legislation (e.g. Cyber SAFETY Act)	→	Limit to "Cyber SECURITY Act (new legislation composed of insurance requirements, liability protections, and legal benefits)"
8 Prioritized Technical Assistance		No Change
9 Procurement Considerations		No Change
10 Public Recognition		No Change
11 Security Disclosure		No Change
12 Streamline Information Security Regulations		No Change
13 Subsidies		No Change
14 Tax Incentives		No Change

Homeland Security

3

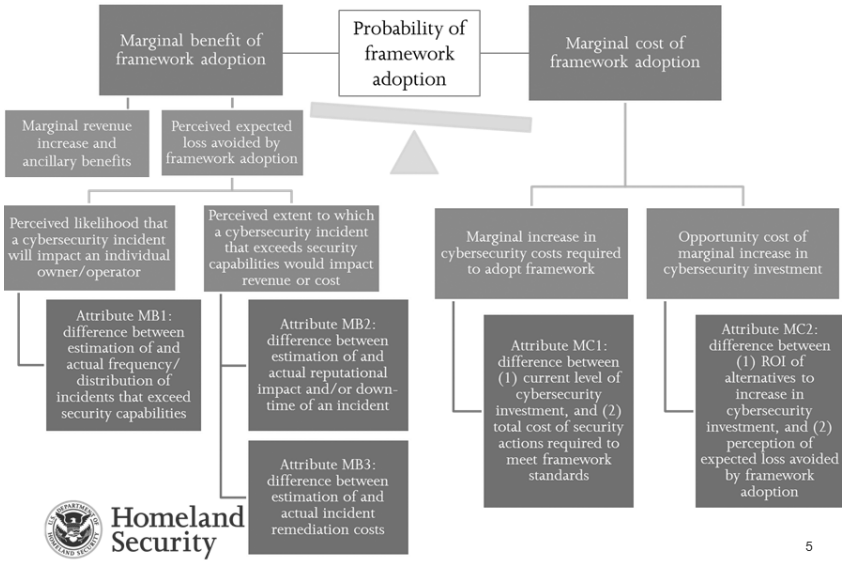
Research Methodology

- Definition. For the purpose of this study, DHS will use the following definition of incentive: a cost or benefit that motivates a decision or action by critical infrastructure asset owners/operators to adopt the cybersecurity framework under development by NIST.
- Central Researchable Question. To what extent would each of the incentives under consideration affect the probability that critical infrastructure asset owners/operators will adopt the cybersecurity framework under development by NIST?
- Basic Methodology. Without better data, a basis for quantitative estimates of the benefits of cybersecurity incentives is lacking, and until the EO-required framework is developed by NIST, the same is largely true of the costs of implementing the framework.
  - As a result, the methodology for analyzing the effectiveness of the cybersecurity incentives under evaluation for the EO relied on evaluations of voluntary non-cybersecurity programs and largely qualitative methods.
  - Evaluations of incentives applied to voluntary non-cybersecurity programs are assumed to be relevant to the study of voluntary cybersecurity programs, though identical results were not assumed.
- Information Sources.
  - Literature review completed with research support from the Council of Economic Advisers, Treasury Tax Policy and Insurance Policy Offices, and Homeland Security Institute, yielding 138 peer-reviewed journal articles, law review articles, conference papers, working papers, government reports, dissertations, and book chapters.
  - DHS/ITF Incentives Workshop: completed April 19, 2013
  - U.S. Department of Commerce Notice of Inquiry (NOI): completed review of 43 comments

Homeland Security

4

Microeconomic Framework



Homeland Security

5

Economic Criteria for Analysis

- Effectiveness: does it work?
  - Effectiveness is the probability of framework adoption and is principally driven by framework cost sharing, though expected loss avoidance, marginal revenue increase, and ancillary benefits also contribute to a lesser extent.
- Efficiency: is there waste?
  - Efficiency applies to cost sharing incentives, and consists of both:
    - Moral hazard, which in this context exists because of differences in the degree to which techniques for adopting the framework are cost-effective, and can be thought of as allowing owners/operators to choose techniques that are not cost-effective; and
    - Adverse selection, which in this context exists due to differences in the cost of adoption among owners/operators within and across sectors, and can be thought of as over-paying "lost cost" owners/operators which are already near the frontier of sophistication.
- Equity: who pays and how much?
  - Government, industry, or consumers; all/most, moderate, or none/little.

Homeland Security

6

Preliminary Analysis

	Incentive	Effectiveness				Efficiency		Equity		
		Probability of Framework Adoption	Framework Cost Sharing	Expected Loss Avoided	Marginal Revenue Increase and Ancillary Benefits	Moral Hazard	Adverse Selection	Government/ Taxpayer Cost	Industry Cost	Consumer Cost
1	Grants to Non Price-Regulated Industries	●	●			●	●		●	●
2	Include Cybersecurity in Rate Base for Price-Regulated Industries	●	●			●	●	●	●	
3	Cyber SECURITY Act (composed of insurance requirements, liability protections, and legal benefits)	○		●				○	○	○
4	Prioritized Technical Assistance			○				●		●
5	Procurement Considerations	○			●			●		○
6	Public Recognition							○		●
7	Security Disclosure							○		○
8	Streamline Information Security Regulations				○			●		●
9	Subsidies	○	○				●		●	●
10	Tax Incentives	○	○				●		●	●

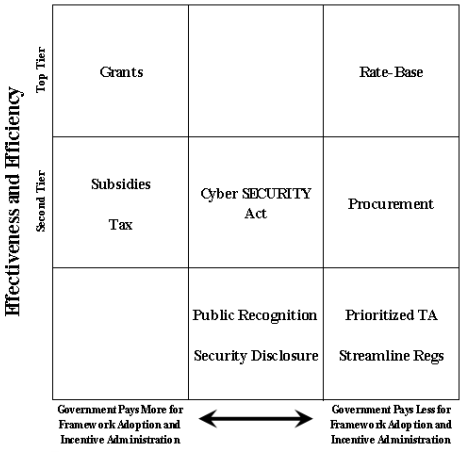
Key

●	Indicates a top tier incentive, relative to other incentives, against the criteria defined *within* each column.
○	Indicates a second tier incentive, relative to other incentives, against the criteria defined *within* each column.
	Indicates neither a top tier nor a second tier incentive, relative to other incentives, against the criteria defined *within* each column.
	Indicates the criteria was not applied to the incentive

Homeland Security

7

Preliminary Findings



- Grants: most effective and efficient with little industry cost but highest government cost
- Include Cybersecurity in Rate Base for Price-Regulated Industries: most effective and efficient with little government and industry cost but highest consumer cost
- New Cyber SECURITY Act (insurance requirements, liability protections, and legal benefits): moderate effectiveness with moderate government cost
- Prioritized Technical Assistance: moderate expected loss avoidance with little government cost
- Procurement Considerations: moderate effectiveness for little government cost
- Public Recognition: little evidence of effectiveness independent of procurement requirements and potential for unintended consequences such as cyber targeting
- Security Disclosure: little evidence of effectiveness and potential for unintended consequences and perverse incentives
- Streamline Information Security Regulations: ancillary benefits with little government cost
- Subsidies: less effective than other cost-sharing incentives and inefficient due to moral hazard with highest government cost
- Tax Incentives: less effective than other cost-sharing incentives and inefficient due to moral hazard with highest government cost

Homeland Security

8

Proposed Procedure for Awarding Incentives

- In practice, it might difficult for DHS to determine whether the framework has been adopted, particularly when incentive awards are based on that determination.
- A more practical solution might be for DHS to follow procedures whereby applicants are evaluated on the extent to which they have adopted a standard.
  - This is also consistent with the administration's *"Pay for Success"* model of payment for performance in the context of social services.
- In this way, either the size of the incentive would be made contingent on the evaluation, or a penalty would be assessed for a low evaluation.
- Owners/operators would be awarded with higher levels of incentives for improving their evaluations, and since it is not tied to cost, moral hazard is eliminated.
- Adverse selection is also addressed, because even a "high cost" owner/operator with a low level of cybersecurity sophistication can be motivated to improve.
  - "Low cost" owners/operators, already near the frontier of sophistication, stop receiving incentives once they reach the highest level of evaluation, though penalties may be assessed for regression.

Upcoming Milestones

- May 21 (today): preliminary results of our analysis briefed to the Incentives WG
- June 12: Incentives recommendations submitted to White House
- Week of June 10 and/or June 17: recommendations presented to private sector critical infrastructure representatives and academia (2013 Workshop on the Economics of Information Security at Georgetown University), as part of our peer-review process
- Summer 2013: Submit an additional or amended report based on feedback received during peer review

Homeland Security

Mr. MEEHAN. The Chairman now recognizes the Ranking Minority Member of the subcommittee, the gentlelady from New York, Ms. Clarke, for any statement that she may have.

Ms. CLARKE. Thank you very much, Mr. Chairman.

Welcome to our panelists this morning.

Our country's reliance on cyber systems cover the waterfront; everything from power plants to pipelines and hospitals to highways, have increased cyber connections dramatically and our infrastructure is more physically and digitally interconnected than ever.

Yet for all of the advantages interconnectivity offers our Nation's critical infrastructure, it is also increasingly vulnerable to attack from an array of cyber threats.

It is vital that we as a country take action to strengthen our National policy on critical infrastructure security and resilience and includes measures to strengthen cybersecurity.

Because the majority of our critical infrastructure is owned and operated by private companies, the public and private sectors have a shared responsibility to reduce the threats to critical infrastructure through a stronger partnership.

The current Federal legislative framework for cybersecurity is complex with more than 50 statutes currently addressing various aspects of it.

However, we can all agree that the current framework is not sufficient to address the growing concerns about the security of cyberspace in the United States and no major cybersecurity legislation has been enacted since 2002, although the Executive branch has taken several notable actions.

The Federal role in protection of privately-held critical infrastructure has been one of the most contentious issues in the debate about cybersecurity legislation.

There appears to be a broad agreement that additional actions are needed to address the security risks, NCI, but there is considerable disagreement about how much, if any, additional Federal regulation is required.

So in February of this year, the President acted through an extraordinary order of directives an Executive Order on cybersecurity and a Presidential Policy Directive on critical infrastructure security and resilience that will likely become National and global references for cybersecurity policymaking.

Under the EO, the Secretary of Commerce is tasked to direct the director of NIST to develop a framework of reducing cyber risks to critical infrastructure.

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

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

It is important that the United States set a positive example regarding the essential role that global standards play for both industry and Government. This framework presents an important opportunity to develop a product that many other countries can replicate and use in their policy environments.

The United States could encourage global acceptance of this framework by seeking comments and support from our allies during its development. This adoption would be beneficial by creating consistent and cohesive approaches across these geographies as well as a commitment to the global standardization process.

A long-standing concern of mine is how we go about addressing cyber workforce considerations and how they will be included in the development of the framework we will be talking about today.

Our National cybersecurity workforce must be trained and be able to maintain the skills necessary to understand the changing operating environment. They must also be able to understand the threats, vulnerabilities to the environment, and most importantly, they must be skilled at practices to combat those threats and vulnerabilities.

I am hoping that you, Mr. Chairman, and I can work together on this important need.

We also have a need of improvement in the fundamental knowledge of cybersecurity. New solutions and approaches have been recognized for well over a decade and those discoveries were a factor in the passage of the Cyber Security Research and Development Act in 2002.

However, the law focuses on cybersecurity R&D by NSF and NIST. The Homeland Security Act of 2002 in contrast does not specifically mention cybersecurity R&D, but DHS and several other Departmental agencies make significant investments in it.

About 60 percent of reported funding by agencies in cybersecurity and information assurance is defense-related and we need to direct some of this R&D in the civilian arena.

I understand that you, Mr. Chairman, have some language along this line, and I hope we can, together, work on this issue.

What we all want for a cybersecurity framework is something that is flexible, repeatable, performance-based, includes a strong privacy and civil liberties protections, and something that is cost-effective.

After all, the President is attempting to help the privately-held owners and operators of the Nation's critical infrastructure to identify, assess, and manage cybersecurity-related risks while protecting business confidentiality and individual privacy and civil liberties.

In short, we need to regain sovereignty over our National and local assets that keep our small businesses running, our city and State governments providing services to citizens, our factories humming, and our essential services protected.

I look forward to testimony today about the progress that is being made because of the President's leadership on cybersecurity, and I hope that Congress can learn some lessons from the process he has set in motion.

I just want to add that I recently received this copy of the incentives study, Mr. Kolasky, and I understand that this is in response to the Executive Order.

It was issued May 21, and it would be great if we engaged in information sharing as well if we are going to demand it from those who are tasked to give guidance to.

With that, Mr. Chairman, I yield back.

[The statement of Ranking Member Clarke follows:]

STATEMENT OF RANKING MEMBER YVETTE D. CLARKE

JULY 18, 2013

Our country's reliance on cyber systems covers the waterfront, everything from power plants to pipelines, and hospitals to highways have increased cyber connections dramatically, and our infrastructure is more physically and digitally interconnected than ever. Yet for all the advantages interconnectivity offers, our Nation's critical infrastructure is also increasingly vulnerable to attack from an array of cyber threats.

It is vital that we, as a country, take action to strengthen our National policy on critical infrastructure security and resilience, and includes measures to strengthen cybersecurity. Because the majority of our critical infrastructure is owned and operated by private companies, the public and private sectors have a shared responsibility to reduce the risks to critical infrastructure through a stronger partnership.

The current Federal legislative framework for cybersecurity is complex, with more than 50 statutes currently addressing various aspects of it. However, we can all agree that the current framework is not sufficient to address the growing concerns about the security of cyber space in the United States, and no major cybersecurity legislation has been enacted since 2002, although the Executive branch has taken several notable actions.

The Federal role in protection of privately-held Critical Infrastructure has been one of the most contentious issues in the debate about cybersecurity legislation. There appears to be broad agreement that additional actions are needed to address the cybersecurity risks to CI but there is considerable disagreement about how much, if any, additional Federal regulation is required.

So, in February of this year, the President acted through an extraordinary pair of directives, an Executive Order on Cybersecurity and a Presidential Policy Directive on Critical Infrastructure Security and Resilience, that will likely become National and global references for cybersecurity policymaking. Under the EO, the Secretary of Commerce is tasked to direct the Director of NIST to develop a framework for reducing cyber risks to critical infrastructure. The Framework will consist of

standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

The Department of Homeland Security, in coordination with sector-specific agencies, will then establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities.

It is important that the United States set a positive example regarding the essential role that global standards play for both industry and Government. This framework presents an important opportunity to develop a product that many other countries can replicate and use in their policy environments. The United States could encourage global acceptance of this framework by seeking comments and support from our allies during its development. This adoption would be beneficial by creating consistent and cohesive approaches across those geographies as well as a commitment to the global standardization process.

A long-standing concern of mine is how we go about addressing Cyber Workforce considerations and how they will be they included in the development of the Framework we will be talking about today. Our National cybersecurity workforce must be trained and be able to maintain the skills necessary to understand the changing operating environment. They must also be able to understand the threats and vulnerabilities to that environment, and most importantly, they must be skilled at practices to combat those threats and vulnerabilities. I am hoping that the Chairman and I can work together on this important need.

We also have a need for improvements in the fundamental knowledge of cybersecurity. New solutions and approaches have been recognized for well over a decade and these discoveries were a factor in the passage of the Cybersecurity Research and Development Act in 2002. However, that law focuses on cybersecurity R&D by NSF and NIST. The Homeland Security Act of 2002, in contrast, does not specifically mention cybersecurity R&D, but DHS and several other Departmental agencies make significant investments in it. About 60% of reported funding by agencies in cybersecurity and information assurance is defense-related, and we need to direct some of this R&D in the civilian arena. I understand the Chairman has some language along this line, and I hope we can work together on this issue too.

What we all want from a Cybersecurity Framework is something that is flexible, repeatable, performance-based, includes strong privacy and civil liberties protections, and something that is cost-effective. After all, the President is attempting to help the privately-held owners and operators of the Nation's critical infrastructure to identify, assess, and manage cybersecurity-related risk while protecting business confidentiality and individual privacy and civil liberties.

In short we need to regain sovereignty over our National and local assets that keep our small businesses running, our city and State governments providing services to citizens, our factories humming, and our essential services protected. I look forward to the testimony today to hear about the progress that is being made because of the President's leadership on cybersecurity, and I hope that Congress can learn some lessons from the process he has set into motion.

Mr. MEEHAN. I thank the gentlelady for her comments and other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JULY 18, 2013

Several years ago, this committee passed the legislation that became the DHS' Chemical Facility Anti-Terrorism Standards (CFATS) program. CFATS was one of this committee's first attempts to proactively explore how to make this country safer by engaging the private sector. We knew that no private facility wanted to become the target of terrorists. But we also knew that the private sector does not often view the Government as a partner.

We needed to create a structure that permitted Government and the private sector to work together without fear of penalty or reprisal. I believe we created such a system. Today, we are here to discuss another instance in which the private sector is being asked to cooperate with the Government to safeguard the American people. While the potential danger posed by a terrorist attack on a chemical facility is easy to understand, the threat posed by an attack on the cyber network of a facility is difficult to envision.

But let's be clear—cyber attacks that cause large-scale system failures among the businesses and organization that we use every day would not only cause inconvenience, for some people, such system failures could be life-threatening.

While something in our history and culture may not allow us to admit it easily, we need to acknowledge that we rely on the everyday presence of power plants, hospitals, manufacturing plants, mass transit and subway systems, airports, and the system of electronic commerce.

And in our current world, none of these systems can exist without a computer network that is linked to many other computer networks. Our National and individual interests depend upon the protection of these networks and the security of the information in them.

Government and the private sector must work together to assure that the owners and operators of these facilities are able to safeguard their operations and assets from the risk of cyber attack.

Also, we must be sure that if attacked by a cyber terrorist, these facilities are able to quickly determine the damage, recover from the injury and move forward.

The cybersecurity Executive Order attempts to achieve these goals. Needless to say, I would prefer that this Congress take up legislation to address the many cybersecurity threats facing the critical infrastructure of this Nation. However, this Congress seems to have a difficult time engaging in the legislative process. Thus, I look forward to the implementation of Executive Order 13636, which directs Federal agencies to coordinate the development and implentation of risk-based standards.

Mr. MEEHAN. We are very pleased to have a distinguished panel before us today, and we thank each of you for the work that you are doing on behalf of our Nation and your efforts to assure that we take every possible step to protect our cyber infrastructure.

We are going to be joined today first by Mr. Robert Kolasky who serves as the director of the Department of Homeland Security's Integrated Task Force that was put together to implement the Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience as well as the President's Executive Order on Critical Infrastructure Cyber Security.

Mr. Kolasky has served in many roles throughout DHS since joining the Federal Government in 2002, and I thank you for your service.

We will be joined by Dr. Charles Romine, the director of Information Technology Laboratory, one of six research laboratories within the National Institute of Standards and Technology.

Dr. Romine oversees research programs designed to promote U.S. innovation and industrial competitiveness by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems.

Thank you, Dr. Romine.

We are joined by Dr. Eric Fischer. He is the senior specialist in science and technology at the Congressional Research Service. In this role, he provides expert written and consultation support to Congress on a broad range of issues in science and technology policy including cybersecurity, environmental issues, and research and development.

He has authored more than 30 CRS reports—and I thank you for that great work. They are a big help to us as we try to negotiate our way through the thicket of issues to increase our understanding—and more than 100 analytical memoranda for Congressional offices on the subjects I just mentioned.

The witnesses' full written statements will appear in the record, and so I ask that you use your time as best you can to help us to hear what is important in your testimony.

I will now recognize Mr. Kolasky for 5 minutes to testify.

Thank you, Mr. Kolasky.

STATEMENT OF ROBERT KOLASKY, DIRECTOR, IMPLEMENTATION TASK FORCE, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. KOLASKY. Good morning, Chairman Meehan, Ranking Member Clarke, and distinguished Members of the committee. I want to thank you for your support of the Department, particularly in our mission to safeguard and secure the Nation's critical infrastructure.

I am pleased to be here before you to discuss the administration's role and DHS's role in implementing PPD 21 on Critical Infrastructure Security Resilience and Executive Order 13636, Critical Infrastructure Cyber Security.

As you know, DHS supports critical infrastructure owners and operators in preparing for, preventing, protecting against, mitigating from, responding to, and recovering from all hazardous events including cyber incidents, natural disasters, and terrorist attacks.

To achieve this, DHS works with public and private-sector partners to identify and promote effective solutions for security and resilience that address the risk facing the Nation's critical infrastructure.

As you mentioned, recognizing the need for collaborative solutions to confront these risks and promote a more secure and resiliant critical infrastructure, President Obama issued Executive Order and the Presidential Policy on Critical Infrastructure Security and Resilience in February of this year.

These two directives aimed to enhance the security and resilience of the Nation's critical structure to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.

Promoting security resilience is a collaborative effort. It involves participation from the private sector, owners and operators, State, local, and Tribal territorial governments as well.

To accomplish this collaborative effort, DHS stood up the integrated task force to implement the EO and PPD and the integrated task force has developed a consultative process for the whole Federal Government to work with the private sector and State and local and Tribal territorial governments as well as nonprofits and academic communities.

At the integrated task force, we have developed nine separate working groups and have conducted more than 100 working sessions involving 1,100 attendees to date. Representatives from DHS have also conducted more than 100 briefings on our effort to nearly 10,000 stakeholders since February 2013.

In addition, DHS has worked with our colleagues at the Department of Commerce's National Institute of Standards and Technology to utilize this consultative process in support of the development of cybersecurity framework, which NIST is leading the effort on.

We have accomplished much over the past 150 days, and I would like to talk about that and I am eager to take questions related to that.

Among the things that we have delivered, as Ranking Member Clarke referenced, an incentives report which analyzes potential incentives that can be used to promote to the adoption of the cybersecurity framework, a description of critical infrastructure functional relationships, instructions on producing unclassified cyber threat reports from all sources of information and making that information available to critical infrastructure partners, procedures for the expansion of the enhanced cybersecurity service program within DHS, which is intended to share cyber threat information with appropriately cleared private-sector cybersecurity providers across all critical infrastructure sectors, recommendations on the feasibility, security benefits, and merits of incorporating security standards into acquisition planning and contract administration, a process for expediting security clearances to those in the private sector with the essential need to know about cyber threat information, and a report outlining how well the current public/private partnership model that is documented in the National Infrastructure Protection Plan is working and recommendations for enhancements to that model.

In addition, we have conducted an evaluation of and are identifying critical infrastructure entities where a cybersecurity incident has the potential to cause National or regionally catastrophic incidents.

While we have made significant progress to date, there is much work still to be done this year. DHS will be focusing its efforts on the following steps throughout the rest of the year.

Updating the National infrastructure protection plan to reflect new policies, a change in the risk environment, and lessons learned working in collaboration across the public and private sector to manage infrastructure risks.

Enhancing near-real-time situational awareness for critical infrastructure, developing a draft of the National Critical Infrastructure Security and Resilience Research and Development Plan and collaborating with our colleagues at NIST on the cybersecurity framework.

It is important to note that the EO and PPD work within current authorities. They do not grant new regulatory authority or establish additional incentives for participation in a voluntary program.

The administration continues to believe that a comprehensive suite of legislation is necessary to implement the full ranges of steps necessary to build a strong public/private partnership and we hope to continue to work with Congress to achieve this.

Among our legislative priorities are: Facilitating cybersecurity for information sharing between the Government and the private sector while maintaining privacy and civil liberties protections and reinforcing the appropriate roles of intelligence and non-intelligence agencies.

Incentivizing the adoption of best practices and standards for critical infrastructure by complementing the process set forth in the Executive Order, updating Federal agency network security laws and codifying DHS' cybersecurity responsibilities, giving law

enforcement the tools to fight crime in the digital age, and creating a new National data breach reporting requirement.

I will end my statements by saying that although we are doing much within the EO and PPD, this is just a start and we hope to continue to work with the owners and operators in State and local and Tribal territorial governments to make progress this year and in the future so that we all have confidence in the security and the resiliency of our critical infrastructure and key networks.

Thank you for the opportunity to discuss the Department's role in improving critical infrastructure security and resilience, and I look forward to the dialogue.

[The prepared statement of Mr. Kolasky follows:]

PREPARED STATEMENT OF ROBERT KOLASKY

JULY 18, 2013

INTRODUCTION

Good morning Chairman Meehan, Ranking Member Clarke, and distinguished Members of the committee. Let me begin by thanking you for your support of the Department of Homeland Security (DHS), particularly in its mission to safeguard and secure the Nation's critical infrastructure. I am pleased to appear before you to discuss the Department's role in implementing Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity,* and Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience*.

DHS supports critical infrastructure owners and operators in preparing for, preventing, protecting against, mitigating from, responding to, and recovering from all-hazards events, including cyber incidents, terrorist attacks, and natural disasters. These activities promote the safety and security of the American public and ensure the provision of essential services and functions, such as energy and communications. To achieve this end, DHS works with public and private-sector partners to identify and promote effective solutions for security and resilience that address the risks facing the Nation's critical infrastructure.

While this increased connectivity has led to significant transformations and advances across our country—and around the world—it also has increased the importance and complexity of our shared risk. Our daily life, economic vitality, and National security depend on cyberspace. A vast array of interdependent IT networks, systems, services, and resources are critical to communication, travel, powering our homes, running our economy, and obtaining Government services. No country, industry, community, or individual is immune to cyber risks.

Critical infrastructure is the backbone of our country's National and economic security. It includes power plants, chemical facilities, communications networks, bridges, highways, and stadiums, as well as the Federal buildings where millions of Americans work and visit each day. DHS coordinates the National protection, prevention, mitigation, and recovery from cyber incidents and works regularly with business owners and operators to take steps to strengthen their facilities and communities. The Department also conducts on-site risk assessments of critical infrastructure and shares risk and threat information with State, local, and private-sector partners.

Protecting critical infrastructure against growing and evolving cyber threats requires a layered approach. DHS actively collaborates with public and private-sector partners every day to improve the security and resilience of critical infrastructure while responding to and mitigating the impacts of attempted disruptions to the Nation's critical cyber and communications networks and to reduce adverse impacts on critical network systems.

Beyond evolving cybersecurity risks, the Nation's critical infrastructure is potentially affected by more frequent and severe weather events, by sustained under-investment in the integrity of aging and degrading infrastructure, and by an evolving terrorist threat.

Recognizing the need for collaborative solutions to confront this changing risk paradigm and promote a more secure and resilient critical infrastructure, President Obama issued EO 13636 and PPD–21. These two directives aim to "enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber

environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

Taken together, these two policy documents are intended to achieve the following:

- Encourage the adoption of effective measures across all critical infrastructure sectors to improve security and resiliency and reduce risk from cyber attacks to essential functions and services by publishing a Cybersecurity Framework (the Framework) that will provide owners and operators with a prioritized, flexible, repeatable, performance-based, and cost-effective set of validated security controls based upon industry best practices.
- Enhance timely, relevant, and accurate information sharing on significant risks by implementing a program to develop and rapidly share unclassified information with critical infrastructure owners and operators, enabling the adoption of effective mitigations to prevent or to reduce the consequences of significant incidents.
- Align responsibilities of public and private partners to efficiently allocate risk reduction responsibilities by conducting an analysis of the existing critical infrastructure public-private partnership model and recommending options for improving the effectiveness of the partnership in managing both the physical and cyber risks.
- Promote innovation in novel risk-reduction solutions by developing a National Critical Infrastructure Security and Resilience Research and Development (R&D) Plan to identify priorities and guide R&D requirements and investments toward those solutions that will help assure the provision of essential functions and services over time.
- Ensure that privacy, civil rights, and civil liberties are protected as a foundational part of all risk management efforts by conducting an assessment of the privacy, civil rights, and civil liberties implications of all EO 13636 and PPD–21 programs and recommending revisions to proposed initiatives as required.

Working in partnership with the Federal interagency, DHS established an Integrated Task Force to:

- Lead the Department's implementation of PPD–21 and EO 13636, including coordination with the Department of Commerce's National Institute of Standards and Technology, on the Cybersecurity Framework;
- Serve as the focal point for collaboration with industry;
- Involve key stakeholders from all levels of government; and
- Prioritize tasks, plan implementation, and coordinate principal offices of responsibility.

The Integrated Task Force is further charged with ensuring the production of various deliverables as mandated under EO 13636 and PPD–21. These deliverables, however, are not an end in themselves; rather, each deliverable is intended to contribute to future efforts that will promote the security and resilience of the Nation's critical infrastructure.

CONSULTATIVE PROCESS

Promoting security and resilience is a collaborative endeavor requiring effort and investment from both the Federal Government and private sector, as well as State, local, Tribal, and territorial partners. Thus, to implement EO 13636 and PPD–21, the Federal Government has actively sought the collaboration, input and engagement of our partners. The Integrated Task Force has developed a "consultative process" pursuant to EO 13636, to work within the Federal Government to collaborate with State, local, Tribal, and territorial government officials as well as private-sector owners and operators of critical infrastructure and the non-profit and academic communities. The consultative process is based on the following principles:

- Seek out opportunities across the whole community;
- Be systematic, transparent, and repeatable;
- Focus on appropriate and meaningful multi-directional communications and collaboration;
- Establish protocols to ensure that progress reports, current direction, and current messaging are broadly shared and understood;
- Document activities to track participation across the whole community;
- Identify and engage the full range of stakeholders across the critical infrastructure and cybersecurity community;
- Utilize established partnership organizations and regimes;
- Promote innovative approaches to maximize opportunities for input from stakeholders across the whole community;

- Ensure that privacy and civil liberties protections are incorporated into the tasks by coordinating with appropriate senior Federal agency officials;
- Foster development of an enduring engagement process that can be used in other cyber and critical infrastructure security and resilience efforts.

Using those principles, the Integrated Task Force developed nine separate working groups and has conducted more than 100 working sessions involving 1,100 attendees, to date. Representatives from DHS have also conducted more than 100 briefings on our efforts to nearly 10,000 stakeholders since February 2013. Outside of the established Integrated Task Force working groups, the cyber and critical infrastructure communities are being engaged through working sessions, conferences, meetings, and virtual collaboration methods such as the Homeland Security Information Network, IdeaScale, and webinars. The format and style of engagement varies according to the needs of the community engaged and the purpose for engagement. The venue and mechanism for engagement is also determined by the outcomes sought and the nature of the constituency involved. In addition, DHS has worked with the Department of Commerce's National Institute of Standards and Technology (NIST) to utilize the consultative process in support of the development of the Framework.

STATUS OF CURRENT EFFORTS

We have accomplished much over the past 150 days using the Consultative Process to engage whole community stakeholders. The Secretary has already submitted several EO 13636 and PPD–21 deliverables to the White House, to include:

- An Incentives Report, which analyzes potential Government incentives that could be used to promote the adoption of the Framework;
- A description of critical infrastructure functional relationships, which illustrates the Federal Government's current organizational structure to deliver risk management support to stakeholders and make it easier for them to collaborate with the Government;
- Instructions on producing unclassified cyber threat reports from all sources of information, including intelligence, to improve the ability of critical infrastructure partners to prevent and respond to significant threats;
- Procedures for expansion of the Enhanced Cybersecurity Services (ECS) program to all critical infrastructure sectors. The ECS program promotes cyber threat information sharing between Government and the private sector, which helps critical infrastructure entities protect themselves against cyber threats to the systems upon which so many Americans rely. DHS will share with appropriately cleared private sector cybersecurity providers the same threat indicators that we rely on to protect the .gov domain. Those providers will then be free to contract with critical infrastructure entities and provide cybersecurity services comparable to those provided to the U.S. Government;
- Recommendations on feasibility, security benefits, and merits of incorporating security standards into acquisition planning and contract administration, addressing what steps can be taken to make existing procurement requirements related to cybersecurity consistent;
- A process for expediting security clearances to those in the private sector with an essential "need to know" regarding Classified cybersecurity risk information. This processing is intended only for those who need access to Classified information. While it is important to ensure that our private-sector partners who have a valid need for access to Classified information receive appropriate security clearances, we believe that most information sharing can be conducted at the Unclassified level; and
- A report outlining how well the current critical infrastructure public-private partnership model as articulated in the National Infrastructure Protection Plan (NIPP) is working toward promoting the security and resilience of the Nation's critical infrastructure, and recommendations to strengthen those partnerships.
- In addition, we have conducted an initial evaluation of and are identifying critical infrastructure entities which would reasonably result in catastrophic consequences from a cybersecurity incident. While we are incorporating lessons from this analysis in developing a repeatable system of critical infrastructure assessments, the results from this preliminary evaluation identified a relatively small list of U.S. critical infrastructure that if impacted by a cybersecurity incident could cause catastrophic consequence to our National security, economic security, public health, and safety.

MOVING FORWARD

While we have made significant progress to date, there is much work still to be done this year to fulfill the vision set forth in EO 13636 and PPD–21. To that end, DHS will be focusing its efforts on the following steps via the Integrated Task Force:

- Updating the NIPP to reflect new policies, a change in the risk environment, and lessons learned working in collaboration across the public and private sectors to manage infrastructure risk;
- Enhancing near-real-time situational awareness for critical infrastructure, with a particular focus on multi-directional information sharing and understanding of interdependencies between physical and cyber systems and critical infrastructure sectors;
- Developing a draft of the National Critical Infrastructure Security and Resilience Research and Development Plan; and
- Collaborating with NIST on the Cybersecurity Framework.

DHS is developing the Performance Goals described in EO 13636 for the Framework collaboratively with critical infrastructure owners and operators using the Consultative Process. By framing the importance of cyber risk in a business context, the Performance Goals will encourage adoption of the Framework. The goals complement the Framework which will outline what businesses should do to manage cyber risk. In turn, the specific standards and controls suggested under the Framework will explain how businesses should manage cyber risk.

Through the Performance Goals, critical infrastructure owners and operators will be able to adopt a common approach to evaluating the effectiveness of risk management investments based upon business outcomes. While DHS will not require nor evaluate the adoption of the Performance Goals among critical infrastructure owners and operators, the Goals will encourage businesses to frame cybersecurity risk in the context of economic sustainability, and thereby facilitate strategic planning and investment to identify changing risks and implement measurably effective solutions.

The Framework will also serve as a basis for a DHS Voluntary Program, which will result in on-going collaboration with industry to promote market-based solutions to higher levels of cybersecurity.

CYBER LEGISLATIVE PRIORITIES

It is important to note that EO 13636 directs Federal agencies to work within current authorities and increase voluntary cooperation with the private sector to provide better protection for computer systems critical to our National and economic security. We continue to believe that a comprehensive suite of legislation is necessary to implement the full range of steps needed to build a strong public-private partnership, and we will continue to work with Congress to achieve this.

Consistent with the proposal that the administration transmitted last Congress, legislation should:

- Facilitate cybersecurity information sharing between the Government and the private sector as well as among private-sector companies. We believe that such sharing can occur in ways that uphold privacy and civil liberties protections, expand upon existing best practices from industry leaders in this area, reinforce the appropriate roles of intelligence and non-intelligence agencies, and include targeted liability protections;
- Incentivize the adoption of best practices and standards for critical infrastructure by complementing the process set forth under the Executive Order;
- Give law enforcement the tools to fight crime in the digital age;
- Update Federal agency network security laws, and codify DHS' cybersecurity responsibilities; and
- Create a National Data Breach Reporting requirement.

In each of these legislative areas, we want to incorporate robust privacy and civil liberties safeguards. The administration stands ready to work with Congress to pass important cybersecurity legislation.

CONCLUSION

Critical infrastructure security and resilience to cyber incidents and other risks is an on-going capability development effort rather than an end-state to be achieved on a given date, or via a defined deliverable. All partners in this National effort will need to continue to contribute to its progress over time. The implementation of EO 13636 and PPD–21 is a key step in achieving these desired outcomes; progress will require sustained effort by both public and private partners, and a recognition of the rapidly evolving risk environment. The desired end-state of the critical infra-

structure partnership model is an environment in which public and private partners work in a networked manner to effectively and efficiently share information and allocate risk-reduction responsibilities. If achieved, this result will maximize the comparative advantage of each and reduce duplication or under-investment, resulting in collaborative solutions to reduce the likelihood of the highest-consequence incidents.

Thank you for the opportunity to discuss the Department's role in improving critical infrastructure security and resilience. I look forward to any questions you may have.

Mr. MEEHAN. Thank you, Mr. Kolasky. That is a—you got a lot on your agenda. That is a big report, and I know we will be looking forward to talking with you about some of that.

Dr. Romine. The Chairman now recognizes you for your 5 minutes of testimony. Thank you.

STATEMENT OF CHARLES H. ROMINE, PH D, DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE

Mr. ROMINE. Thank you, Chairman Meehan, Ranking Member Clarke, and Members of the subcommittee. Thank you very much for the opportunity to testify today.

As directed in the Executive Order, NIST is working with industry to develop the cybersecurity framework to improve the cybersecurity of critical infrastructures and working with the Department of Homeland Security to establish performance goals.

Our partnership with industry and with DHS is driving much of our effort. Earlier this year, we signed a memorandum agreement with DHS to ensure that our work on the framework and also with cybersecurity standards best practices and metrics is fully integrated with information sharing, threat analysis, response, and operational work of DHS.

We believe this will enable a more holistic approach to addressing the complex challenges that we face. The framework is an important element in addressing the challenges of improving the cybersecurity of our critical infrastructure.

A NIST-coordinated and industry-led framework will draw on standards and best practices that industry already develops and uses. NIST is ensuring that the process is open and transparent to all stakeholders and will ensure a robust technical underpinning to the framework.

This approach will significantly bolster the relevance of the resulting framework to industry making it more appealing for industry to adopt. This multi-stakeholder approach leverages the respective strengths of the public and private sectors and helps to develop solutions in which both sides will be invested.

The approach does not dictate solutions to industry but rather facilitates industry coming together to develop and offer solutions that the private sector is best positioned to embrace.

I would also like to note that this is not a new or novel approach for NIST. We have used very similar approaches in the recent past to address other pressing National priorities.

For example, NIST's work in the area of cloud computing technologies enabled us to develop important definitions and architectures and is now enabling broad Federal Government deployment

of secure cloud computing technologies. The lessons learned from this experience and others are informing how we are planning for and structuring our current effort.

NIST's initial steps toward implementing the Executive Order included issuing a request for information or RFI this past February to gather relevant input from industry and other stakeholders and asking stakeholders to participate in the cybersecurity framework process.

The responses to the RFI, a total of 244, were posted on NIST's website. Those responding ranged from individuals to large corporations and trade associations and they provided comments as brief as a few sentences on specific topics as well as so comprehensive that they ran over 100 pages. We published an analysis of these comments in May.

NIST is also engaging with stakeholders through a series of workshops and events to ensure that we can cover the breadth of considerations that will be needed to make this National priority a success. Our first such session held in April initiated the process of identifying existing resources and gaps and prioritized the issues to be addressed as part of the framework.

At the end of May, a second workshop at Carnegie Mellon University brought together a broad cross-section of participants representing critical infrastructure owners and operators, industry associations, standards developing organizations, individual companies, and Government agencies.

This 3-day working session using the analysis of the RFI comments as input was designed to identify and achieve consensus on the standards, guidelines, and practices that will be used in the framework.

Last week, NIST held its third workshop to present initial considerations for the framework. This workshop had a particular emphasis on issues that have been identified from the initial work including the specific needs of different sectors.

During the workshop, NIST gained consensus on several elements that the framework will include. At 8 months, we will have a preliminary framework that builds on these elements. After a year-long effort, once we have developed an initial framework, there will still be much to do.

For example, we will work with specific sectors and DHS to build strong voluntary programs for specific critical infrastructure areas. Their work will then inform the needs of critical infrastructure and the next versions of the framework.

The goal at the end of this process will be for industry itself to take ownership and update the cyber secure framework ensuring that the framework will continue to evolve as needed.

We have made significant progress, but we have a lot of work still ahead of us, and I look forward to working with this committee and others to help us address these pressing challenges.

I will be pleased to answer any questions you may have for me. Thank you.

[The prepared statement of Mr. Romine follows:]

PREPARED STATEMENT OF CHARLES H. ROMINE

JULY 18, 2013

INTRODUCTION

Chairman Meehan, Ranking Member Clarke, Members of the subcommittee, I am Chuck Romine, director of the Information Technology Laboratory of the National Institute of Standards and Technology (NIST), a non-regulatory bureau within the U.S. Department of Commerce. Thank you for this opportunity to testify today on NIST's role under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" and our responsibility to develop a framework for reducing cyber risks to critical infrastructure.

THE ROLE OF NIST IN CYBERSECURITY

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

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

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

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

EXECUTIVE ORDER 13636, "IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY"

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

Our partnership with DHS will drive much of our effort. Earlier this year, we signed a Memorandum of Agreement with DHS to ensure that our work on the Cybersecurity Framework, and also with cybersecurity standards, best practices, and metrics, is fully integrated with the information sharing, threat analysis, response, and operational work of DHS. We believe this will enable a more holistic approach to addressing the complex challenges we face.

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

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

I would also like to note that this is not a new or novel approach for NIST. We have utilized very similar approaches in the recent past to address other pressing

National priorities. For example, NIST's work in the area of cloud computing technologies enabled us to develop important definitions and architectures, and is now enabling broad Federal Government deployment of secure cloud computing technologies. The lessons learned from this experience and others are informing how we are planning for and structuring our current effort.

DEVELOPING THE CYBERSECURITY FRAMEWORK

The Cybersecurity Framework will consist of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks for critical infrastructure. Once the final Framework is established, the Department of Homeland Security (DHS), in coordination with sector-specific agencies, will then support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities through a voluntary program. Regulatory agencies will also review the Cybersecurity Framework to determine if current cybersecurity requirements are sufficient, and propose new actions to ensure consistency.

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

CURRENT STATUS OF THE CYBERSECURITY FRAMEWORK

Underlying all of this work, NIST sees its role in developing the Cybersecurity Framework as partnering with industry and other stakeholders to help them develop the Framework. NIST's unique technical expertise in various aspects of cybersecurity-related research and technology development, and our established track record of working with a broad cross-section of industry and Government agencies in the development of standards and best practices, positions us very well to address this significant National challenge in a timely and effective manner.

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

The responses to the RFI—a total of 244—were posted on NIST's website. Those responding ranged from individuals to large corporations and trade associations and they provided comments as brief as a few sentences on specific topics, as well as so comprehensive that they ran over a hundred pages. We published an analysis of these comments in May.

NIST is also engaging with stakeholders through a series of workshops and events to ensure that we can cover the breadth of considerations that will be needed to make this National priority a success. Our first such session—held in April—initiated the process of identifying existing resources and gaps, and prioritized the issues to be addressed as part of the Framework.

At the end of May, a second workshop at Carnegie Mellon University brought together a broad cross-section of participants representing critical infrastructure owners and operators, industry associations, standards-developing organizations, individual companies, and Government agencies. This 3-day working session, using the analysis of the RFI comments as input, was designed to identify and achieve consensus on the standards, guidelines, and practices that will be used in the Framework.

Based on the responses to the RFI, conclusions from the workshops, and NIST analyses, the preliminary Framework is designed and intended:

- To be an adaptable, flexible, and scalable tool for voluntary use;
- To assist in assessing, measuring, evaluating, and improving an organization's readiness to deal with cybersecurity risks;
- To be actionable across an organization;
- To be prioritized, flexible, repeatable, performance-based, and cost-effective;
- To rely on standards, guidelines, and practices that align with policy, business, and technological approaches to cybersecurity;
- To complement rather than to conflict with current regulatory authorities;

- To promote, rather than to constrain, technological innovation in this dynamic arena;
- To focus on outcomes;
- To raise awareness and appreciation for the challenges of cybersecurity but also the means for understanding and managing the related risks;
- To be built upon international standards and other standards, best practices and guidelines that are used globally.

Last week, NIST held its third workshop to present initial considerations for the Framework. This workshop had a particular emphasis on issues that have been identified from the initial work—including the specific needs of different sectors. During the workshop, NIST gained consensus on the elements of the Framework that include:

- A section for senior executives and others on using this Framework to evaluate an organization's preparation for potential cybersecurity-related impacts on their assets and on the organizations ability to deliver products and services. By using this Framework, senior executives can manage cybersecurity risks within their enterprise's broader risks and business plans and operations.
- A User's Guide to help organizations understand how to apply the Framework.
- Core Sections to address:
  - Five major cybersecurity functions and their categories, subcategories, and informative references;
  - Three Framework Implementation Levels associated with an organization's cybersecurity functions and how well that organization implements the Framework.
  - A compendium of informative references, existing standards, guidelines, and practices to assist with specific implementation.

At 8 months, we will have a preliminary Framework that builds on these elements. In a year's time, once we have developed an initial Framework, there will still be much to do. For example, we will work with specific sectors to build strong voluntary programs for specific critical infrastructure areas. Their work will then inform the needs of critical infrastructure and the next versions of the Framework. The goal at the end of this process will be for industry itself to take "ownership" and update the Cybersecurity Framework—ensuring that the Framework will continue to evolve as needed.

CONCLUSION

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

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

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

Mr. MEEHAN. Thank you, Dr. Romine.

The Chairman now recognizes Dr. Fischer for 5 minutes of testimony.

Dr. Fischer.

STATEMENT OF ERIC A. FISCHER, PH D, SENIOR SPECIALIST, SCIENCE AND TECHNOLOGY, CONGRESSIONAL RESEARCH SERVICE, LIBRARY OF CONGRESS

Mr. FISCHER. Good morning, Chairman Meehan, Ranking Member Clarke, and distinguished Members of the subcommittee. On

behalf of the Congressional Research Service, thank you for the opportunity to testify today.

Over the past several years, evidence has grown that U.S. critical infrastructure is vulnerable to potentially damaging cyber attacks. Calls for action have come from many corridors. The 111th and 112th Congresses considered but did not enact legislation to address those vulnerabilities.

Last year, the Obama administration announced that it was in developing Executive Order, which as you heard was—as, you know, was released in February of this year.

Five goals in the order have received the most public attention. They are No. 1, expanded information sharing including Classified information between the Government and the private sector.

No. 2, identification of critical infrastructure for which successful cyber attacks could have catastrophic impacts.

No. 3, a voluntary framework of cybersecurity standards and best practices for critical infrastructure developed with the private sector.

No. 4, incentives for voluntary adoption of that framework.

No. 5, review of regulatory requirements on cybersecurity and recommendations on how to improve them.

The order called for fulfillment of its information-sharing requirements and certain others by mid-June of this year and for the high-risk critical infrastructure to be designated by mid-July.

The framework is to be finalized by next February along with the report addressing privacy and civil liberties protections. The review of regulatory requirements is to be completed in two stages with gaps to be identified by next March and the problematic requirements by February 2016.

The administration issued Presidential Policy Directive 21 along with the Executive Order. The Directive makes cybersecurity an integral component of critical infrastructure security and resilience.

Generally, reaction to the Executive Order and Directive from stakeholders has been positive. Criticisms have tended to fall into five categories: Whether the Order does anything new, the implementation time table, adoption of the framework, the critical infrastructure designation process, and the Order's influence on Congressional action. For all five categories, arguments have been made on both sides.

One criticism of the Order was also raised against some of the legislative proposals in the 112th Congress that it would result in increased industry regulation that would be both ineffective and burdensome.

Such critics say that even a voluntary framework can become mandatory in practice. An alternative view is that voluntary approaches have not been particularly effective in this area and regulation appears to be working in sectors such as electric power. Others believe that voluntary approaches can be effective without causing undue burdens.

Some argue that it will be better for this Congress to wait until the Order is fully implemented before considering legislation. Others believe, however, that the Order merely clarifies what changes are needed to current law.

It may be too early to determine how at least some of those concerns above will be addressed, let alone whether the responses will satisfy critics. Overall, however, response from the private sector appears to be cautiously optimistic.

With respect to current legislation, the Cybersecurity Enhancement Act, H.R. 756, would require a triennial strategic plan for cybersecurity R&D. It would be prepared using an interagency process similar to that established under the High Performance Computing Act of 1991 and related laws.

PPD 21 also requires a periodic R&D plan, but it would focus specifically on critical infrastructure and cover physical as well as a cybersecurity.

It would also be quadrennial rather than triennial, and it would be led by the Secretary of Homeland Security rather than the Office of Science and Technology Policy.

CISPA, H.R. 624, would permit sharing of classified information with private-sector critical infrastructure entities. Under the bill, procedures would be established by the Director of National Intelligence. The Executive Order in contrast puts the Secretary of Homeland Security in the lead.

CISPA also requires that the establishment of new procedures relating to privacy and civil liberties; whereas the Order requires agencies to apply protections consistent with established principles.

Finally, I should mention that CISPA would address one of the perceived gaps in current law. It would explicitly permit information sharing between private entities and would provide liability protections. Significant debate has centered on the scope of those changes and the potential impacts on privacy and civil liberties.

That concludes my testimony. Once again, thank you for asking me to appear before you today.

[The prepared statement of Mr. Fischer follows:]

PREPARED STATEMENT OF ERIC A. FISCHER

JULY 18, 2013

Chairman Meehan, Ranking Member Clarke, and distinguished Members of the subcommittee:

Thank you for the opportunity to discuss Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, with you today. In my testimony, I will provide some background on the development of the Order and describe its major provisions, including the roles it proposes for the private sector and reaction to it by those stakeholders, as well as its relationship to Congressional legislation and the new Obama administration policy directive on critical infrastructure.

DEVELOPMENT OF THE EXECUTIVE ORDER

Both the George W. Bush administration and the Obama administration have made improvements to the cybersecurity of critical infrastructure a priority. The Bush administration created the Comprehensive National Cybersecurity Initiative (the CNCI) in 2008 via a Classified Presidential Directive.[1] The Obama administration performed an interagency review of Federal cybersecurity initiatives in 2009, culminating in the release of its *Cyberspace Policy Review*[2] and the creation of the White House position of Cybersecurity Coordinator.

[1] National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD–54/HSPD–23).

[2] The White House, *Cyberspace Policy Review,* May 29, 2009, *http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf;* The White House, "Cyberspace Policy

Continued

Both those efforts and a number of reports from agencies, think tanks, and other groups identified gaps in Federal efforts. Both the 111th and 112th Congresses considered legislative proposals to close those gaps, but none were enacted. In the absence of enacted legislation, the Obama administration began drafting a cybersecurity Executive Order in 2012. The development involved a lengthy interagency process, with both agencies and stakeholders in the private sector providing input.

The White House released Executive Order 13636 on February 12, 2013, along with a new policy directive on critical infrastructure. Relevant legislation is also being developed by the 113th Congress. Four bills with cybersecurity provisions (H.R. 624, H.R. 756, H.R. 967, and H.R. 1163) that were introduced in the month after the release of the Executive Order passed the House in April, and additional bills in the House and the Senate are reportedly being drafted.

REQUIREMENTS IN THE EXECUTIVE ORDER

The Order uses existing statutory and Constitutional authority to:

- *Expand information sharing and collaboration* between the Government and the private sector, including sharing Classified information by broadening a program developed for the defense industrial base to other critical-infrastructure sectors;
- *Develop a voluntary framework of cybersecurity standards and best practices* for protecting critical infrastructure, through a public/private effort;
- *Establish a consultative process* for improving critical-infrastructure cybersecurity;
- *Identify critical infrastructure with especially high priority for protection,* using the consultative process;
- *Establish a program with incentives for voluntary adoption of the framework* by critical-infrastructure owners and operators;
- *Review cybersecurity regulatory requirements* to determine if they are sufficient and appropriate; and
- *Incorporate privacy and civil liberties protections* in activities under the Order.

The information-sharing and framework provisions in particular have received significant public attention.

Information Sharing

The Order formalizes a previously existing program, now called Enhanced Cybersecurity Services, in the Department of Homeland Security (DHS), for providing classified threat information to eligible critical infrastructure companies and to their eligible internet, network, communications, and cybersecurity service providers (known jointly as commercial service providers or CSPs). The program developed out of a pilot involving the Department of Defense and companies in the defense industrial base, which is one of the 16 recognized critical-infrastructure sectors.

The Order also requires the Secretary of Homeland Security, the Attorney General, and the Director of National Intelligence to expedite dissemination to targeted entities of unclassified and, where authorized, classified threat indicators. Additionally, the Secretary of Homeland Security is to expedite processing of security clearances to appropriate critical-infrastructure personnel and expand programs to place relevant private-sector experts in Federal agencies on a temporary basis.

Cybersecurity Framework

Executive Order 13636 requires the National Institute of Standards and Technology (NIST) to lead the development of a Cybersecurity Framework that uses an open, consultative process to identify cross-sector, voluntary consensus standards and business best practices that can reduce cybersecurity risks to critical infrastructure. The framework is to be technology-neutral. It must identify areas for improvement and be reviewed and updated as necessary.

The Secretary of Homeland Security is required to set performance goals for the framework, establish a voluntary program to support its adoption, and coordinate establishment of incentives for adoption. The sector-specific agencies must coordinate review of the framework and development of sector-specific guidance, and report annually to the President on participation by critical-infrastructure sectors. Agencies with regulatory responsibilities for critical infrastructure are required to engage in consultative review of the framework, determine whether existing cybersecurity requirements are adequate, report to the President whether the agencies have authority to establish requirements that sufficiently address the risks, propose

---

Review [Supporting Documents]," May 2009, *http://www.whitehouse.gov/cyberreview/documents/*.

additional authority where required, and identify and recommend remedies for ineffective, conflicting, or excessively burdensome cybersecurity requirements.

The development of the framework is arguably the most innovative and labor-intensive requirement in the Executive Order. It builds on the involvement of NIST in the development of cybersecurity technical standards [3] and its statutory responsibilities to work with both Government and private entities on various aspects of standards and technology.[4]

None of the major legislative proposals in the 111th and 112th Congresses had proposed using NIST to coordinate an effort led by the private sector to develop a framework for cybersecurity, such as is envisioned by the Executive Order. Hundreds of entities have been involved in NIST's efforts to date, beginning with a Request for Information in February and including public workshops in April, May, and July of 2013.[5] An additional workshop is planned for September.

Other Requirements

Acquisition and Contracting. The Secretary of Defense and the Administrator of General Services must make recommendations to the President on incorporating security standards in acquisition and contracting processes, including harmonization of cybersecurity requirements.

Consultative Process. The Secretary of Homeland Security is required to establish a broad consultative process to coordinate improvements in the cybersecurity of critical infrastructure.

Cybersecurity Workforce. The Secretary of Homeland Security is required to coordinate technical assistance to critical-infrastructure regulatory agencies on development of their cybersecurity workforce and programs.

High-Risk Critical Infrastructure. The Order requires the Secretary of Homeland Security to use consistent and objective criteria, the consultative process established under the Order, and information from relevant stakeholders to identify and update annually a list of critical infrastructure for which a cyber attack could have catastrophic regional or National impact, but not including commercial information technology products or consumer information technology services. The Secretary must confidentially notify owners and operators of critical infrastructure that is so identified of its designation and provide a process to request reconsideration.

Privacy and Civil Liberties. The Order requires agencies to ensure incorporation of privacy and civil liberties protections in agency activities under the Order, including protection from disclosure of information submitted by private entities, as permitted by law. The DHS Chief Privacy Officer and Officer for Civil Rights and Civil Liberties must assess risks to privacy and civil liberties of DHS activities under the Order and recommend methods of mitigation to the Secretary in a public report. Agency privacy and civil liberties officials must provide assessments of agency activities to DHS.

Implementation Deliverables and Deadlines

The Order contains several requirements with deadlines, and other requirements with no associated dates. In March 2013, DHS announced that it had formed a task force with eight working groups focused on the various deliverables for which it is responsible.[6] There are 12 deliverables with specific associated dates:

June 12, 2013

- Instructions for producing unclassified threat reports (Secretary of Homeland Security, Attorney General, Director of National Intelligence) (Sec. 4(a)).
- Procedures for expansion of the Enhanced Cybersecurity Services Program (Secretary of Homeland Security) (Sec. 4(c)).
- Recommendations to the President on incentives to participate in the framework (Secretaries of Homeland Security, Commerce, and the Treasury) (Sec. 8(d)).
- Recommendations to the President on acquisitions and contracts (Secretary of Defense, Administrator of General Services) (Sec 8(e)).

---

[3] See, e.g., National Institute of Standards and Technology, "Computer Security Resource Center," February 20, 2013, *http://csrc.nist.gov/*.

[4] 15 U.S.C. §272.

[5] National Institute of Standards and Technology, "Cybersecurity Framework," July 2, 2013, *http://www.nist.gov/itl/cyberframework.cfm.*

[6] Department of Homeland Security, "Integrated Task Force," March 18, 2013, *http://www.dhs.gov/sites/default/files/publications/EO-PPD%20Fact%20Sheet%2018March13.pdf.*

July 12, 2013

- Designation of critical infrastructure at greatest risk (Secretary of Homeland Security) (Sec. 9(a)).

October 10, 2013

- Publication of preliminary Cybersecurity Framework (Director of the National Institute of Standards and Technology) (Sec. 7(e)).

February 12, 2014

- Report on privacy and civil liberties, preceded by consultations (Chief Privacy Officer and Officer for Civil Rights and Civil Liberties of DHS) (Sec. 5(b)).
- Publication of final Cybersecurity Framework (Director of the National Institute of Standards and Technology) (Sec. 7(e)).

May 13, 2014

- Reports to the President on review of regulatory requirements (agencies with regulatory responsibilities for critical infrastructure) (Sec. 10(a)).
- Proposed additional risk mitigation actions (agencies with regulatory responsibilities for critical infrastructure) (Sec. 10(b)).

February 12, 2016

- Reports to the Office of Management and Budget on ineffective, conflicting, or burdensome requirements (agencies with regulatory responsibilities for critical infrastructure) (Sec. 10(c)).

The Order also includes more than 20 actions for which no specific date is provided. While many of the activities under the Order are in the process of development, some provisions may already have had some effect. For example, the provision on expedited security clearances was apparently used in responses to a cyber attack this past spring on several banks, to facilitate communication by the FBI with the banks.[7]

RELATIONSHIP OF THE EXECUTIVE ORDER TO THE PRESIDENTIAL POLICY DIRECTIVE

Presidential Policy Directive 21 (PPD 21),[8] *Critical Infrastructure Security and Resilience*, on protection of critical infrastructure, was released in tandem with Executive Order 13636. PPD 21 supersedes Homeland Security Presidential Directive 7 (HSPD 7), *Critical Infrastructure Identification, Prioritization, and Protection*, released December 17, 2003. PPD 21 includes cybersecurity broadly as a need to be addressed along with physical security. It seeks to strengthen both the cyber- and physical security and resilience of critical infrastructure by:

- clarifying functional relationships among Federal agencies, including the establishment of separate DHS operational centers for physical and cyber-infrastructure;
- identifying baseline requirements for information sharing, to facilitate timely and efficient information exchange between Government and critical-infrastructure entities while respecting privacy and civil liberties;
- applying integration and analysis capabilities in DHS to prioritize and manage risks and impacts, recommend preventive and responsive actions, and support incident management and restoration efforts for critical infrastructure; and
- organizing research and development (R&D) to enable secure and resilient critical infrastructure, enhance impact-modeling capabilities, and support strategic DHS guidance.

Implementation Deliverables and Deadlines

June 12, 2013

- Description of functional relationships within DHS and across other Federal agencies relating to critical infrastructure security and resilience (Secretary of Homeland Security).

July 12, 2013

- Analysis of public-private partnership models with recommended improvements (Secretary of Homeland Security).

---

[7] Joseph Menn, "FBI Says More Cooperation with Banks Key to Probe of Cyber Attacks," *Reuters,* May 13, 2013, *http://www.reuters.com/article/2013/05/13/us-cyber-summit-fbi-banks-idUSBRE94C0XH20130513.*

[8] The White House, "Critical Infrastructure Security and Resilience," Presidential Policy Directive 21, February 12, 2013, *http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil*.

August 11, 2013

- Convening of experts to identify baseline information and intelligence exchange requirements (Secretary of Homeland Security).

October 10, 2013

- Demonstration of "near-real-time" situational-awareness capability for critical infrastructure (Secretary of Homeland Security).
- Updated National Infrastructure Protection Plan that addresses implementation of the directive (Secretary of Homeland Security).

February 12, 2015

- First quadrennial National Critical Infrastructure Security and Resilience R&D Plan (Secretary of Homeland Security).[9]

In addition to DHS, the Directive describes specific responsibilities for the Departments of Commerce, Interior, Justice, and State, the intelligence community, the General Services Administration, the Federal Communications Commission, the sector-specific agencies, and all Federal departments and agencies.[10]

RELATIONSHIP OF THE EXECUTIVE ORDER TO THE CYBER INTELLIGENCE SHARING AND PROTECTION ACT (CISPA, H.R. 624) AND OTHER LEGISLATION

A number of observers, both in the Federal Government and the private sector, have stated that Executive Order 13636 is not sufficient to protect U.S. critical infrastructure from cyber threats, and that legislation is needed. In 2011, the White House proposed legislation with provisions on personnel authorities, criminal penalties, data breach notification, authorities of the Department of Homeland Security (DHS), a regulatory framework for cybersecurity of critical infrastructure, and reform of the Federal Information Security Management Act (FISMA). Related provisions also appeared in bills introduced in recent Congresses. Both the White House proposal and several bills have contained incentives for information sharing by the private sector with the Federal Government and other private entities, including protection from legal liability and exemption from provisions in the Freedom of Information Act.

At a hearing before the Senate Committee on Homeland Security and Governmental Affairs in September 2012, Secretary of Homeland Security Janet Napolitano stated that in addition to the Executive Order, there were at least three things for which legislation would be necessary: Personnel authorities, liability protections, and criminal penalties (S. Hrg. 112–639, p. 23). A number of private-sector entities have also stated that liability and disclosure protections are needed to encourage private-sector information sharing.

Among the cybersecurity bills that have been introduced in the 113th Congress, H.R. 624, the Cyber Intelligence Sharing and Protection Act (CISPA), which passed the House in April, addresses information sharing. Some provisions in CISPA, as in the Executive Order, would provide for expedited security clearances and sharing of classified information by the Federal Government with the private sector. The bill would additionally permit entities providing cybersecurity services to themselves or others (which the bill calls cybersecurity providers) to obtain and share threat information for purposes of protection, notwithstanding any other provision of law.

CISPA would also make such entities and those they protect exempt from liability for good-faith use of cybersecurity systems to obtain or share threat information and decisions based on such information.

In the Senate, the Committee on Commerce, Science, and Transportation is reportedly drafting a bill that would provide a legislative basis for NIST's role in developing and updating the framework in the Executive Order.[11] The draft bill would also reportedly require a Federal cybersecurity research and development plan, as would H.R. 756, the Cybersecurity Enhancement Act of 2013, which passed the House in April. PPD–21 requires an R&D plan that addresses security and resiliency for critical infrastructure, including cybersecurity.

---

[9] PPD 7 gave primary responsibility for coordinating R&D to the Office of Science and Technology Policy.

[10] PPD 7 did not describe specific responsibilities of the intelligence community, the General Services Administration, or the Federal Communications Commission.

[11] John Eggerton, "Rockefeller, Thune Circulate Cybersecurity Draft," *Broadcasting & Cable*, July 12, 2013, *http://www.broadcastingcable.com/article/494447-Rockefeller__Thune__Circulate__Cybersecurity__Draft.php*.

PRIVATE-SECTOR REACTIONS TO THE EXECUTIVE ORDER

Given the absence of enacted comprehensive cybersecurity legislation, some security observers contend that the Executive Order is a necessary step in securing vital assets against cyber threats. Some observers, however, have raised concerns.[12] Common themes by such critics include the following claims:

- *The Order offers little more than do existing processes.* Such critics point out that, for example, the Enhanced Cybersecurity Services program was in place before the release of the Order, and that a variety of efforts have been underway to develop and adopt voluntary standards and best practices in cybersecurity for many years. Proponents of the Order argue that it lays out and clarifies Obama administration goals, requires specific deliverables and time lines, and that the framework and other provisions are in fact new with the Executive Order.
- *The Order could make enactment of legislation less likely.* These critics express concern that Congress might decide to wait until the major provisions of the Order have been fully implemented before considering legislation. Proponents state that immediate action was necessary in the absence of legislation, and that changes in current law are necessary no matter how successful the Executive Order might be, to provide liability protections for information sharing and to meet other needs.
- *The process for developing the framework is either too slow or too rushed.* Some observers believe that some actions to protect critical infrastructure are well-established and should be taken immediately, given the nature and extent of the current threat. They state that the year-long process to develop the framework may delay implementation of needed security measures[13] and creates unnecessary and unacceptable risks. Others counter that widespread adoption of the framework requires consensus, which takes time to achieve, and that the 1-year time frame may be insufficient, given that the process for developing and updating consensus standards often takes several years. Some also state that the framework process does not preclude entities from adopting established security measures immediately.
- *The framework risks becoming a form of de facto regulation, or alternatively, its voluntary nature makes it insufficiently enforceable.* Another concern of some is that it could lead to Government intrusiveness into private-sector activities, for example through increased regulation under existing statutory authority,[14] while others contend that voluntary measures have a poor history of success. Some others, however, have argued that changes in the business environment—such as the advent of continuous monitoring, more powerful analytical tools, and a better prepared workforce—improve the likelihood that a voluntary approach can be successful.[15]
- The Order could lead to overclassification or underclassification of high-risk critical infrastructure by DHS. Some observers have expressed concern that the requirement in the Order for DHS to designate high-risk critical infrastructure may be insufficiently clear and could lead to either harmfully expansive des-

[12] See, for example, Paul Rosenzweig and David Inserra, *Obama's Cybersecurity Executive Order Falls Short*, Issue Brief No. 3852, February 14, 2013, *http://www.heritage.org/research/reports/2013/02/obama-s-cybersecurity-executive-order-falls-short*; Dave Frymier, "The Cyber Security Executive Order Is Not Enough," *Innovation Insights: Wired.com*, March 1, 2013, *http://www.wired.com/insights/2013/03/the-cyber-security-executive-order-is-not-enough/*.

[13] For example, some suppliers to the Federal Government have reportedly called for suspension of procurement rulemaking relating to cybersecurity until the framework has been published (Aliya Sternstein, "Contractors Ask GSA to Freeze Cyber-Related Regulations," *Nextgov*, May 17, 2013, *http://www.nextgov.com/cybersecurity/2013/05/contractors-ask-gsa-freeze-cyber-related-regulations/63244/?oref=nextgov_cybersecurity*).

[14] For example, some believe that the framework, while voluntary, "could develop in such a way that companies will be forced to adopt prescriptive standards due to the fact that information on program adoption for 'high-risk' industries may be made public. More concerning, this could be done without a review process and could be used to leverage [sic] in ways that may not be beneficial to lowering overall risk" (Testimony of David E. Kepler, Senate Committee on Homeland Security and Governmental Affairs and Senate Committee on Commerce, Science, and Transportation, "The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security," hearing, March 7, 2013, *http://www.hsgac.senate.gov/hearings/the-cybersecurity-partnership-between-the-private-sector-and-our-government-protecting-our-national-and-economic-security*).

[15] CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.; Mike McConnell et al., *The Cybersecurity Executive Order* (Booz Allen Hamilton, April 26, 2013), *http://www.boozallen.com/media/file/BA13-051CybersecurityEOVP.pdf*.

ignations or inappropriate exclusions of entities.[16] This might be particularly a problem if the criteria are not sufficiently validated.[17]

It appears to be too early in the development of the components of the Executive Order to determine how the concerns described above will be addressed and whether the responses will satisfy critics and skeptics. Overall, however, response to the Order from the private sector—including critical-infrastructure entities, trade associations, and cybersecurity practitioners—appears to be cautiously optimistic.

Mr. MEEHAN. Well, thank you Dr. Fischer.

I thank each of the panelists for your opening statements.

Now I recognize myself for 5 minutes of questions.

Dr. Romine, let me just start with you because the focus of our hearing today is NIST and the work that has been done, and I know you gave a little bit of an opening with regard to some of the progress, but give me a sense as to where you are by virtue of the three separate meetings that have been done and what you expect will be the next most critical steps moving into the meetings in Dallas next month.

Mr. ROMINE. Thank you for the question. I am actually quite excited by the progress that we have made and the response that we have gotten from the private sector.

One of the concerns that you always have when you begin an issue like this is ensuring that you get a good participation and a vigorous discussion with the private sector if you are going to establish a voluntary program with the framework as the backbone.

I am really gratified in two ways. We have gotten vigorous discussions and vigorous debate and we have achieved over the course of a relatively short time a lot of consensus on the overall structure of the framework. We are going to take that, the consensus that we have received in San Diego just last week on elements of it and establish a pretty solid draft framework in preparation for the meeting in Dallas.

As you know, the deliverable will be immediately after or just a short time after the Dallas——

Mr. MEEHAN. What do you think the essence of that deliverable is going to be? What was going to come out at the conclusion of this process?

Mr. ROMINE. So I think there are a few key elements to the framework that have to be there. One is an executive summary that is digestible by the very senior leadership of corporations, companies, the owners and operators of the critical infrastructure.

This is something that they are going to have to integrate into their business decision process, and so we have to convey enough information in a way that is digestible to them so that they——

Mr. MEEHAN. I guess—who and how? That is part of what a lot of this is—you know, the questions become—we often talk about

---

[16] Testimony of Roger Mayer, House Committee on Energy and Commerce, "Cyber Threats and Security Solutions," hearing, May 21, 2013, *http://energycommerce.house.gov/hearing/cyber-threats-and-security-solutions*.

[17] The Government Accountability Office (GAO) expressed similar concerns about DHS's National Critical Infrastructure Prioritization Program (NCIPP) list of highest-priority U.S. infrastructure (Government Accountability Office, *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress*, GAO–13–296, March 2013, *http://www.gao.gov/assets/660/653300.pdf).* The relationship between the NCIPP list and that under the Executive Order has raised some concerns. There appear to be some differences between the lists that have resulted in some disagreements with the private sector (see, for example, Testimony of Dave McCurdy, House Committee on Energy and Commerce, Cyber Threats and Security Solutions, hearing, May 21, 2013, *http://energycommerce.house.gov/hearing/cyber-threats-and-security-solutions*).

the weakest link, but there is also the—when you talk about business and other kinds of, you know, public and private-sector entities that it is an endless process of who may or may not be included.

Who do we think this is targeted to, you know, to be received by, and what kind of activity are we expecting them to undertake as a result of the creation of the standards?

Mr. ROMINE. Well, I think the goal is for all of the critical infrastructure sectors that have been identified through the DHS process and are going to be responsive to the adoption of this voluntary framework and that includes companies at various levels of both sophistication and various levels of import in terms of the critical infrastructure.

So there are going to be some very major corporations who already have a lot of mature business processes in place and cybersecurity risk assessment in place to adopt the framework because they may be the most critical of the critical infrastructures and I am sure Mr. Kolasky——

Mr. MEEHAN. Mr. Kolasky, let me jump onto that with you in terms of the identification of this most critical infrastructure because this is one of the pieces as well, and while I know you can't talk with specificity about that at this point in time because my understanding is that it will be something that will be more or less protected information, but where do you come off of the work that is being done in here and how will the identification of specific sectors uniquely vulnerable relate to what is being done and how about those that are not identified as the most vulnerable but will still be out there in commerce?

Mr. KOLASKY. Sure. Thank you, Chairman Meehan.

First and foremost, to do the work to identify the critical infrastructure where cybersecurity incident could cause catastrophe, we had to work with all of the 16 critical infrastructure sectors and we set up a process to do so.

In doing so, we identified the critical functions that each of those infrastructure produce. That and analytic work done in collaboration with industry is very helpful for understanding the overall scope of critical infrastructure in a relationship with cybersecurity which will help the framework adoption.

In terms of the actual critical infrastructure that we have identified or are in the process of identifying, it is a relatively small list. It is a list where we think a cybersecurity incident can cause public safety or significant economic damage or National security implications, we plan to work with those industries, those entities, those businesses——

Mr. MEEHAN. Are many or most of those industries already pretty far along in terms of their commitment to cybersecurity or are you concerned about some real outliers?

Mr. KOLASKY. I think it is fair to say that we are confident that they are very well along with cybersecurity. Most of those entities we have on-going relationships with and we plan to continue those on-going relationships. We will work with them to identify risk management approaches and provide Federal resources to support them, but we are confident that they have taken a cybersecurity

problem very seriously and that they have gone a long way in mitigating their vulnerabilities.

Mr. MEEHAN. Okay.

Well, thank you.

My time is expired, but I know we are going to have an opportunity to ask a series of questions, so I look forward to exploring it further.

The Chairman now recognizes the gentlelady from New York, Ms. Clarke.

Ms. CLARKE. Thank you—thank you very much, Mr. Chairman.

The privacy and the civil liberties protections established in the Executive Order process are to be consistent with the fair information practice principles including the principle of data minimization.

What steps are being taken to ensure that once a final framework is in place personally identifiable information that is irrelevant and unnecessary to accomplish a specified cybersecurity purpose will not be collected?

I want to extend that question to all of the panelists.

Mr. ROMINE. Well, I can certainly start on the development on the framework through the workshops. I will give a specific example in San Diego. We had a separate breakout section specifically devoted to privacy and civil liberties issues where we got the chance to engage with a broad cross-section of stakeholders and received their input on the importance and some of the techniques that are already being used by these industries to ensure protection of privacy and civil liberties.

That was led by my laboratory's senior advisor for privacy, a position that I am committed to. I think that is an important position for an information technology laboratory to have. So I am very proud of that.

We also at NIST have the information security and privacy advisory board or ISPAB, a Federal advisory committee that we keep apprised of our activities that are relevant in that space and so we engage with them and we are hoping to engage with the privacy and civil liberties board that has been recently reconstituted as well. It is baked into many of the discussions that we have during the framework development.

Ms. CLARKE. Do either of you have——

Mr. KOLASKY. Sure. I would just add that across the EO, the PPD as part of the integrated task force, we have stood up an assessments working group particularly thinking of privacy and civil liberties assessments for all of the work that is going on with the EO PPD.

We did this at the front end of the work and these members have been sitting on our working groups and working in collaboration across the interagency because we very much want to bake privacy and civil liberties into all the work we are doing rather than review and assess at the end of it.

Ms. CLARKE. Very well. Let me move on to my second question then.

Section 5(a) of the Executive Order requires agencies to coordinate their activities with their senior privacy and civil liberties officials. Are senior privacy and civil liberties officials at each agency,

being NIST and DHS—excuse me—are these civil liberty officials at each agency given the opportunity to provide substantive policy recommendations during the development of the phase of the framework? Can you expand on their role in the process?

Mr. KOLASKY. As I was just talking about with the assessments working group, very much so. This is a collaboration across the senior civil liberties and privacy officials.

It has been a great opportunity in some of the departments and agencies. Traditionally these folks haven't worked on critical infrastructure issues.

It has created a community practice and they been given an opportunity in addition, you know, with all our work we are briefing the advocacy community and other interested parties regularly on what is going on.

Ms. CLARKE. Very well.

Mr. ROMINE. I would say within the Department of Commerce, the privacy and civil liberties officer at NIST is our chief information officer. He is down the hall from me. I get the opportunity to talk with him on a regular basis about everything that our laboratory is doing including this effort.

At the Department of Commerce, as you know, it is the Secretary of Commerce who was directed by the President to direct the director of NIST under the Executive Order to undertake this framework development and they are certainly aware of all of the actions that we are taking.

They are at the Secretary's level—they have the Privacy and Civil Liberties Office and they are certainly aware as well.

Ms. CLARKE. Very well.

Let me ask Mr. Kolasky, Presidential Policy Directive 21 which accompanied the Executive Order requires an evaluation of existing public-private partnership model and recommendations for improving public/private collaboration.

Can you characterize for the committee the current status of the public/private partnership model and what steps are being considered to improve the model?

Mr. KOLASKY. Sure, yes, ma'am. First of all, we delivered this report last week and I think the good news is we really do believe that the model has been established over the last 15 years to work on critical infrastructure security and resilience is working and has the potential to work to solve tough critical infrastructure security and resilience issues.

I think the process that we have been undergoing over the last 6 months is a great demonstration of that. There were improvements that can be made but the key is to understand that we have been able to collaborate with the private sector through these processes and work with State and local and Tribal territorial governments.

The reason I think we can do that is there is a shared sense of purpose. We have improved communications. We are working toward joint priorities and things like that. That all leads to trust. Nothing is more important to trust that industry and Government and at different levels of government can come together to work on these issues.

In terms of recommendations going forward, we—as I said, although it is working we think there are some enhancements that can be made. We would like to move from more of a process-focused and outcome-focused partnership.

We would like to use the partnership to set joint National priorities, and I think that is an important step. We would like to explore how to promote regional networks and bring some of the good work down to the regional level, and finally we would like to look at new methods to unleash innovation through public and private programs.

Ms. CLARKE. Thank you all very much. I yield back, Mr. Chairman.

Mr. MEEHAN. I thank the gentlelady.

The Chairman now recognizes the distinguished gentleman from Pennsylvania, the former United States attorney, from the middle District of Pennsylvania, Congressman Marino.

Mr. Marino.

Mr. MARINO. Thank you, Chairman.

Good morning, gentlemen, and I apologize for being late and not hearing all of the opening statements. I am trying to juggle three and four things as my colleagues know that we do.

I have a concern following up on my colleague across the aisle as far as security but from a different perspective. We have certainly seen where this administration has a series of bungles concerning IRS, Benghazi, Fast and Furious, but the President happens to come up with, "I didn't know about it," "I don't know anything about it," and usually there is a low-level person that gets blamed for it—who is still on the payroll as a matter of fact.

So what can you do, what can be done if the President is going to take the responsibility for this to make sure that we don't have Snowdens running around gathering critical information about what we are doing and those involved and then sharing it with our enemies?

Mr. Kolasky, perhaps you could start with this.

Mr. KOLASKY. Sure. Thank you, Congressman, and thank you for the question.

As you know, this is an important issue that whatever we do we need to protect the security of the information that we are providing and that we are collecting.

The security approaches within the Executive Order relate to information sharing and we are thinking of it in two different ways; one of which is we are working to separate Classified information from Unclassified information and focus on getting Unclassified information on how to mitigate cyber vulnerabilities based on cyber threats out as efficiently and quickly as possible in an actual manner to help industry take action to mitigate those threats.

That is a very important step. This doesn't have to be done at a Classified level in a lot of places and if we can improve those processes, that will help very much.

The second side to promote the protection of Classified information, we have made improvements in our enhanced cybersecurity service program and made that available to a limited number of commercial service providers to promote the airing of information

we have about cyber threat indicators and these are particular cyber threat indicators.

They are things like malware and email language and we want to make sure that is available but we want to make sure that security is protected in doing so and finally we want to make sure that anyone that gets a security clearance in Government has undergone proper vetting.

Mr. MARINO. Thank you.

Doctor, please.

Mr. ROMINE. Congressman, from the standpoint of the framework, I think your question really relates principally to the idea of risk mitigation strategies for the insider threat.

So that has been a source of on-going discussion, but as a part of a more general discussion among owners and operators of critical infrastructure to ensure the, sort of, full risk management approach for cybersecurity and that includes both the insider threat as well as Congresswoman Clarke's concerns about protection of privacy and civil liberties.

Mr. MARINO. Doctor.

Mr. FISCHER. Thank you, Mr. Marino. I would just like to add that I would say that a lot of experts believe that it would—it is basically impossible to prevent any, you know, insider threat from being successful——

Mr. MARINO. As a prosecutor, I am aware it is basically—it is impossible to prevent anything, but it does happen, but it just seems that it is happening ad nauseam with this administration.

Mr. FISCHER. Right. So the question then becomes, what are the levels at which that kind of problem can be tolerated, and how does it relate to the potential benefits of what is being done.

So for example, with respect to the information sharing, you know, one of the things that DHS has been doing with the enhanced cybersecurity services program is to focus—if I understand correctly—on what they call cybersecurity service or commercial service providers which have to do with the internet service providers and that sort of thing rather than opening up the dissemination of this threat information to all sorts of critical infrastructure entities, and so the critical infrastructure entities work through these CSPs.

So to the extent that that sort of thing is successful, the idea of narrowing the vulnerabilities to specific areas may be useful.

Mr. MARINO. Thank you.

I have another question, but perhaps we will have another round, and so I yield back.

Mr. MEEHAN. I thank the gentleman.

The Chairman now recognizes the distinguished gentleman from Texas, Mr. Vela.

Mr. VELA. Thank you for your testimony today.

Dr. Romine, Executive Order 13636 specifically provides that the cybersecurity framework and protection against cyber threats should include physical threats; not just computer viruses and hacking.

The White House Strategic National Risk Assessment includes natural electromagnetic pulse from a geomagnetic super-storm as an example of a physical threats to critical infrastructures.

Does the cybersecurity framework as you envision it include threats not only from computer viruses and hacking but physical threats especially from EMP?

Mr. ROMINE. I would say yes in general although EMP is not spotlighted as much as just the overall risk assessment that each of these owners and operators is going to be involved in.

When we talk about a cybersecurity and protection of critical infrastructure, we are keenly aware of the cyber physical systems nature of many of these infrastructures that the information systems are not in fact independent but rather often interact with physical or other kinds of systems.

So the risk assessment approach that we are taking or the risk management approach that we are taking in the framework is intended to encompass the impact or the risks holistically rather than just with regard to viruses and other kinds of cyber threats, traditional cyber threats.

Mr. VELA. Dr. Fischer, what additional challenges are imposed globally in terms of privacy protection and the sharing of personally identifiable information across borders?

Mr. FISCHER. Sir, Mr. Vela, could I clarify? You say what challenges to with respect to the Executive Order and——

Mr. VELA. Yes, no it is: What additional challenges are imposed globally in terms of privacy protection and the sharing of personal identifiable information across borders?

Mr. FISCHER. I see, okay.

Yes, well, two quick things I can say to that. First of all, there obviously—the work is being done within the United States is done in the context, international context and there is quite a network of international agreements.

There is no, currently, no global cybersecurity treaty. Some people have tried to—tried to draft such a thing, but it hasn't been adopted, and there are a lot of bilateral agreements which often would be the vehicles in which these sorts of concerns would, I think, be addressed.

With respect to specific—or specific questions or with respect to privacy and civil liberties, I would say that is outside of my expertise, but we do have experts on our cybersecurity team within CRS who deal specifically with those issues and we would be happy to talk with you about that or answer questions for the record.

Mr. VELA. Okay. I guess we will wait for another day on those.

For the whole panel, what are examples of effective risk-based approach in the framework?

Mr. ROMINE. So one of the exciting things that we have had in the workshops is seeing the representatives of various industries talking with each other about the approaches that they take and the effectiveness of those approaches.

One of those approaches involves something that in the energy sector is called the C2M2 which essentially regardless of that, the expansion of that, the idea is to have a, sort of, set of maturity levels associated with specific functions.

If you take a look at the framework outline that we provided in San Diego and some of the consensus that we received, that model seems to be very attractive to the vast majority of the participants and the critical infrastructures.

So that kind of risk assessment—NIST has a very strong history in risk-based management of cybersecurity through the Federal Information Security Management Act or FISMA, activities.

We have had special publications that are quite influential in this space with regard to the private sector and have been adopted widely by the public sector and have been adopted widely by the private sector as well because of their effectiveness.

Mr. KOLASKY. I would just add one of the things I have observed through the process is an example of what works is if corporate leadership gets involved in the process and we have heard that repeatedly that you have to produce a framework that resonates at the board level and resonates as the CEO level and in doing so, that will help organizations make risk management decisions.

Mr. FISCHER. I don't believe I would have anything to add it to those comments at this point. Thank you, sir.

Mr. VELA. I yield back.

Mr. MEEHAN. I thank the gentleman from Texas.

I recognize myself now for 5 minutes of follow-up questions.

One of the issues that we have been dealing with throughout the concept of not only the creation of the NIST standards but as the underlying concept of voluntary adoption of those standards and it permeates the language in the report, I mean in the Executive Order that these are voluntary.

But at the same time we are creating a framework, and I would like to explore the extent to which people begin to see this framework as a basis for further activity, not the least of which could become further activity in which that framework is used as the basis for other regulatory agencies to say that they are now authorized to begin to create required adherence to certain of these standards.

I would like the panel to individually address your perception of what voluntariness means and where you believe and to the extent certainly, Mr. Kolasky and Dr. Romine, to the extent that you are dealing with NIST, where you believe this goes to and what you believe the intention is with regard to whether these will ultimately be utilized in some way to become requirements.

Because I am aware of a number of shalls in the Executive Order and, you know, the shall-proposed, prioritized, risk-based, coordinated actions, you know, if the current regulatory requirements are deemed to be insufficient.

So please, Dr. Romine, first.

Mr. ROMINE. I can start with that. NIST has a long history of developing in coordination with industry guidelines and best practices and ultimately industry-led standards that do govern the industry in a purely voluntary way, and that has been very effective in the past, and we expect it to be effective in the future with the Executive Order and the framework.

The only way that works is vigorous participation on the part of the private sector so that they have buy-in and a stake in the outcome of the framework itself.

So I think with that understanding and the fact that we believe that we have that vigorous participation, I am not as concerned about this being a, sort of, a hidden way of getting regulatory authority. I really think the voluntary nature of it is quite explicit and quite transparent and we expect it to continue to be that way.

Mr. MEEHAN. Mr. Kolasky, what is your impression of this from DHS?

Mr. KOLASKY. Sure. First principle of ours as we participated in this is for the framework to be successful and in the attached assessments—incentives it has to make sense for businesses to make business decisions.

Businesses make rational decisions and they have to see that this is in their business interest and because of that, as Dr. Romine just referred to, it is very important to listen to businesses and we have taken that obligation——

Mr. MEEHAN. I mean, you don't question—and I often talk to businesses. Businesses will say we are way ahead of the Government in many ways because we appreciate that the exposure that we have to our business—so we are asking you, what are you doing to help us, and then I get that part. What I am concerned about is when we begin to get to a point where some businesses say hey, we think we are doing something and we start to get Washington coming in and creating a requirement.

Mr. KOLASKY. Right. That is why the voluntary nature of this is so important. If we can create confidence in the marketplace that businesses are doing something, if we can offer information to continue to incentivize them to do something, then I don't think Government needs to get involved in that kind of manner that you are talking about.

So it is really important for us to set up a framework that gives the market confidence so businesses can do business with each other and with the Government is that they are taking——

Mr. MEEHAN. So to the extent said that you speak for Department of Homeland Security and you are allowed to discuss it as a matter of policies, it is your perception that the Department is looking at this as a voluntary program?

Mr. KOLASKY. I can speak with certainty that the Department is looking at this——

Mr. MEEHAN. Dr. Fischer, you have had the ability to see these kinds of things not just in this particular area with cyber, but in the broader spectrum with other agencies in which there have been standards that have been utilized, Department of Defense, EPA, other kinds of things and in your own testimony you discussed the different pieces of this issue. Would you articulate more fully your sense as to whether or not these kinds of the voluntary standards may or have been utilized in other situations to become regulations and requirements?

Mr. FISCHER. So there are a few points I think might be useful to make here.

No. 1 is that we have been asked particularly in the last Congress by a number of Congressional offices about the question of what the current regulatory capabilities or powers are of the Federal Government with respect to cybersecurity.

Our answer had to be that there—except for cases in which they are explicitly laid out and clear—where there are such regulations such as a width of the electric power sector—it is difficult to say because until the agency actually tries to create a regulations, one doesn't know what is really going to happen because the regulatory

process is a separate process. It involves industry and other stakeholders in——

Mr. MEEHAN. But do you believe as it stands right now and I am sorry to cut you off and please go forward if you can, but I do want to ask this question. Do you believe that the way the Executive Order is written right now as it moves in it opens the door to the ability of agencies to say, in our interpretation and it may be a particular agency that may look in just say, in our interpretation, there is an opportunity here for us to use this as a basis to ask for, you know, more cyber protection in a particular area?

Mr. FISCHER. Certainly the Executive Order explicitly requires that agencies make recommendations with respect to where the gaps are. So to the extent that those gaps would be I guess fillable under current law, then it is clear that agencies could in fact attempt to create regulations in those areas.

To the extent that they are not as capable under current law, then that is the interpretation, then they would have to come to Congress for additional authority.

Mr. MEEHAN. Well, this is where they have to come to Congress for additional authority to do what? To do rulemaking of regulations because as I see this they are talking about——

Mr. FISCHER. Well, to be able to—right—so if for example the current—if the current regulation—if the current authority of an agency to create regulations is limited or the agency determines that it doesn't have the authority currently——

Mr. MEEHAN. Well, I have never—we don't have a problem here in Washington with agencies who believe that they have limited authority to enter into issues and that is why I am trying to explore this provision in the Order which says, you know, if the current regulatory requirements are deemed to be insufficient—now I don't know who deems them to be insufficient but it may be the agency itself that says hey, we believe that this is, you know, the current regulatory requirements are insufficient, you know, within 90 days we will publish a final of the—published final framework, we are going to propose, you know, further coordinated actions and that appears to me to be regulation or rulemaking.

Mr. FISCHER. Right. So to me, the question becomes whether or not the agency currently has the authority to make those rules and regulations. If they do have that authority, then they may do it anyways.

So for example, with respect to the pipeline sector and certainly we have people who can talk to very specifically about that, but with respect to pipelines, the TSA has the capability of or says that it has the capability of creating cybersecurity regulations, but they have decided that those regulations are not needed and might in fact be counterproductive to date. That is my understanding of what they have said.

So, you know, so there are examples in which they clearly—agencies apparently have not——

Mr. MEEHAN. That is left to the discretion of the agency or are they constrained by law?

Mr. FISCHER. Well, TSA appears to have that authority under current law. Now whether that is true for others is hard to say.

So for example, I would say that, generally speaking, you know, we certainly haven't found anything with respect to the IT sector that would permit such things, which isn't to say that some agency might not claim that they have it, that authority, though.

Mr. MEEHAN. All right.

Well, thank you Dr. Fischer.

I now turn it to the distinguished lady from New York.

Ms. CLARKE. Thank you, Mr. Chairman.

Just following up on the line of inquiry that our Chairman posed to you.

Mr. Romine, what does flexibility mean in the context of the framework?

Mr. ROMINE. I would say the primary reason for the need for flexibility is the different sectors have very different characteristics in the way that they operate and you have to have a framework that is capable of recognizing that.

In addition, the owner-operators might range from multibillion-dollar international corporations to relatively small regional concerns who still own and operate some portion of what is deemed to be critical infrastructure. The capabilities represented by those two things also mandates that we have a flexible approach.

Ms. CLARKE. So in effect, it is addressing the nuances of the specificity of industry and company size, what have you?

Mr. ROMINE. That is right, and I think an additional point I would make is that many of these critical infrastructures have in place a series of protections that they have invested in and believe are quite effective.

We want to be sure that the framework is flexible enough to recognize that those measures that are already being taken if they are effective should not be replaced by something else as a result of the framework. So we are trying to be mindful of that as well.

One final point I would make is that in many cases, these particular critical infrastructures are regulated already to one degree or another and in some cases, very heavily regulated, and I think the intent of this notion of regulation review is to ensure that we harmonize the framework in a way that recognizes the regulations that are already in place so that we are not committing sectors to an onerous change in the way that they do their business.

Ms. CLARKE. Very well.

Mr. Kolasky, Dr. Fischer, how can implementation of the framework be used to demonstrate compliance with existing regulatory requirements? That is, sort of, I think, where Dr. Romine was going. Is that something that you have also recognized?

Mr. KOLASKY. Yes, it is. Let me talk about it in a couple of terms. One of which you mentioned earlier, the incentives work that we have done in analysis and over and over again we heard from our private-sector partners as well as some of our advisory councils that one potential incentive would be to allow the cybersecurity framework to meet the information security requirements for already-regulated industry ergo reducing compliance costs and we think that that is something that needs to be pursued and thought about because if you can demonstrate you have got good cybersecurity in place you shouldn't have to demonstrate it twice to the Government.

Second, just to echo Dr. Romine, I think it is really important to think about the idea of regulatory relief and are there regulations in place that are going to impede the adoption of the cybersecurity framework and the Executive Order asks the regulatory agencies to think about that because we don't want regulations that are in place that will cause people from not adopting good positive flexible cybersecurity solutions.

Mr. FISCHER. I guess the only question I might have about that would be—obviously—if to the extent you have let's say many private-sector entities are—feel more comfortable with—those that are regulated—feel have developed good relations within their current regulatory environment and feel comfortable with the like, for example the electric sector, but others as well.

So they are somewhat concerned if in fact they feel that that environment will be changed to the extent that other agencies would end up being involved say in the regulation.

So to the extent that the current environment could be kept stable for them, I think they would be more receptive to the possibility of—to compliance.

I think I will stop there.

Ms. CLARKE. Dr. Fischer, that is a very intriguing statement you have made for me because I understand how industry could want to remain in a stable environment but the environment around them is changing and so to the extent, I guess it is an evolutionary process in terms of adaptation, but the status quo wouldn't necessarily work.

Mr. FISCHER. Well, we are—yes. So with respect to cyberspace, the situation is somewhat different than it may be with—in other areas. So, you know, I often say cyberspace is the most rapidly evolving technology space in human history, and the technology is evolving, the threat environment is evolving, things are changing constantly.

I think it is widely recognized within experts in this area, and the private-sector people have paid attention to this, that in fact that kind of rapid evolution means that static, particularly design-based standards, for example, have a very limited usefulness.

Now performance standards are usually considered to be better but the problem with performance standards is of course that you have to come up with what the performance criteria are and that can be sometimes more difficult and they can sometimes be more difficult to enforce.

But I think that most people who have looked at this question seriously have in fact said that well, there is basically kind of a baseline of standards that are going to be true no matter what, performance standards, but there has to be the flexibility to be able to change things on a much more rapid basis in reaction to what happens with respect to, you know, with respect to the environment.

Now I just want to say one more thing about that. There is this—it has been some time ago that, right, there is this design problem in cybersecurity that is that the cyberspace was not designed with security in mind is often said.

One of the reactions to that is well, what you have to do is build security in. Now right now, I mean, everybody kind of seems I think to agree with that, but there are two things.

No. 1 is there is always going to be a need to add things on because there is always going to be problems that you couldn't possibly anticipate when you design something.

The second point I think is that there are always or there appear to be in the current—with the current incentive structure with respect to cybersecurity—there appear to be, sort of, counter incentives to building security in from the get-go.

Now whether those are essentially fundamental or not is something that I don't think anybody really understands, but that is always, you know, an issue. So to the extent that you are going to have to add this stuff on later is a question.

Ms. CLARKE. I yield back, Mr. Chairman.

Thank you, gentlemen.

Mr. MEEHAN. I thank the gentlelady.

Just using the prerogative of the Chairman for one second, Dr. Fischer, you are articulating something which is at the heart of where we, I think, appreciate and need to be sensitive to, which is the dynamic nature of the cyber threat.

Such that what you build today as a defense will not only be analyzed but it will be—there are those who will spend their time purposely trying to get around it; therefore we have got—it is a constant state of cat and mouse, so to speak, for lack of a better word.

The framework itself that we are talking about is very admirable in the sense that it creates a place for people to begin to have a sense about what they can and should be doing, but do we create a problem if they see the framework as a check-the-box kind of thing that says, okay, now I am cyber safe.

Mr. FISCHER. Right. I appreciate the question, Mr. Chairman. One of the criticisms that has been leveled by some people, and I can't say to the degree to which they are accurate about this, but one of the things that has been leveled is that for example, by analogy with FISMA, one of the criticisms of the Federal Information Security Management Act has been that it has become something of a check-box exercise where, you know, it is very process-oriented and it doesn't really focus on the question of how you keep systems actually safe and secure.

Now there are obviously attempts to revise FISMA, to amend FISMA, and also I would say the administration has been doing—the current administration and the Bush administration as well—have been doing things to try to actually make systems secure and focus more on that aspect of what the law intends, the goals of the law.

But to the extent that the framework of, would it become a kind of bureaucratic, you know, check list, that would be a problem. I certainly wouldn't want to speak to how NIST and DHS are trying to avoid having that happen, but I am sure that they are aware of that problem as well.

Mr. MEEHAN. Thank you.

Thank you for the indulgence.

The Chairman now recognizes the gentleman from Pennsylvania.

Mr. MARINO. Thank you, Chairman.

My colleague, the Chairman and of course my colleague is a former U.S. attorney as well-spawned a thought based on his questioning and the question I am asking and that I am going to follow up with a little statement is who or whom, what person as far as general, what people, or what entities are we focusing on because several weeks ago, Mayor Giuliani came in and testified before the full committee, and I agreed with him 100 percent on his observations.

He said we cannot take our eye off of the ball but we have several balls in the air that we must be watching simultaneously.

We cannot take our eye off of al-Qaeda and there are those that think that al-Qaeda is defeated and we really don't have to worry about them anymore. I think that couldn't be any more from the truth than anything at all.

But then there are individuals that think we need to focus on individual terrorists, who the leaders of the terrorist organizations persuade some fanatic, young terrorist to do something whether that is through propaganda or initial contact—and by the way, you never see the terrorists who are running the organizations strap bombs to themselves or their families, it is always that they convince somebody else to do it.

But Giuliani was very specific saying we have to keep our eye on the rogue such as the Boston terrorists and organizations such as al-Qaeda and without tipping the cards, what say each of you about where we are as far as watching the whole scheme? Do you understand my question?

Mr. Kolasky.

Mr. KOLASKY. Sure. Thank you, Congressman Marino.

It is a hard challenge, and that is what is so important about the intelligence component of this and we have made a lot of investments in trying to understand both the adversaries' tactics and the nature of the adversary and, you know, their incentives and what they are trying to do and we will continue to make those investments and as we learn from that, as I talked about earlier, one of our jobs is to get the information out to those who are protecting the networks so they know what to be looking for.

This threat, unfortunately, is coming from a lot of different places. It is coming from international, it is coming from domestically, it is coming from the mid-level hackers in the organized coalitions, and in criminals.

And so because of that, we have to learn and we had to get that information out to folks at an Unclassified level so that they can protect their networks.

Mr. MARINO. Sure, and as you mentioned, we do have the individual hackers, we do have the genius kid and we have, I think, still al-Qaeda and other organizations, and we have the Chinese. So I am just hoping that we are keeping—I am pretty sure we are keeping our eye on each one of these entities.

Doctor, would you please respond?

Mr. ROMINE. I would say from the framework's standpoint and though work that NIST is doing, the threat space is very broad and evolving as you have correctly noted and part of Congresswoman Clarke's question, if I could amend my answer, I would also include

the evolution of the threat space as an important component of being flexible in our response.

I think the goal of the framework is to assist the private-sector owners and operators to raise the bar as much as we can in the cybersecurity space so that all of these threat vectors are—it is much, much more difficult to cause harm to the United States regardless of whether you are in a basement or in a foreign country.

Mr. MARINO. Thank you, Doctor.

Mr. FISCHER. Yes. Well, I tend to—we tend to think about different classes of potential actors with respect to threats. So clearly as you mentioned, I mean, you have on the one hand there is the criminal element and often they are interested in, you know, financial gain through illegal means; basically ordinary crime through cyber means is what it amounts to. But increasingly, there appears to be an organized crime element of—with respect to cyber attacks as well.

Then there is what you might call the cyber hacktivists—the—or—you know, sometimes there is just, sort of, you know, the script kiddie types, you know, people who are trying to just, you know, created an exploit of some sort. But also, those are making some political statement.

Then the third is would be the terrorists, the al-Qaeda types, and the like that are more organized and have a specific political goal and then finally the, kind of, state actors, you know, which sometimes called the advanced, persistent threats if you don't want to give a name to a particular country.

But all those are going to have—those actors are going to have different goals. They are going to have different levels of sophistication. I think that to the extent that the—you know, that the framework and the other aspects of the EO and PPD can in fact take those into account, obviously they will be more effective.

Mr. MARINO. Gentlemen, your task is monumental and I appreciate what you are doing for this country.

I yield back.

Mr. MEEHAN. Thank the gentleman from Pennsylvania.

The Chairman now recognizes the distinguished former prosecutor from Massachusetts.

Mr. KEATING. Thank you, Mr. Chairman.

Thank you, Ranking Member Clarke, for having this important meeting.

Just quickly, I just want to hone in on one thing is that as you go about the task, both with, you know, establishing the framework around the Executive Order of the President and as you are dealing with the National Institute responsibility of developing a framework to secure the information, in this whole process, is it going to be role carved out more specifically, or at least the flexibility for universities to get more involved and other involved Northeastern, in my own home State, has worked very closely with some of you folks.

But I want to just see what your view is and is there because I think it is critically important. I think it is an area where you have maybe information gathering and research done that may not be biased by existing economic impacts to an individual business although there are some.

Also it is another important area for us not just with Homeland Security but in terms of other Government agencies and private agencies as well to really develop trained people which I see as one of the major problems that we will continue to have as people move in and out of the private-sector jobs.

That we really need the intellectual and educational brainpower to keep up as well. So I see the benefits of universities being great. Could you just comment on what you are going to do; how they have a place in this?

Mr. ROMINE. Certainly, and thank you very much for the question.

You are absolutely right. It is no accident that the three working sessions or workshops that we—two that we have already held and one that we are going to be holding are at university venues—we had our second overall workshop was at Carnegie Mellon University. The third one which we had last week was at the University of California at San Diego and the next is going to be at the University of Texas, Dallas.

That is an attempt, an explicit attempt on our part to engage a cross-section of the academic community as well. We have strong relationships with many academic institutions and I couldn't agree more.

One of the risks that has been identified consistently in many of our cybersecurity efforts but certainly during the framework development with industry is industry telling us as well that workforce—a cyber-educated workforce is a key risk that they see—the lack of the ability to attract cybersecurity talent.

So, I agree with you. I think the other thing, the other role that the universities can play is at the point where we have identified a substantial gap whether it is in the standards space or whether it is in the technology space, universities are well-poised to help us in that area as well.

Mr. KEATING. Great. Well, thank you, and I would particularly appreciate anything that you might offer to me and the committee as a whole to tell us what we can do to try and encourage that because I see those gaps and I see them as becoming more and more of a problem going forward.

So with that, I will yield back my time and I think my colleague also for letting me go. Thank you.

Mr. MEEHAN. The Chairman now recognizes the gentleman from Texas, Mr. Vela.

Mr. VELA. Yes, I have a couple more questions for the panel.

Section 9(b) of the Executive Order allows other Federal agencies to share information with the Department of Homeland Security to identify at-risk infrastructure.

Since the Executive Order was issued in February, what has been the nature of this inter-agency information sharing?

Mr. KOLASKY. Sure, thank you, Congressman.

So that specific task has been met by us working with the sectors of the critical infrastructure sectors to identify critical infrastructure. So this has necessitated close collaboration with the sector-specific agencies particularly agencies like the Department of Energy, the EPA, the Department of Transportation, and others, Health and Human Services and others.

So the nature of that engagement is really to understand how these sectors come to work and to bring in private-sector partners to have a conversation. We have focused largely in doing that work in understanding the most critical infrastructure in the infrastructure that can cause high consequences so it is critical that we have the folks who understand how those industries work, bringing them to the table, and then we work with our industry partners to understand if there is any nexus to cyber technologies.

Mr. VELA. Have the Department of Defense, law enforcement, or intelligence communities shared information with DHS under this provision?

Mr. KOLASKY. Sure. The Department of Defense is also a sector-specific agency. It is the sector-specific agency for the defense industrial base and so we work closely with them in that regard.

The law enforcement community and intelligence community were involved in the discussions on the methodology and the approach we took, but given that the approach largely focused on understanding how systems work and consequences related to systems failing, those are questions that are largely outside of the sphere of the intelligence community and the law enforcement community.

So although they participated in the discussions, they have not really been the focus of the information sharing.

Mr. VELA. Mr. Kolasky, Section 9(a) requires that the Secretary of Homeland Security in consultation with private-sector partners and other relevant agencies identify critical infrastructure at the greatest risk. What criteria is being used for this purpose?

Mr. KOLASKY. Sure, sure. The Executive Order talks about the criteria in terms of public safety and health consequences, economic consequences, and the impact to National security.

So as we defined that, when we are talking—and it uses the phrase catastrophic—and we take that phrase to be a fairly high threshold—so catastrophe is something that is very significant to this country either at a National or regional level.

So as we have developed a criteria, we have looked to pass critical infrastructure efforts and we thought about economic security and economic loss in terms of tens of billions of dollars, significant loss of life, and negative ability for us to project power, our military to protect power through National security needs.

Mr. VELA. Last week, the administration held its first strategic economic dialogue with Chinese officials. Administration officials cited progress in the talks while stating that continued intellectual property theft originating from China was unacceptable. How does the Executive Order help stem the loss of intellectual property? I don't know who is best to answer that question.

Mr. KOLASKY. I think very much intellectual property theft is one of the cybersecurity incidents that we are very cognizant of, so our information-sharing efforts certainly take that into account; so do our protective efforts in the work that is being done via the framework.

Mr. ROMINE. I would just add that intellectual property loss is one of the risks that the owners and operators do face in the critical infrastructure domain and so to that extent, it fits into the

overall risk management and risk mitigation strategy that the framework promotes.

Mr. FISCHER. You know, I would just like to add that the economics of cybersecurity both even with respect to the question of what real losses are and what it means is an area that is currently undergoing a lot of examination. A lot of things about it aren't clear.

It depends on the scale at which one is looking at it, whether you are looking at it on the scale of an individual company or the scale of a country or global scale, and from some of the efforts I have seen, I think there is a pretty good chance that there will be a lot of clear understanding of that over the next year or so.

Mr. VELA. Thank you. I yield back my time.

Mr. MEEHAN. I thank the gentleman.

I just have some closing questions. If I may, and they really go into two areas. Let me start with one. You know, we have mentioned the issue of liability a number of times as we move into this and it is sort of the back-end of incentives in some ways because we are trying to incent our partners to step up to the plate.

But I also, in my experience, and of course we have work to jointly here on this committee with ourselves and with staff from both sides of the aisle reaching out to a cross-section of participants in the various sectors, and the input has been good because it really gives you a sense as to the way they see the world why they are trying to evaluate the threat.

But one of the concerns is a lot of folks are already struggling with where they make commitments of resources when it is hard to define what the impact of, you know, protective stances is so that you could do an endless amount of investment and not be certain how much you are increasing your security.

Therefore, there is a concern about, you know, steps that are being taken. What happens if we create this framework that then is utilized as a basis for somebody to say rightly or wrongly in litigation you should have taken some steps? Where does it start to become a standard that becomes something that is used?

Dr. Fischer, do you have a thought on that?

Mr. FISCHER. Well, I just—sort of following up on a previous question with respect to this—one of the things that can happen with voluntary standards is that if they become a business norm, then of course businesses that don't follow those standards can be subject to certainly criticism and potentially lawsuits.

So that would certainly be something that would have to be paid attention to. I think that is what you are referring to and what some critics of the framework have said with respect to a voluntary framework becoming effectively de facto mandatory.

Now I should mention that, you know, with respect to the particular legal issues, that is outside of my area of expertise, but we do have experts on our team who can talk with you about it.

Mr. MEEHAN. All right. Thank you.

Let me just step into one last thing so long as we are here. The gentlelady from New York in her opening statement identified a document that I am also in possession of and it is called as the "DHS Incentive Study Preliminary Analysis and Findings", Mr.

Kolasky, and of course it is as I am sure with anything, when it is called preliminary, this represents some of the current thinking.

But I would like to explore if I can some of this which is before us because it looks at the very concept of incentives and maybe you can explain to me what the document is first and then there are a few specific questions——

Mr. KOLASKY. That is a work product that we shared on May 21 in advance of us delivering a document to the White House on June 12. That work product was shared broadly with our working group in the integrated task force, which includes representatives from industry.

What we were trying to do there is present a look at the research that is out there and get feedback from the owner-operator community to help us shape our final recommendations. So I think it is fine that you have the document because we made it regularly—we made it widely available so we could collect feedback so we could hone in on our recommendations and then I am happy to talk about——

Mr. MEEHAN. Well, if you can, can we walk down a couple of things here because I know that you know, we are discussing first the idea of a legislative proposal. Can you indicate to me what is meant by a legislative proposal and what is the intention of DHS or the administration or others to introduce new or additional legislation in the area of cybersecurity?

Mr. KOLASKY. Sure. Again, we are still, at the administration level, we are still having conversations. DHS issued a report. So did the Department of Treasury. So did to the Department of Commerce as well as GSA and DOD on Federal procurement incentives and so my understanding and in talking with administration, is those four reports that are up there and we are now talking at the administration level, the policy process and steps forward as you refer to in the document.

Some of the incentives that have been recommended by various folks along the way and incentives reports would take legislative action and so there is a possibility that the administration would come and talk to you all about particularly——

Mr. MEEHAN. So as you are looking into the future, but, you know, we have been working on a bipartisan basis to try to consider whether there are legislative steps that ought to be taken in addition to and some argue that legislation is necessary—legislation, we believe necessary to help you in your job in terms of codifying the ability of DHS and then further to give DHS the ability to be a point of importance as we move forward.

So in light of the fact that legislation generally begins in the Congress, it would be very good if conversations about legislation include us.

Mr. KOLASKY. I think we are happy to do that and happy to have conversations particularly on the incentives and I will echo my opening statements that as we pointed out, we appreciate the fact that one of the things that we hope is in the new legislation is to codify some of DHS's roles in general and cybersecurity and also that some of these incentives if we think they make sense, we have to work together to put them in place because they are outside of the authority of the Executive branch.

Mr. MEEHAN. Okay. Can I ask, there is a couple of things in here—you talk about insurance, removed as an independent category of incentives and we are going to put it into the cybersecurity act. What steps are being considered with respected to insurance?

Mr. KOLASKY. So what we said in our incentives report is we are very much in favor of the evolution of the cyber insurance market. We think that a lot of progress has been made independent of Government action to create a cyber insurance market and we hope that that will continue. The best incentives are market-based incentives.

In terms of if you are thinking about—and what that refers to—if you are thinking about any liability protections of that need to be put in place, we have to think carefully as you have talked about, Congressman Meehan, we have to think carefully about not creating liability protections that incent bad behavior and that any liability protections may have to be tied with insurance requirements.

Mr. MEEHAN. Well, since insurance is generally a market-based thing, what is the legislative aspect that relates to insurance?

Mr. KOLASKY. We do not recommend any legislative aspects related to insurance. We think that the Government has convenient power to promote the insurance market, but——

Mr. MEEHAN. I am only saying final incentive category—I am reading the document—remove as independent category, include in cybersecurity act, which I am presuming is the legislation.

Mr. KOLASKY. That was an acronym that was created. We do not recommend that specifically in our——

Mr. MEEHAN. Would that be the same thing for liability considerations and legal benefits? I mean, those are two and so is there I guess I would ask liability considerations—is there some discussion of legislation that would deal with liability?

Mr. KOLASKY. Not that I am aware of at DHS.

Mr. MEEHAN. And legal benefits. I am just, again, coming from the document. Do you understand what that might refer to in any specific sense?

Mr. KOLASKY. Sure. Other legal benefits could be things like antitrust protections, which obviously is something that——

Mr. MEEHAN. Right. FOIA?

Mr. KOLASKY. It could be another legal benefit, and again, the document that you are looking at is a review of incentives that are available, not a review of our recommended incentives.

Mr. MEEHAN. Well, do you have recommended incentives? Are you going to make recommendations in these particular areas?

Mr. KOLASKY. We have made general recommendation pending the creation of the cybersecurity framework. As I said, our recommendations were done in coordination with Treasury and Commerce but are independent of each other and the administration is considering all of those and all of us will work together to chart a path forward.

Mr. MEEHAN. Okay. Let me just ask one then. I am sorry for overrunning my time, but I want to work with this document. If I could ask just one last question. Just the—tell me where you are on the expedited security clearance process because this seems to

suggest that you are going to remove that incentive, that there is a sense that this is moving along at an appropriate enough pace.

Mr. KOLASKY. Yes. We do not believe that that is an incentive. We believe that should be done on a need-to-know basis and that we should work with owners and operators.

We should not attach that to the cybersecurity framework but instead, work with owners and operators to identify critical infrastructure and individuals within critical infrastructure owner and operators companies who have the need to get Classified cyber threat information; at the 150-day mark we deliver to the administration, update on DHS's program to get private-sector individuals clearances, and improvements and enhancements——

Mr. MEEHAN. You know, because that is the thing that I hear again and again and again and you are a little bit better than another agency we hear frequently about but it—you know, we get asked for all kinds of information to be dumped into the Government and then we never hear anything again.

Mr. KOLASKY. We have made a lot of progress since February, but in doing so, we wanted it to be measured progress related to Congressman Marino's question to make sure we aren't giving clearances to people who don't need clearances.

Mr. MEEHAN. Okay. I thank you for your testimony.

Does the gentlelady have any follow-up questions?

Ms. CLARKE. No, I am fine.

Mr. MEEHAN. Okay.

Well, I want to express my deep appreciation for your testimony today. The witnesses' testimony has been very valuable to us. There may be possible questions from some of the other Members of the committee and if in fact there are and they are forwarded to you, I ask that you would do your best to respond in writing.

So without objection, the subcommittee stands adjourned.

[Whereupon, at 11:41 a.m., the subcommittee was adjourned.]

○