AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

DOE MODERNIZATION: LEGISLATION ADDRESSING CYBERSECURITY AND EMERGENCY RESPONSE

HEARING

BEFORE THE

SUBCOMMITTEE ON ENERGY

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

MARCH 14, 2018

Serial No. 115–108



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

U.S. GOVERNMENT PUBLISHING OFFICE
30–558 WASHINGTON : 2018

COMMITTEE ON ENERGY AND COMMERCE

GREG WALDEN, Oregon
Chairman

JOE BARTON, Texas
Vice Chairman
FRED UPTON, Michigan
JOHN SHIMKUS, Illinois
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota
TIM WALBERG, Michigan
MIMI WALTERS, California
RYAN A. COSTELLO, Pennsylvania
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina

FRANK PALLONE, JR., New Jersey
Ranking Member
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CARDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan

SUBCOMMITTEE ON ENERGY

FRED UPTON, Michigan
Chairman

PETE OLSON, Texas
Vice Chairman
JOE BARTON, Texas
JOHN SHIMKUS, Illinois
ROBERT E. LATTA, Ohio
GREGG HARPER, Mississippi
DAVID B. MCKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
BILL JOHNSON, Ohio
BILLY LONG, Missouri
LARRY BUCSHON, Indiana
BILL FLORES, Texas
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
KEVIN CRAMER, North Dakota
TIM WALBERG, Michigan
JEFF DUNCAN, South Carolina
GREG WALDEN, Oregon *(ex officio)*

BOBBY L. RUSH, Illinois
Ranking Member
JERRY MCNERNEY, California
SCOTT H. PETERS, California
GENE GREEN, Texas
MICHAEL F. DOYLE, Pennsylvania
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont
PAUL TONKO, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
G.K. BUTTERFIELD, North Carolina
FRANK PALLONE, JR., New Jersey *(ex officio)*

CONTENTS

Page

Hon. Fred Upton, a Representative in Congress from the State of Michigan, opening statement 1
Prepared statement 3
Hon. Greg Walden, a Representative in Congress from the State of Oregon, opening statement 21
Prepared statement 22
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement 23

WITNESSES

Mark Menezes, Under Secretary, U.S. Department of Energy 25
Prepared statement 28
Answers to submitted questions 169
Tristan Vance, Director, Chief Energy Officer, Indiana Office of Energy Development 64
Prepared statement 67
Zachary Tudor, Associate Laboratory Director for National and Homeland Security, Idaho National Laboratory 77
Prepared statement 79
Mark Engels, Senior Enterprise Security Advisor, Dominion Energy 86
Prepared statement 88
Kyle Pitsor, Vice President, Government Relations, National Electrical Manufacturers Association 104
Prepared statement 106
Scott Aaronson, Vice President, Security and Preparedness, Edison Electric Institute 117
Prepared statement 119

SUBMITTED MATERIAL

H.R. 5174 5
H.R. 5175 7
H.R. 5239 10
H.R. 5240 14
Statement of the American Public Power Association and the National Rural Electric Cooperative Association 140
Report entitled, "Cybersecurity Program Update," The American Puclic Power Association, ... 143
Letter of January 24, 2018, from the Committee to Secretary of Energy Rick Perry 155
Letter of March 13, 2018, from Secretary of Energy Rick Perry to the Subcommittee on Energy 158
Statement of Siemens Energy 165

DOE MODERNIZATION: LEGISLATION ADDRESSING CYBERSECURITY AND EMERGENCY RESPONSE

WEDNESDAY, MARCH 14, 2018

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ENERGY,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:04 a.m., in room 2322 Rayburn House Office Building, Hon. Fred Upton (chairman of the subcommittee) presiding.

Members present: Representatives Upton, Olson, Barton, Shimkus, Latta, Harper, McKinley, Kinzinger, Griffith, Johnson, Long, Bucshon, Mullin, Hudson, Walberg, Duncan, Walden (ex officio), Rush, McNerney, Peters, Castor, Sarbanes, Welch, Tonko, Loebsack, Butterfield, and Pallone (ex officio).

Staff present: Mike Bloomquist, Staff Director; Daniel Butler, Staff Assistant; Kelly Collins, Legislative Clerk, Energy/Environment; Jordan Davis, Director of Policy and External Affairs; Wyatt Ellertson, Professional Staff, Energy/Environment; Margaret Tucker Fogarty, Staff Assistant; Adam Fromm, Director of Outreach and Coalitions; Jordan Haverly, Policy Coordinator, Environment; Ben Lieberman, Senior Counsel, Energy; Mary Martin, Chief Counsel, Energy/Environment; Drew McDowell, Executive Assistant; Brandon Mooney, Deputy Chief Counsel, Energy; Mark Ratner, Policy Coordinator; Annelise Rickert, Counsel, Energy; Dan Schneider, Press Secretary; Peter Spencer, Professional Staff Member, Energy; Jason Stanek, Senior Counsel, Energy; Austin Stonebraker, Press Assistant; Madeline Vey, Policy Coordinator, Digital Commerce and Consumer Protection; Hamlin Wade, Special Advisor, External Affairs; Everett Winnick, Director of Information Technology; Priscilla Barbour, Minority Energy Fellow; Jeff Carroll, Minority Staff Director; Jean Fruci, Minority Energy and Environment Policy Advisor; Tiffany Guarascio, Minority Deputy Staff Director and Chief Health Advisor; Rick Kessler, Minority Senior Advisor and Staff Director, Energy and Environment; John Marshall, Minority Policy Coordinator; Alexander Ratner, Minority Policy Analyst; and C.J. Young, Minority Press Secretary.

OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. UPTON. Good morning. Good morning. So, this DOE modernization hearing is going to focus on the proposed legislation re-

lating to core energy security missions of the Department. This mission is to ensure the supply and delivery of energy that is vital to our economic and national security, our public welfare, and health.

For the last two Congresses we have been working to update the Department's authorities and capabilities both to mitigate against and respond to energy supply emergencies, especially with respect to critical energy infrastructure and to cybersecurity.

For example, we directed the Department to modernize its strategic petroleum reserve and response capabilities. We clarified and enhanced DOE's role as the sector-specific agency for the energy sector, especially for critical electric infrastructure. We moved through the House H.R. 3050 last summer to strengthen DOE's support for state energy emergency offices in their cybersecurity efforts and the common theme has been to update DOE's cybersecurity and emergency coordinating functions and provisions of technical assistance to other agencies, states, and asset owners. So in keeping with these modernization efforts, the legislation today continues that work.

H.R. 5174, the Energy Emergency Leadership Act, introduced by Mr. Walberg and Ranking Member Rush, elevates the role in DOE and specifies certain emergency and preparedness functions to ensure full attention to the risks of cybersecurity and other threats to the energy sector.

Given the reliance on energy in modern society, ensuring that supply has become of such surpassing importance that we have to be able to make sure that the agency has sufficient leadership focus to meet its responsibilities.

Similarly, H.R. 5175, the Pipeline and LNG Facility Cybersecurity Preparedness Act, which I introduced along with Mr. Loebsack would enhance DOE's ability to coordinate the interconnected systems of energy delivery and supply which includes ensuring the security of digital systems in pipeline and grid operations.

Although several governmental authorities play a role, DOE has got to have the adequate visibility across the energy sector to ensure the Federal, State, and asset owners are sufficiently prepared and coordinated and to efficiently deploy, where needed, its world class technological capabilities. This bill certainly aims to assure that it can be done.

Both H.R. 5239, the Cyber Sense Act of 2018, and H.R. 5240, the Enhancing Grid Security Through Public-Private Partnership Act, have been introduced by Mr. Latta and Mr. McNerney, two leaders on grid innovation. The Cyber Sense bill, a version of which passed the House as part of H.R. 8 back in 2016, seeks to establish a voluntary DOE program that would permit cybersecure products intended for use in the bulk-power system.

And the Enhancing Grid Security Act bill seeks to facilitate and encourage public-private partnerships aimed at strengthening the physical and cybersecurity electric utilities, especially mid-size and small utilities which may not have met the resources to identify and address cybersecurity vulnerabilities and system risks.

Two panels of witnesses this morning are going to provide their perspective on these bills and discuss what other measures may be

helpful to ensure DOE can fulfill its energy security and emergency missions.

I want to welcome back Undersecretary of Energy Mark Menezes, who returns from his appearance in January. I look forward to his comments and to talk about his own plans to elevate DOE's leadership in emergency response. He's accompanied by Pat Hoffman, Principal Deputy Assistant Secretary in the Office of Electricity, who can provide technical perspective from her experience addressing cybersecurity and energy emergency functions.

Our second panel will feature a range of energy security and emergency perspectives. One witness from DOE's Idaho National Lab will help us understand federal capabilities to support cybersecurity in the energy sector.

We are going to hear from the State of Indiana's Emergency Response Authority from Dominion Energy on pipeline security from EEI on electric cybersecurity and from the National Electrical Manufacturers Association to talk about cybersecurity of grid components.

We welcome you all and with that I would yield to the ranking member of the subcommittee, my friend, Mr. Rush.

[The prepared statement of Mr. Upton follows:]

PREPARED STATEMENT OF HON. FRED UPTON

Our DOE modernization hearing today will focus on proposed legislation relating to a core energy security mission of the Department. This mission is to ensure the supply and delivery of energy that is vital to our economic and national security, our public health and welfare.

For the past two Congresses we've been working to update the Department's authorities and capabilities both to mitigate against and respond to energy supply emergencies, especially with respect to critical energy infrastructure and to cybersecurity.

For example, we directed the Department to modernize its strategic petroleum reserve and response capabilities; we clarified and enhanced DOE's role as the sector specific agency for the energy sector, especially for critical electric infrastructure; we moved through the House H.R. 3050 last summer to strengthen DOE's support for state energy emergency offices and their cybersecurity efforts.

The common theme here is to update DOE's cybersecurity and emergency coordinating functions and provision of technical assistance to other agencies, states, and asset owners. So, in keeping with these modernization efforts, the legislation today continues this work.

H.R. 5174, the Energy Emergency Leadership Act, introduced by Mr. Walberg and Ranking Member Rush, elevates the role in DOE and specifies certain emergency and preparedness functions to ensure full attention to the risks of cybersecurity and other threats to the energy sector.

Given the reliance on energy in modern society, ensuring its supply has become of such surpassing importance, we should be sure the agency has sufficient leadership focus to meet its responsibilities.

Similarly, H.R. 5175, the Pipeline and LNG Facility Cybersecurity Preparedness Act, which I introduced along with Mr. Loebsack, would enhance DOE's ability to coordinate the interconnected systems of energy delivery and supply, which includes ensuring the security of digital systems in pipeline and grid operations.

Although several governmental authorities play a role, DOE must have adequate visibility across the energy sector, to ensure the Federal, State, and asset owners are sufficiently prepared and coordinated, and to efficiently deploy, where needed, its world class technological capabilities. This bill aims to assure this can be done.

Both H.R. 5239, the Cyber Sense Act of 2018, and H.R. 5240, the Enhancing Grid Security through Public-Private Partnership Act, have been introduced by Mr. Latta and Mr. McNerney, two leaders on grid innovation. The Cyber Sense bill, a version of which passed the House as part of H.R. 8 in 2016, seeks to establish a voluntary DOE program that would promote cyber-secure products intended for use in the bulk-power system.

The Enhancing Grid Security bill seeks to facilitate and encourage public-private partnerships aimed at strengthening the physical and cybersecurity of electric utilities, especially mid-sized and small utilities, which may not have the resources to identify and address cybersecurity vulnerabilities and system risks.

Two panels of witnesses this morning will provide perspective on these bills and discuss what other measures may be helpful to ensure DOE can fulfill its energy security and emergency missions.

I'd like to welcome back Under Secretary of Energy Mark Menezes, who returns from his appearance in January. I look forward to his comments and to talk about his own plans to elevate DOE's leadership on emergency response. He is accompanied by Pat Hoffman, Principal Deputy Assistant Secretary in the Office of Electricity, who can provide technical perspective from her experience addressing cybersecurity and energy emergencies.

Our second panel features a range of energy security and emergency perspectives. Our witness from DOE's Idaho National Lab will help us understand federal capabilities to support cybersecurity in the energy sector.

We'll hear from the State of Indiana's emergency response authority; we'll hear from Dominion Energy on pipeline security, from the Edison Electric Institute on electric cybersecurity, and from National Electrical Manufacturers Association, to talk about cybersecurity of grid components.

Welcome, and I look forward to the discussion.

[H.R. 5174, H.R. 5175, H.R. 5239, and H.R. 5240 follow:]

.....

(Original Signature of Member)

115TH CONGRESS
2D SESSION

H. R. 5174

To amend the Department of Energy Organization Act with respect to functions assigned to Assistant Secretaries, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. WALBERG (for himself and Mr. RUSH) introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the Department of Energy Organization Act with respect to functions assigned to Assistant Secretaries, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Energy Emergency Leadership Act".

SEC. 2. FUNCTIONS ASSIGNED TO ASSISTANT SECRETARIES.

Subsection (a) of section 203 of the Department of Energy Organization Act (42 U.S.C. 7133(a)) is amended by adding at the end the following new paragraph:

"(12) Energy emergency and energy security functions, including—

"(A) responsibilities with respect to infrastructure, cybersecurity, emerging threats, supply, and emergency planning, coordination, response, and restoration; and

"(B) upon request of a State, local, or tribal government or energy sector entity, and in consultation with other Federal agencies as appropriate, provision of technical assistance, support, and response capabilities with respect to energy security threats, risks, and incidents.".

.....

(Original Signature of Member)

115TH CONGRESS
2D SESSION

H. R. 5175

To require the Secretary of Energy to carry out a program relating to physical security and cybersecurity for pipelines and liquified natural gas facilities.

IN THE HOUSE OF REPRESENTATIVES

Mr. UPTON (for himself and Mr. LOEBSACK) introduced the following bill; which was referred to the Committee on _____

A BILL

To require the Secretary of Energy to carry out a program relating to physical security and cybersecurity for pipelines and liquified natural gas facilities.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Pipeline and LNG Facility Cybersecurity Preparedness Act".

SEC. 2. PHYSICAL SECURITY AND CYBERSECURITY FOR PIPELINES AND LIQUEFIED NATURAL GAS FACILITIES.

The Secretary of Energy, in carrying out the Department of Energy's functions pursuant to the Department of Energy Organization Act (42 U.S.C. 7101 et seq.), and in consultation with appropriate Federal agencies, representatives of the energy sector, the States, and other stakeholders, shall carry out a program—

(1) to establish policies and procedures to coordinate Federal agencies, States, and the energy sector to ensure the security, resiliency, and survivability of natural gas pipelines (including natural gas transmission and distribution pipelines), hazardous liquid pipelines, and liquefied natural gas facilities;

(2) to coordinate response and recovery by Federal agencies, States, and the energy sector, to physical incidents and cyber incidents impacting the energy sector;

(3) to develop advanced cybersecurity applications and technologies for natural gas pipelines (including natural gas transmission and distribution pipelines), hazardous liquid pipelines, and liquefied natural gas facilities;

(4) to perform pilot demonstration projects relating to physical security and cybersecurity for natural gas pipelines (including natural gas transmission and distribution pipelines), hazardous liquid pipelines, and liquefied natural gas facilities with representatives of the energy sector;

(5) to develop workforce development curricula for the energy sector relating to physical security and cybersecurity for natural gas pipelines (including natural gas transmission and distribution pipelines), hazardous liquid pipelines, and liquefied natural gas facilities; and

(6) to provide mechanisms to help the energy sector evaluate, prioritize, and improve physical security and cybersecurity capabilities for natural gas pipelines (including natural gas transmission and distribution pipelines), hazardous liquid pipelines, and liquefied natural gas facilities.

.....

(Original Signature of Member)

115TH CONGRESS
2D SESSION

H. R. 5239

To require the Secretary of Energy to establish a voluntary Cyber Sense program to identify and promote cyber-secure products intended for use in the bulk-power system, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. LATTA (for himself and Mr. MCNERNEY) introduced the following bill; which was referred to the Committee on _____

A BILL

To require the Secretary of Energy to establish a voluntary Cyber Sense program to identify and promote cyber-secure products intended for use in the bulk-power system, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cyber Sense Act of 2018".

SEC. 2. CYBER SENSE.

(a) IN GENERAL.—The Secretary of Energy shall establish a voluntary Cyber Sense program to identify and promote cyber-secure products intended for use in the bulk-power system, as defined in section 215(a) of the Federal Power Act (16 U.S.C. 824o(a)).

(b) PROGRAM REQUIREMENTS.—In carrying out subsection (a), the Secretary of Energy shall—

(1) establish a Cyber Sense testing process to identify products and technologies intended for use in the bulk-power system that are cyber-secure, including products relating to industrial control systems, such as supervisory control and data acquisition systems;

(2) for products tested and identified as cyber-secure under the Cyber Sense program, establish and maintain cybersecurity vulnerability reporting processes and a related database;

(3) provide technical assistance to electric utilities, product manufacturers, and other electricity sector stakeholders to develop solutions to mitigate identified cybersecurity vulnerabilities in products tested and identified as cyber-secure under the Cyber Sense program;

(4) biennially review products tested and identified as cyber-secure under the Cyber Sense program

for cybersecurity vulnerabilities and provide analysis with respect to how such products respond to and mitigate cyber threats;

(5) develop procurement guidance for electric utilities for products tested and identified as cyber-secure under the Cyber Sense program;

(6) provide reasonable notice to the public, and solicit comments from the public, prior to establishing or revising the Cyber Sense testing process;

(7) establish procedures for disqualifying products that were tested and identified as cyber-secure under the Cyber Sense program but that no longer meet the qualifications to be identified cyber-secure products under such program;

(8) oversee Cyber Sense testing carried out by third parties; and

(9) consider incentives to encourage the use in the bulk-power system of products tested and identified as cyber-secure under the Cyber Sense program.

(c) DISCLOSURE OF INFORMATION.—Any cybersecurity vulnerability reported pursuant to the process established under subsection (b)(2), the disclosure of which the Secretary of Energy reasonably foresees would cause harm to critical electric infrastructure (as defined in section 215A of the Federal Power Act), shall be deemed to be

critical electric infrastructure information for purposes of section 215A(d) of the Federal Power Act.

(d) FEDERAL GOVERNMENT LIABILITY.—Nothing in this section shall be construed to authorize the commencement of an action against the United States Government with respect to the testing and identification of a product under the Cyber Sense program.

.....

(Original Signature of Member)

115TH CONGRESS
2D SESSION

H. R. 5240

To provide for certain programs and developments in the Department of Energy concerning the cybersecurity and vulnerabilities of, and physical threats to, the electric grid, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. MCNERNEY (for himself and Mr. LATTA) introduced the following bill; which was referred to the Committee on _____

A BILL

To provide for certain programs and developments in the Department of Energy concerning the cybersecurity and vulnerabilities of, and physical threats to, the electric grid, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Enhancing Grid Security through Public-Private Partnerships Act".

SEC. 2. PROGRAM TO PROMOTE AND ADVANCE PHYSICAL SECURITY AND CYBERSECURITY OF ELECTRIC UTILITIES.

(a) ESTABLISHMENT.—The Secretary of Energy, in consultation with State regulatory authorities, industry stakeholders, and other Federal agencies the Secretary determines appropriate, shall carry out a program to—

(1) develop, and provide for voluntary implementation of, maturity models, self-assessments, and auditing methods for assessing the physical security and cybersecurity of electric utilities;

(2) provide training to electric utilities to address and mitigate cybersecurity supply chain management risks;

(3) increase opportunities for sharing best practices and data collection within the electric sector;

(4) assist with cybersecurity training for electric utilities;

(5) advance the cybersecurity of third-party vendors that work in partnerships with electric utilities; and

(6) provide technical assistance for electric utilities subject to the program.

(b) SCOPE.—In carrying out the program under subsection (a), the Secretary of Energy shall—

(1) take into consideration different sizes of electric utilities and the regions that such electric utilities serve;

(2) prioritize electric utilities with fewer available resources due to size or region; and

(3) to the extent practicable, utilize and leverage existing Department of Energy programs.

(c) PROTECTION OF INFORMATION.—Information provided to, or collected by, the Federal Government pursuant to this section—

(1) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and

(2) shall not be made available by any Federal, State, political subdivision or tribal authority pursuant to any Federal, State, political subdivision, or tribal law requiring public disclosure of information or records.

SEC. 3. REPORT ON CYBERSECURITY AND DISTRIBUTION SYSTEMS.

(a) IN GENERAL.—The Secretary of Energy, in consultation with State regulatory authorities, industry stakeholders, and other Federal agencies the Secretary determines appropriate, shall submit to Congress a report that assesses—

(1) priorities, policies, procedures, and actions for enhancing the physical security and cybersecurity of electricity distribution systems to address threats to, and vulnerabilities of, such electricity distribution systems; and

(2) implementation of such priorities, policies, procedures, and actions, including an estimate of potential costs and benefits of such implementation, including any public-private cost-sharing opportunities.

(b) PROTECTION OF INFORMATION.—Information provided to, or collected by, the Federal Government pursuant to this section—

(1) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and

(2) shall not be made available by any Federal, State, political subdivision or tribal authority pursuant to any Federal, State, political subdivision, or tribal law requiring public disclosure of information or records.

SEC. 4. ELECTRICITY INTERRUPTION INFORMATION.

(a) INTERRUPTION COST ESTIMATE CALCULATOR.—The Secretary of Energy, in consultation with the Federal Energy Regulatory Commission, State regulatory authorities, industry stakeholders, and other Federal agencies the Secretary determines appropriate, shall update the Inter-

ruption Cost Estimate Calculator, as often as appropriate and feasible, but not less than once every 2 years.

(b) INDICES.—The Secretary of Energy, in consultation with the Federal Energy Regulatory Commission, State regulatory authorities, industry stakeholders, and other Federal agencies the Secretary determines appropriate, shall, as often as appropriate and feasible, update the following:

(1) The System Average Interruption Duration Index.

(2) The System Average Interruption Frequency Index.

(3) The Customer Average Interruption Duration Index.

(c) SURVEY.—The Administrator of the Energy Information Administration shall collect information on electricity interruption costs, if available, from a representative sample of owners of electric grid assets through a biennial survey.

SEC. 5. DEFINITIONS.

In the Act, the following definitions apply:

(1) ELECTRIC UTILITY.—The term "electric utility" has the meaning given such term in section 3 of the Federal Power Act (16 U.S.C. 796).

(2) STATE REGULATORY AUTHORITY.—The term "State regulatory authority" has the meaning given such term in section 3 of the Federal Power Act (16 U.S.C. 796).

Mr. RUSH. I want to thank you, Mr. Chairman, for holding this important hearing today on legislation addressing cybersecurity and emergency response.

Mr. Chairman, I support the four bills before us and I want to specifically and respectfully acknowledge Mr. Walberg of Michigan who worked with my office on the Energy Emergency Leadership Act. This bill will establish a new DOE assistant secretary position with jurisdiction over all energy emergency and security functions related to energy supply, infrastructure, and cybersecurity.

Mr. Chairman, while cybersecurity is an important issue, I would be remiss if I did not point out that today at this very same time students have declared this as National Walk-Out Day. And as we speak, Mr. Chairman, students from across the country are leaving their classrooms to honor the lives of the 17 people killed at Stoneman Douglas High School last month and to press policy makers to pass commonsense gun control laws.

Mr. Chairman, cybersecurity is a serious issue that must be addressed. However, nothing can be more urgent than answering the cries and the pleas emanating from our Nation's youth—students who have had enough of being scared and anxious and frustrated by the lack of leadership coming from both the administration and this Congress on the issue of gun violence.

Mr. Chairman, as policy makers, as parents, as grandparents, as adults, and as leaders we are failing our youth by letting politics and influential interest groups come before our most sacred responsibility, and that is protecting our children.

Mr. Chairman, every single Democrat on the four Energy and Commerce committees sent a letter to Chairman Walden on March 7th urging him to hold hearings as soon as possible to address gun violence in America. That followed a February 16th letter also signed by all 24 Democrats on the full committee to Chairman Walden and Health Subcommittee Chairman Burgess urging the Republican leadership to hold a hearing as soon as possible on federal investment in gun violence prevention research.

Mr. Chairman, we owe it to our children at the very least to examine this problem in a serious and thoughtful manner and I can assure you that this issue will come up again and again, regardless of the planned topic of discussion until we hold a hearing.

With that, I yield the remainder of my time to my friend and colleague from California, Mr. McNerney.

Mr. MCNERNEY. Well, I thank the ranking member for yielding and the chairman for holding this hearing.

Today, we will examine several legislative proposals concerning our Nation's grid security. As co-chairs of the Grid Innovation Caucus, Bob Latta and I are focused on providing a forum that advocates for grid investments and examines the risks and opportunities with our grid.

Our work, through the Grid Caucus, has led to the introduction of two bills we will discussing today. H.R. 5239, the Cyber Sense Act of 2018 would create a program to identify cybersecure products for the bulk power grid system through testing and verification. The bulk power system is the backbone of American industry and provides all the benefits of reliable electric power to the American people. It's essential that we make this system as se-

cure as possible as cyberattacks pose a serious threat to our electric grid. Any vulnerable components of our grid is a threat to our security and this bill will go a long way to strengthen our system.

Mr. Latta and I are also co-leads of H.R. 5240, the Enhancing Grid Security Through Public-Private Partnerships Act. This bill will create a program to enhance the physical and cybersecurity of electric utilities through assessing security vulnerabilities, increase cybersecurity training, and data collection. It will also require the interruption cost estimate calculator, which is used to calculate the return on investment on utility investments, to be updated at least every 2 years to ensure accurate calculations.

These two bipartisan bills, along with the other bills we have before us today, will help put us on the path to better securing our electric utility system.

I welcome the panelists and look forward to hearing their insights on the useful of our legislation and how it may be improved.

Thank you. I yield back.

Mr. UPTON. Gentleman's time is expired.

The chair will recognize the chairman of the full committee, the gentleman from Oregon, Mr. Walden.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

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

I want to thank my colleague from California for his good work on these issues. This is really important stuff for our country and those of us who have been briefed up on it know the importance of the work that's going on in our agencies and the security issues that are really before us.

Today's hearing examines legislation addressing cybersecurity and emergency response. It will help us respond to some of the most urgent challenges—the reliability of our Nation's energy infrastructure. Because our energy infrastructure drives the entire Nation's economy, I've made it a top priority for this committee to focus on emerging threats and proposed solutions to make our infrastructure more resilient. We are looking ahead to make sure we are doing everything we can to protect our electric grid and our oil and natural gas infrastructure as well and improve our ability to respond when the unexpected happens.

Because nearly all of our Nation's energy infrastructure is privately owned and operated, the Federal Government needs to work closely with representatives of the energy sector and the companies in the supply chain that manufacture equipment and technologies. In today's highly interconnected world, the threat of cyberattacks is ever present. So we have to be vigilant. We must also be prepared for physical threats whether they be sabotage or natural disasters like the hurricanes we experienced last year.

As the sector-specific agency for energy, the Department of Energy has a very important coordinating role to play and this function was on display earlier this year in response to Hurricanes Nate, Maria, Irma, and Harvey. Many of us followed DOE's situation reports on the storms' impacts and the energy industry's recovery and restoration activities. The Department of Energy's emergency responders in the field provided critical subject matter exper-

tise and assisted with waivers and special permits to aid restoration. To prevent a major fuel supply emergency, the Department of Energy's strategic petroleum reserve provided much-needed oil to refiners. TDOE also analyzed electricity supply to determine whether it needed to draw on its Federal Power Act authorities to secure the energy grid.

So today's hearing will examine four bipartisan bills designed to improve DOE's energy security and emergency response authorities. I want to thank all our members for working across the aisle on these important issues.

I join Chairman Upton in welcoming back Under Secretary of Energy Mark Menezes to our panel. I look forward to your comments on the Department of Energy's security priorities and its views on the legislation.

I also want to welcome the witnesses appearing on the second panel where we will hear a range of perspectives from state government, the energy industry, and supply chain manufacturers. We are also joined by a witness from DOE's Idaho National Lab. I was there on Monday. I very much appreciated the briefings including the classified ones and so I am very impressed by the work that goes on at INL and our country should be very proud of the incredible men and women and the work they do there in every regard. I also saw the unique capabilities to test system wide cybersecurity applications on a full scale electric grid loop. INL is one of 17 DOE national labs tackling the critical scientific challenges of our time and the threats that come our way and I want to thank INL leadership and staff for sharing their research and expertise with the Committee.

This subcommittee has held dozens of hearings on energy infrastructure and produced several bipartisan bills to improve the resilience and reliability of our Nation's energy delivery system and these bills will ultimately make our nation more energy secure, reduce the cost of fuels and electricity for consumers.

So at the end of the day, if we focus on what's best for consumers we will continue to make good public policy decisions.

With that, Mr. Chairman, I yield back the balance of my time and thank our witnesses for their participation.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Today's hearing, examining legislation addressing cybersecurity and emergency response, will help us respond to some of the most urgent challenges to the reliability of our Nation's energy infrastructure. Because our energy infrastructure drives the entire Nation's economy, I've made it a top priority for the committee to focus on emerging threats and propose solutions to make our infrastructure more resilient. We're looking ahead, to make sure we're doing everything we can to protect our electric grid and our oil and natural gas infrastructure, and to improve our ability to respond when the unexpected happens.

Because nearly all our Nation's energy infrastructure is privately owned and operated, the Federal Government needs to work closely with representatives of the energy sector and the companies in the supply chain that manufacture equipment and technologies. In today's highly interconnected world, the threat of cyber-attacks is ever present, so we must be vigilant. We must also be prepared for physical threats, whether they be sabotage or natural disasters, like the hurricanes we experienced this summer.

As the sector-specific agency for energy, the Department of Energy has a very important coordinating role to play. This function was on display earlier this year in

response to hurricanes Nate, Maria, Irma and Harvey. Many of us followed DOE's situation reports on the storms' impacts and the energy industry's recovery and restoration activities. DOE's emergency responders in the field provided critical subject matter expertise and assisted with waivers and special permits to aid restoration. To prevent a major fuel supply emergency, DOE's Strategic Petroleum Reserve provided much needed oil to refiners. DOE also analyzed electricity supply to determine whether it needed to draw on its Federal Power Act authorities to secure the grid.

Today's hearing will examine four bipartisan bills designed to improve DOE's energy security and emergency response authorities. I want to thank our members for working across the aisle on these important issues.

I join Chairman Upton in welcoming back Under Secretary of Energy Mark Menezes to join our first panel. I look forward to his comments on the department's energy security priorities and its views on the legislation.

I also want to welcome the witnesses appearing on the second panel. We'll hear a range of perspectives from state government, the energy industry, and supply chain manufacturers. We're also joined by a witness from DOE's Idaho National Lab, which I had the privilege of visiting earlier this week. Idaho National Lab, or INL, is the nation's leading nuclear research laboratory. INL also has unique capabilities to test system-wide cybersecurity applications on a full scale electric grid loop. INL is one of seventeen DOE national labs tackling the critical scientific challenges of our time and I want to thank INL leadership and staff for sharing their research and expertise with the Committee.

This subcommittee has held dozens of hearings on energy infrastructure and produced several bipartisan bills to improve the resilience and reliability of our Nation's energy delivery systems. These bills will ultimately make our nation more energy secure and reduce the cost of fuels and electricity for consumers. At the end of the day, if we focus on what's best for consumers we'll continue make good policy decisions.

Mr. UPTON. Gentleman yields back.

The chair recognizes the ranking member of the full committee, the gentleman from New Jersey, Mr. Pallone.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Mr. Chairman.

Today's hearing revolves around a quartet of bipartisan bills designed to enhance the security of our Nation's energy infrastructure. However, before we get to cybersecurity, I'd like to talk for a minute about the security of our Nation's children.

Today, 1 month has passed since the tragic shootings at Marjorie Stoneman Douglas High School that took the lives of 17 children and educators, and as we sit here students all across the Nation have just completed a 17-minute walkout in memory of those killed in that attack as well as to protest this body's refusal to take action on the gun violence epidemic.

Students and their families are justifiably frustrated with the inaction here in Washington. They are sick and tired of a president who says one thing in front of the cameras and then works behind the scenes to push the NRA agenda as soon as he thinks the cameras are focused somewhere else. And they are also sick and tired of a Republican leadership in Congress that won't move forward on any common sense legislation, some of which has strong bipartisan support.

Americans have legitimate questions about the ever-increasing capacity of guns to kill in large numbers and the ease with which people who are in danger to themselves and others can obtain them in the marketplace and those questions at least deserve to be explored through hearings in this committee.

Every Democrat on this committee has asked in two separate letters to the chairman for a series of five hearings on the gun violence epidemic. We have not received a response and no hearings have yet to be scheduled. So I hope that the chairman and my Republican colleagues will finally see the need to schedule the five hearings we requested.

We don't expect them to necessarily agree with us or those participating in today's walkout on all the solutions to the gun violence epidemic. However, we do hope that they will finally acknowledge the legitimate need to explore the questions we are asking and for this committee to take action. And now, with regard to cybersecurity, I appreciate the majority taking these small but important bipartisan steps to enhance the Department of Energy's authorities with regard to our Nation's energy infrastructure.

These four bills build upon the good work done by this committee and the FAST Act under Chairman Upton's leadership. I think it makes sense from both the security and business standpoint to have the department with the best knowledge of the energy industry taking the primary role in coordinating efforts to prevent and respond to cyberattacks on these facilities.

In general, I am supportive of each of these bills. H.R. 5174, the Energy Emergency Leadership Act sponsored by Representative Walberg and Ranking Member Rush, would create a new DOE assistant secretary position with jurisdiction over all energy emergency and security functions related to energy supply, infrastructure and cybersecurity.

H.R. 5175, the Pipeline and LNG Facilities Cybersecurity Preparedness Act, was introduced by Chairman Upton and Mr. Loebsack. It would require the secretary of energy to carry out a program to establish policies and procedures that would improve the physical and cybersecurity of natural gas transmission and distribution pipelines, hazardous liquid pipelines and liquefied natural gas facilities.

Representative Latta and McNerney's bill, H.R. 5239, the Cyber Sense Act of 2018, is based on McNerney's language included in the last Congress energy bill. It would require the secretary to establish a voluntary program to identify cybersecure products that can be used in bulk power systems.

Mr. McNerney and Mr. Latta also introduced H.R. 5240, the Enhancing Grid Security Through Public-Private Partnership Act, which directs the secretary to create and implement a program to enhance the physical and cybersecurity of electric utilities.

In addition to these bills, I also wanted to direct the Committee's attention to the LIFT America Act, the infrastructure bill that committee Democrats introduced last year.

A number of the bill's provisions would enhance the security and resiliency of the grid through new grant programs and by requiring certain projects receiving DOE assistance including the cybersecurity plan written in accordance with guidelines developed by the secretary.

And the bill would also establish a strategic transformer reserve program to reduce electric grid vulnerability to physical and cyberattacks, natural disasters, and climate change, and these are provisions that will better assure the security of our energy infra-

structure and I hope this committee will consider them as we move forward.

And again, Mr. Chairman, thanks for bringing up these bipartisan bills and I yield back.

Mr. UPTON. Gentleman yields back, and as I indicated, we are joined for our first panel with the Honorable Mark Menezes, the undersecretary of energy.

I would just note for those of us that went on the bipartisan trip to look at the hurricane damage in Puerto Rico, on my local radio website this morning I see that the bridge that we saw that was washed out was rededicated yesterday with the governor and it's opened up. It's been 6 months. It connects 60 families in a town of about 33,000 folks. So I know we were there for an hour or so back in December. So I just thought I'd give that little update.

And with that, Mr. Menezes, welcome back again to the Committee. We look forward to your testimony. You know the rules. Thank you in advance for your testimony. We will give you 5 minutes to sum it up and then we will ask questions from that point.

So welcome.

STATEMENT OF THE HONORABLE MARK MENEZES, UNDER SECRETARY, U.S. DEPARTMENT OF ENERGY

Mr. MENEZES. Thank you, Chairman Upton, Ranking Member Rush, and distinguished members of the subcommittee.

Good morning, and thank you for the opportunity to participate in this legislative hearing to discuss the strategic priorities addressing the cybersecurity threats facing our national energy infrastructure and the Department of Energy's role in protecting these critical assets and responding to emergencies.

Maintaining and improving the resilient energy infrastructure is a top priority of the secretary and a major focus of the department. You referred to the written statement. I have submitted a much more comprehensive written statement so my remarks will be limited to just the highlights.

To demonstrate our commitment and focus on this mission, the secretary announced last month that he is establishing the Office of Cybersecurity, Energy Security, and Emergency Response, to be known as CESER. This organizational change will strengthen the department's role as the sector-specific agency or energy sector cybersecurity supporting our national security responsibilities.

The creation of the CESER office will accomplish several goals: One, build on the programs that we have today; two, elevate the department's focus on energy infrastructure protection and response; three, enable a more coordinated preparedness and response to cyber and physical threats and natural disasters; and most importantly, four, create a structure and an office with an evolving mission to ensure sufficient authorities and resources are in place to address present and future threats.

The focus of the office will necessarily include electricity delivery, oil and natural gas infrastructure, and all forms of generation. The secretary's desire to create dedicated and focused attention on these responsibilities will provide greater visibility, accountability, and flexibility to better protect our Nation's energy infrastructure and support its asset owners.

As more fully explained in my submitted written testimony, DOE works in collaboration with other agencies and private sector organizations including the Federal Government's designated lead agencies for coordinating the response to significant cyber incidents—DHS, the FBI, the National Cyber Investigative Joint Task Force, as well as DOT, PHMSA, U.S. Coast Guard, and FERC and others through the Energy Government Coordinating Council and other coordinating councils.

The FAST Act designated DOE as the sector-specific agency for energy sector cybersecurity. Congress enacted several important new energy security measures in the FAST Act as it relates to cybersecurity. The secretary of energy was provided new authority upon declaration of a grid security emergency by the President to issue emergency orders to protect, restore, or defend the reliability of critical electric infrastructure. This authority allows DOE to respond as needed to threats of cyber and physical attacks on the grid, and although the administration does not have a formal position on any of the legislation under discussion today, we are pleased to continue to work with the committee to provide technical assistance. And this morning, I would like to provide the subcommittee with some high-level priorities of the department in the context of the President's fiscal year 2019 budget request and which is the subject matter of today's bills.

Overall, investing in energy security and resilience from an all-hazards approach is vital, given the natural and manmade threats facing the Nation's energy infrastructure, the energy industry, and the supply chain. The fiscal year 2019 request would provide the department an opportunity to invest in early-stage research, network threat detection, cyber incident response teams, and the testing of supply chain components and systems.

Beyond providing guidance and technical support to the energy sector, our Office of Electricity supports R&D designed to develop advanced tools and techniques to provide enhanced cyberprotection for key energy systems. OE cybersecurity for energy delivery systems' R&D program is designed to assist energy sector asset owners by developing cybersecurity solutions for our energy infrastructure. OE co-funds projects with industry, our national labs, and university partners to make advances in cybersecurity capabilities. These research partnerships are helping to detect, prevent, and mitigate consequences of a cyber incident for our present and future energy systems.

It's important to emphasize that DOE plays a critical role in supporting the entire energy sector's efforts to enhance the security and resilience of the Nation's critical energy infrastructure. To address today's ever increasing and sophisticated challenges, it is critical for us to be leaders and cultivate a culture of resilience.

We must constantly develop, educate, and train a robust network of producers, distributors, vendors, public partners, regulators, policy makers, and stakeholders acting together to strengthen our ability to prepare, to respond, and recover. As part of a comprehensive energy cybersecurity resilient strategy, the department supports efforts to enhance visibility and situational awareness of operation networks, increase alignment of cyber preparedness and

planning across local, State, and Federal levels and leverage the expertise of DOE's national labs to drive cybersecurity innovation.

As always, the department appreciates the opportunity to appear before this committee and discuss cybersecurity and emergency response in the energy sector and we applaud your leadership.

We look forward to working with you and your respective staffs and continue to address cyber and physical security challenges, and I look forward to your questions.

Thank you.

[The prepared statement of Mr. Menezes follows:]

Written Testimony of Under Secretary Mark Menezes

U.S. Department of Energy

Before the

Subcommittee on Energy

Committee on Energy and Commerce

U.S. House of Representatives

March 14, 2018

Introduction

Chairman Upton, Ranking Member Rush, and distinguished Members of the Subcommittee, thank you for the opportunity to participate in this legislative hearing to discuss strategic priorities for addressing the cybersecurity threats facing our national energy infrastructure and the Department of Energy's (DOE's) role in protecting these critical assets. Maintaining and improving a resilient energy infrastructure is a top priority of the Secretary and a major focus of the Department; hence, our focus on cybersecurity is paramount.

Our national security and economy depend on the availability of a reliable and resilient energy infrastructure. The mission of the Office of Electricity Delivery and Energy Reliability (DOE-OE) is to strengthen, transform, and improve the resilience of energy infrastructure to ensure access to reliable and secure sources of energy. The Secretary and DOE are committed to working with our public and private sector partners to protect the Nation's critical energy infrastructure from physical security events, natural and man-made disasters, and cybersecurity threats.

Office of Cybersecurity, Energy Security, and Emergency Response

To demonstrate our focus on the aforementioned mission, the Secretary announced last month that he is establishing an Office of Cybersecurity, Energy Security, and Emergency Response (CESER). This organizational change will strengthen the Department's role as the Sector-Specific Agency (SSA) for Energy Sector Cybersecurity, supporting our national security responsibilities.

The CESER office will play an essential role in coordinating government and industry efforts to address these energy sector threats. Initially, the office will be comprised of work we currently do in DOE-OE's Infrastructure Security and Energy Restoration (ISER) division and Cybersecurity and Emerging Threats Research and Development (CET R&D) division.

The President has requested slightly more than $95 million in FY 2019 for CESER with a focus on early-stage activities that improve cybersecurity and resilience to harden and evolve critical energy infrastructure. These activities include early-stage R&D at National Laboratories to develop the next generation of control systems, components, and devices with cybersecurity built in. This includes a greater ability to share time-critical data with industry to detect, prevent, and recover from cyber events.

The creation of the CESER office will build on all that we do today and elevate the Department's focus on energy infrastructure protection and will enable more coordinated preparedness and response to cyber and physical threats and natural disasters. This must include electricity delivery, oil and natural gas infrastructure, and all forms of generation. The Secretary's desire to create dedicated and focused attention on these responsibilities will provide greater visibility, accountability, and flexibility to better protect our Nation's energy infrastructure and support asset owners.

DOE's Roles and Responsibilities for Energy Sector Cybersecurity

In preparation for, and response to, cybersecurity threats, the Federal government's operational framework is provided by Presidential Policy Directive-41 (PPD-41). A primary purpose of PPD-41 is to clarify the roles and responsibilities of the Federal government during a "significant cyber incident," which is described as a cyber incident that is "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."

Under the PPD-41 framework, DOE works in collaboration with other agencies and private sector organizations, including the Federal government's designated lead agencies for coordinating the response to significant cyber incidents: Department of Homeland Security (DHS), acting through the National Cybersecurity and Communications Integration Center (NCCIC), and the Department of Justice (DOJ), acting through the Federal Bureau of Investigation (FBI), and the National Cyber Investigative Joint Task Force, respectively. In the event of a cybersecurity emergency in the energy sector, closely aligning DOE's activities with those of our partners at DHS and DOJ ensures DOE's deep expertise with the sector is appropriately leveraged.

DOE's role in energy sector cybersecurity was codified by Congress through the Fixing America's Surface Transportation (FAST) Act. That legislation designated DOE as the Sector-Specific Agency for Energy Sector Cybersecurity. In extreme cases, the Department can use its legal authorities such as those in the Federal Power Act, as amended by the FAST Act, to assist in response and recovery operations. Congress enacted several important new energy security measures in the FAST Act as it relates to cybersecurity. The Secretary of Energy was provided a new authority, upon declaration of a "Grid Security Emergency" by the President, to issue emergency orders to protect or restore the reliability of critical electric infrastructure or defense critical electric infrastructure. This authority allows DOE to respond as needed to the threat of cyber and physical attacks on the grid. The Grid Security Emergency authority is unique to DOE

and an important element in partnering with DHS and DOJ to fully address the cybersecurity risks to the energy sector.

In the energy sector, the core of critical infrastructure partners consists of the Electricity Subsector Coordinating Council (ESCC), the Oil and Natural Gas Subsector Coordinating Council (ONG SCC), and the Energy Government Coordinating Council (EGCC). The ESCC and ONG SCC represent the interests of their respective industries. The EGCC, led by DOE and co-chaired with DHS, is where the interagency partners, states, and international partners come together to discuss the important security and resilience issues for the energy sector. This forum ensures that we are working together in a whole-of-government response.

As defined in the National Infrastructure Protection Plan, the industry coordinating councils or "SCCs" are created by owners and operators and are self-organized, self-run, and self-governed, with leadership designated by the SCC membership. The SCCs serve as the principal collaboration points between the government and private sector owners and operators for critical infrastructure security and resilience coordination and planning, as well as a range of sector-specific activities and issues.

The SCCs, EGCC, and associated working groups operate under DHS's Critical Infrastructure Partnership Advisory Council (CIPAC) framework, which provides a mechanism for industry and government coordination. The public-private critical infrastructure community engages in open dialogue to mitigate critical infrastructure vulnerabilities and to help reduce impacts from threats.

Legislative Technical Assistance

Although the Administration does not have a position on any of the legislation under discussion today, I would like to provide the Subcommittee with some high level priorities for the Department in context of the FY 2019 budget request and some specific comments on each of the cyber bills. Overall, investing in energy security and resilience from an all hazards approach is vital, given the natural and man-made threats facing the Nation's energy infrastructure, the energy industry, and supply chain. The FY 2019 request would provide the Department an opportunity to invest in early stage research, network threat detection, cyber incident response teams, and testing of supply chain components and systems.

Amending the Department of Energy Organization Act

The DOE Organization Act, enacted in 1977, emphasizes energy supply shortages as a threat to national security and does not explicitly address threats posed by malicious actors targeting the Nation's critical energy infrastructure. DOE currently has broad authority to act in the event of a Grid Security emergency. Continuing to conduct preparedness and response activities will help DOE fulfill its responsibilities and expectations of our role as the lead SSA for the Energy Sector.

Cybersecurity and Physical Threats to the Electric Grid

The cyber attacks on the Ukrainian grid underscored the urgency of the cyber threat to everyone involved in the protection and operation of the Nation's power grid. Continuing to build off current work is critical in mitigating the risks that the electric grid faces. Sharing and promoting best practices, including maturity model assessments, physical and cyber risk assessments, and training are all important components of this risk mitigation.

Presidential Policy Directive-21 (PPD-21) clearly defines resilience as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

The energy industry's challenge in addressing resilience is defining cost-effectiveness as it builds in cybersecurity and invests in mitigation solutions that provide a strong return on investment. The Interruption Cost Estimate (ICE) Calculator tool, which was developed by Lawrence Berkeley National Laboratory and Nexant, Inc. and funded by DOE-OE, is designed for electric reliability planners at utilities, government organizations, or other entities that are interested in estimating interruption costs and/or the benefits associated with reliability improvements in the United States. For any hazard, including cyber events, the ICE Calculator provides analytical foundations for reliability investments. In 2015, the Department updated the 2009 meta-analysis that provides estimates of the value of service reliability for U.S. electricity customers. The meta-dataset now includes 34 different datasets from surveys fielded by 10 different utility companies between 1989 and 2012.[1]

The Department, in partnership with the ESCC, has identified several priorities moving forward, including resilient communications systems (which are heavily interdependent with energy systems), control system monitoring, proactive cyber threat detection and threat analysis, and supply chain assessments and mitigation to supply chain threats. Additionally, DOE is prioritizing providing preparedness and response support to the energy sector through the facilitation of requests for technical assistance. DOE serves as the a central hub for the energy sector and, in coordination with the Department of Homeland Security (DHS) and other interagency partners as described above, is able to help integrate DOE and DHS response teams with industry response and planning activities. The Department has been asked to provide financial and technical assistance to state, local, tribal, and territorial governments to revise and implement energy security and resilience plans as well.

Cyber Sense

Securing the electric sector supply chain is critical to the security and resilience of the electric grid. Products must be tested for known vulnerabilities in order to assess risk and develop mitigations. Universities, third parties and the National Laboratories have all conducted vulnerability testing.

---

[1] https://eaei.lbl.gov/tool/interruption-cost-estimate-calculator; https://eaei.lbl.gov/publications/updated-value-service-reliability

Ultimately, success in any product development program includes a strong quality control process through which a business seeks to ensure that product quality is maintained or improved and manufacturing errors are reduced or eliminated, even as products are updated. Quality control requires the business to create an environment in which both management and employees strive for perfection. This process is applicable to the integration of cybersecurity in the energy sector's supply chain design and manufacturing process. It is also important to note that in terms of supply, this bill references components and devices in the electric system.

In FY 2019, the Department is proposing a supply chain testing program to test and mitigate vulnerabilities in partnership with industry. Liability protections for any action or asserted failure to act by the United States, participating energy sector entity, or National Laboratory during such activities would enable the Department to develop integrated testing capabilities to understand supply chain, component, and network vulnerabilities and inform the design of resilient products.

Cybersecurity for Pipelines and Liquefied Natural Gas Facilities

As part of the Transportation Sector, DHS and the Department of Transportation (DOT) are the co-lead sector-specific agencies for pipeline cybersecurity. As the sector-specific agency for the energy sector, DOE works closely with relevant government agencies and oil and natural gas subsector partners on security and resilience, including cybersecurity through the ONG SCC and EGCC. DOE works with the DHS National Protection and Programs Directorate, the Transportation Security Administration, the U.S. Coast Guard, the DOT Transportation Pipeline and Hazardous Materials Safety Administration, and the Federal Energy Regulatory Commission regarding pipeline security and safety initiatives as they relate to resilience and reliability. Similar to the electric sector, physical and cybersecurity of crude and petroleum pipelines and liquefied natural gas facilities are critical.

DOE's Cybersecurity Strategy for the Energy Sector

DOE plays a critical role in supporting energy sector cybersecurity to enhance the security and resilience of the Nation's critical energy infrastructure. To address these challenges, it is critical for us to be proactive and cultivate an ecosystem of resilience: a network of producers, distributors, regulators, vendors, and public partners, acting together to strengthen our ability to prepare, respond, and recover.

As part of a comprehensive energy cybersecurity resilience strategy, the Department is focusing cyber support efforts to enhance visibility and situational awareness of operational networks; increase alignment of cyber preparedness and planning across local, state, and Federal levels; and leverage the expertise of DOE's National Labs to drive cybersecurity innovation.

Enhance Visibility and Situational Awareness of Operational Networks

It is necessary for partners in the energy sector and the government to share emerging threat data and vulnerability information to help prevent, detect, identify, and thwart cyber attacks more rapidly. An example of this type of collaboration is the Cybersecurity Risk Information Sharing

Program (CRISP), a voluntary public-private partnership that is primarily funded by industry, administered by the Electricity Information Sharing and Analysis Center (E-ISAC), and enhanced by DOE through intelligence analysis by DOE's Office of Intelligence and Counterintelligence.

The purpose of CRISP is to share information among electricity subsector partners, DOE, and the Intelligence Community to facilitate the timely bi-directional sharing of unclassified and classified threat information to enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources. CRISP leverages network sensors and threat analysis techniques developed by DOE along with DOE's expertise as part of the Intelligence Community to better inform the energy sector of the high-level cyber risks.

Current CRISP participants provide power to over 75 percent of continental United States electricity customers. If CRISP has demonstrated one finding to DOE, it is that continuous monitoring of critical networks and shared situational awareness is of utmost importance in protecting against malicious cyber activities. Programs such as CRISP are critical for facilitating the identification of and response to advanced persistent threats targeting the energy sector.

DOE's CRISP program is an example of how DOE, as the Sector-Specific Agency for Energy, integrates additional efforts, including information from other public-private cybersecurity programs, such as DHS's Automated Indicator Sharing (AIS). The AIS program also allows for the bidirectional sharing of observed cyber threat indicators amongst DHS and participating companies.

Advancing the ability to improve situational awareness of OT networks is a key focus of DOE's current activities. The Department is currently in the early stages of taking the lessons learned from CRISP and developing an analogous capability for threat detection on OT networks via the Cybersecurity for the Operational Technology Environment (CYOTE) pilot project. Observing anomalous traffic on networks – and having the ability to store and retrieve network traffic from the recent past – can be the first step in stopping an attack in its early stages.

Increase Alignment of Cyber Preparedness and Planning Across Local, State, and Federal Levels

As the Energy SSA, DOE works at many levels of the electricity, petroleum, and natural gas industries. We interact with numerous stakeholders and industry partners to share both classified and unclassified information, discuss coordination mechanisms, and promote scientific and technological innovation to support energy security and reliability. By partnering through working groups between government and industry at the national, regional, state, and local levels, DOE facilitates enhanced cybersecurity preparedness.

Last year, DOE-OE and the National Association of Regulatory Utility Commissioners (NARUC) released the third edition of a cybersecurity primer for regulatory utility commissioners. The updated primer provides best practices, access to industry and national standards, and clearly written reference materials for state commissions in their engagements with utilities to ensure their systems are resilient to cyber threats. This document is publicly

available on the NARUC Research Lab website, benefitting not only regulators, but state officials as well.

We are continuing to work with the NARUC Research Lab to support regional trainings on cybersecurity throughout the year, with the goal of building commissioner and commission staff expertise on cybersecurity so they ensure cyber investments are both resilient and economically sound.

DOE also continues to work closely with our public and private partners so our response and recovery capabilities fully support and bolster the actions needed to help ensure the reliable delivery of energy. We continue to coordinate with industry through the SCCs to synchronize government and industry cyber incident response playbooks.

DOE-OE engages directly with our public and private sector stakeholders to help ensure we all are prepared and coordinated in the event of a cyber incident to the industry. Innovation and preparedness are vital to grid resilience. DOE and the National Association of State Energy Officials (NASEO) co-hosted the Liberty Eclipse Exercise in Newport, Rhode Island, which focused on a hypothetical cyber incident that cascaded into the physical world, resulting in power outages and damage to oil and natural gas infrastructure. The event featured 96 participants from 13 states, and included representatives from state energy offices, emergency management departments, utility commissions, as well as Federal partners, such as FEMA, and private sector utilities and petroleum companies.

And late last year, DOE participated in GridEx IV, a biennial exercise led by the North American Electric Reliability Corporation (NERC) that was designed to simulate a cyber and physical attack on electric and other critical infrastructures across North America. This and other similar large scale exercises continue to highlight the interdependencies between our Nation's energy infrastructure and other sectors.

While the after-action report has yet to be released, during GridEx IV, it was clear that collaboration between industry and the Federal government has strengthened greatly since Superstorm Sandy and GridEx III. The executed coordination in response to this year's hurricane season also is evidence of this strengthening.

Communication capabilities that are survivable, reliable, and accessible, by both industry and government, will be key to coordinate various efforts showcased in the exercise, including unity of messaging required to recover from a real-life version of the exercise scenario.

In preparation for any future grid security emergency, it is critical that we continue working with our industry, Federal, and state partners now to further shape the types of orders that may be executed under the Secretary's authority, while also clarifying how we communicate and coordinate the operational implementation of these orders.

Continued coordination with Federal and industry partners and participation in preparedness activities like GridEx enables DOE to identify gaps and develop capabilities to support cyber response as the SSA.

Leverage the Expertise of DOE's National Laboratories to Drive Cybersecurity Innovation

Beyond providing guidance and technical support to the energy sector, DOE-OE also supports a R&D portfolio designed to develop advanced tools and techniques to provide enhanced cyber protection for key energy systems. Intentional, malicious cyber threat challenges to our energy systems are on the rise in both number and sophistication. This evolution has profound impacts on the energy sector.

Cybersecurity for energy control and OT systems is much different than that of typical IT systems. Power systems must operate continuously with high reliability and availability. Upgrades and patches can be difficult and time consuming, with components dispersed over wide geographic regions. Further, many assets are in publicly accessible areas where they can be subject to physical tampering. Real time operations are imperative and latency is unacceptable for many applications. Immediate emergency response capability is mandatory and active scanning of the network can be difficult.

DOE-OE's Cybersecurity for Energy Delivery Systems (CEDS) R&D program is designed to assist energy sector asset owners by developing cybersecurity solutions for energy delivery systems through a focused research and development effort. DOE-OE co-funds industry-led, National Laboratory-led, and university-led projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems. These research partnerships are helping to detect, prevent, and mitigate the consequences of a cyber incident for our present and future energy delivery systems.

DOE is also working in conjunction with the National Rural Electric Cooperative Association (NRECA) and the American Public Power Association (APPA) to help further enhance the culture of security within their utility members' organizations. With more than a quarter of the Nation's electricity customers served by municipal public power providers and rural electric cooperatives, it is critical they have the tools and resources needed to address security challenges. APPA and NRECA are developing security tools, educational resources, updated guidelines, and training on common strategies that can be used by their members to improve their cyber and physical security postures. Exercises, utility site assessments, and a comprehensive range of information sharing with their members will all be used to bolster their security capabilities.

Conclusion

Cyber threats continue to evolve and DOE is working diligently to eliminate and mitigate the potential consequences of these threats. Establishing the CESER office is a result of our laser focused attention to cyber and physical security. Our long-term vision is significant and will positively impact our national security. The establishment of this office will be the first step in

the transformational change necessary to meet the ever changing cyber landscape highlighted by our National Intelligence Agencies.

Finally, I would like to highlight that the risk of physical and cyber threats is continuously being exacerbated by a set of circumstances that are increasing the interdependence of the various energy systems throughout the Nation. This significantly increases our overall risk due to the increased number of penetration points that can significantly impact national security and the economy.

As always, I appreciate the opportunity to appear before this Subcommittee to discuss cybersecurity in the energy sector, and I applaud your leadership. I look forward to working with you and your respective staffs to continue to address cyber and physical security challenges.

Mr. UPTON. Thank you for your testimony and, as you know, we are talking about several bills this morning.

We want to make sure that DOE in fact does have the clear authority in the energy sector to be prepared for emergencies, particularly concerning the distribution of oil and gas and electricity, and we welcome your commitment to work with us and the bill's sponsors, as you indicated in your testimony, to provide the technical assistance to make sure that these proposals provide the tools that the agency can use.

I want to particularly thank, as Chairman Walden indicated in his opening statement, the willingness to work with the Idaho National Lab. I know that he had a very productive day out there earlier this week and I will tell members of our subcommittee that we are planning to have a classified briefing with them at some point in the near future so that we can know precisely what we have to be ready for and be able to ask questions in a classified setting. We are looking forward to setting that up in the next couple of weeks.

Let me just ask if you can help us identify other areas we might be able to clarify and strengthen your authorities to respond to energy supply emergencies, if we can have that commitment again today, and if you want to share any specifics today or certainly down the road where you can help us make sure that the worst doesn't happen and we will put out thousands, maybe hundreds of thousands, maybe even millions of folks without the ability to hook into the needed energy resources for their daily lives.

Mr. MENEZES. Thank you for the question, Chairman Upton.

Indeed, having a robust communications and coordination system with our industry asset owners is critical to do this. We currently serve on a variety of and coordinate subsector coordinating councils. We work closely with industry. We have regular meetings. We coordinate. We make our labs available to those that need it. We train, we practice, and we prepare. We do all that and, to be sure, we work with our sister agencies through the Energy Government Coordinating Council and work really on a daily basis with, as I mentioned, DHS and the other agencies.

All of that we are doing today. When the system is stressed when we have the emergencies in Puerto Rico, the art then is to put all that in place and respond in real time and to work with our sister agencies, and I have testified before that the expectations that the DOE has and the technologies that we have and the abilities to mobilize and to react are sometimes exceeded by the authorities and the resources that we have.

It is important for the department with the bills that you have to be clear on the authorities, you know, that we have and if I could say, too, it would be important to ensure that we have the authority to get the resources that we have when we are working with the other committees to ensure that we have the resources. So we thank you for your leadership on that. But clear direction and the authorization to have the resources would be very helpful.

Mr. UPTON. So DOE works with the Department of Homeland Security, TSA, and other agencies to ensure the protection of pipelines. But these agencies, as we know, certainly have other priorities. It is my understanding that TSA, despite having some 50,000

employees, is only able to dedicate some—a handful of folks, literally, three or four—to pipeline security.

So the question I might have is are you concerned by that fact, that a lead agency for pipeline safety is so stretched that only a handful of people would be working on pipelines?

Mr. MENEZES. Well, I can't speak directly to the resources and demands that they have but I can tell you from the experience that we have at DOE, having been over there now almost 4 months, all agencies are constrained to use existing resources to respond to new and additional obligations, for example, and it is a constant effort to find adequate resources to do things to accomplish our statutory obligations.

I will say that with pipelines both DHS and DOT co-chair, that sector-specific pipeline industry. We are involved through the oil and natural gas subsector coordinating council. And so we have regular interaction with the agencies that you mentioned and other agencies but also with the industry.

So, we are involved in it. But, again, it's always a challenge to find adequate resources within the current budget—to do the things that are expected of you.

Mr. UPTON. Thank you.

I yield for questions to the ranking member of the subcommittee, Mr. Rush.

Mr. RUSH. I want to thank you, Mr. Chairman.

Mr. Under Secretary, to date we have not experienced any large-scale cyberattacks on our energy grid. However, there have been minor incidences, maybe even what we might call probes into the system.

In your professional opinion, would you say that we have not experienced any large-scale attacks due to our defenses or is it simply because no entity has as of yet really attempted to launch a full-scale attack?

And do we really even know, rather, what their capabilities are of some of these foreign entities or rogue states that may eventually try to do us some harm?

Mr. MENEZES. Thank you for the question, Ranking Member Rush.

Yes, a very important question. We are at probably a historical turning point from what has been going on in the past. I had mentioned the ever increasing level of sophistication and the ever increasing number of threats. What has happened in the past simply is over and every day presents new challenges.

Some of the questions you asked would involve classified material that I can't get into today but it is public that we are facing threats today that we haven't seen in the past. The Internet of Things, all software, all of these are providing opportunities for those that are very creative to try to attack our systems, and it's ongoing. It's daily. It's 24/7. It is around the clock. Interestingly, as we know, that now it is machines that are doing all this and they're using artificial intelligence. So you have machines.

Our goal, of course, would be to counter their machines with our machines and our artificial intelligence. But it's an ever-escalating battle.

So you're right to ask the question. We don't even know what the future threats are. And this is part of the reason why we are standing up this office. We want this to be highly visible. We want this to be accountable to other agencies, to the Congress, so that you all have a much higher visibility on what DOE is doing.

So you asked the right questions. We are concerned about not only current but future threats and having the resources.

Pat, did you want to say something?

Ms. HOFFMAN. I just would also like to credit the strong partnership we have with industry and that we are keeping pace with respect to intelligence and classified information sharing, partnership with the ISAC for alerts and getting information out to industry as soon as possible, as well as partnerships and looking at engineering solutions and looking at technology solutions that will help mitigate some of the issues.

Mr. RUSH. That leads me to another concern, and that's our Nation's workforce preparedness when it comes to cybersecurity. Are we doing all that we can to ensure that we have a highly skilled trained workforce both presently and in the future to address cybersecurity issues?

Mr. MENEZES. We are doing what we can. I am not sure that we are doing everything that we can but we certainly are elevating education in the realm of preparedness in addition to response and ultimately recovery. But it's going to be research and development and breakthrough technologies to be able to protect and defend our system and to be able to respond.

So we currently have training programs in place where we deal with not only our workforce but also the industry's workforce because they have to have the benefit of everything that we see, we know, and that we are developing so that they can train and they can instill a culture of resilience within their organizations.

And I can testify firsthand on the past success of the leadership of this committee and working with the ESCC and the industry partners in DOE's role. I can assure you it was important for the electricity sector to have their CEOs participate, and when the CEOs participate they return to the company and they instill a culture of compliance and resilience and that they make many changes and they make sure that the workforce is very educated on these very technical and highly sophisticated programs.

So we are committed to ensuring that we have a dedicated and educated workforce.

Mr. RUSH. Thank you, Mr. Chairman. I yield back.

Mr. UPTON. The chair recognizes the gentleman from Texas, Mr. Barton.

Mr. BARTON. Thank you, Mr. Chairman. It's always good to see our good friend here in such a highposition.

This is an important hearing that we are having today because it addresses an issue that we really haven't done a very good job of addressing—this issue of cybersecurity and emergency response.

I am not real sure what cybersecurity is, first of all. So I guess my first question would be does the Department of Energy have a definition of cybersecurity?

Mr. MENEZES. Well, let me go back to the days that I was on that side of the dais in '05 when we decided to add the word cybersecu-

rity into the mandatory reliability provisions that we put in EPAC of '05.

We thought whether we should define it back then, to be frank about it, and we decided then that it was better to have it as, frankly, broad as it could be because we weren't sure what it would become.

And so consequently I am not sure if we have a formal definition. I am looking over at——

Mr. BARTON. So far you have done a very good job of dissimulating and not saying a darn thing so——

[Laughter.]

Mr. MENEZES. I know that.

Mr. BARTON [continuing]. But roles do change.

Mr. MENEZES. Yes. I don't think we have a formal definition. But——

Mr. BARTON. Well, do we need one.?

Mr. MENEZES [continuing]. Again, the Internet of Things and software typically are ways that they seek to gain entry into systems via those mechanisms.

Mr. BARTON. Mr. Chairman, let's let the record show that I stumped the under secretary of energy on the first question, but in a polite way, because he and I are friends.

Well, would you say that cybersecurity deals with the internet intercepting—somehow making it difficult for computer systems to operate, hacking into a controlled system or power plants or pipeline controls? Would that be a practical type of cybersecurity attack—something like that?

Mr. MENEZES. Yes, and you mentioned those are threats, right. But there's a security part of that, too. So it would include the communication systems, making sure you have resilient communication systems, control systems that you can monitor and detect and react and take action.

You had mentioned the threat detection and the analysis, and it's not limited to just one sector of the energy industry, for example. So you have points of potential entry into any systems and we are talking about supply chain today but we have generation. We have all the distribution. We have transmission. We have the producers, the vendors. It's all up and down the, every point.

Mr. BARTON. Well, let me ask another simple question, which you may not want to answer.

Which of our industries are sectors that the Department of Energy has responsibility for would you consider to be most vulnerable to a cybersecurity attack?

Mr. MENEZES. I think any that use the internet and use computers and are part of a system. And so when you get the briefings, we are members.

DOE is a member of the National Security Council and as such we have intelligence and counterintelligence and access to all of our sister agencies and we have eyes on things.

When you look at it, those that wish to penetrate our system will try all segments. So in that respect, we are all vulnerable. We are all constantly vulnerable.

Mr. BARTON. Let me ask my final question. To the department's knowledge, have there been any cybersecurity attacks on our energy sector that the Department of Energy is responsible for?

Mr. MENEZES. Attacks?

Mr. BARTON. Yes. Have there been attempts to——

Mr. MENEZES. Our systems are constantly being attacked. Constantly. Not only the DOE system but also the energy system.

Mr. BARTON. OK. Well, if you say constantly then I would interpret that to mean that we've successfully fended them off, since I am not aware of any breakdowns in our energy infrastructure.

Mr. MENEZES. Well, there have been some reported breaches, if you will. We are fortunate that we haven't had a major consequence of attacks and thus far we have been successful in identifying.

Part of this analysis involves modeling, information sharing, and monitoring. You may collect data and then you will use our experts' abilities to evaluate what we are seeing and then try to figure out what is happening.

Mr. BARTON. My time has expired. But would the department be willing to have a bipartisan briefing where you could go into some detail about the attempted attacks?

Mr. MENEZES. Yes, sir.

Mr. BARTON. Thank you.

Thank you, Mr. Chairman.

Mr. UPTON. Gentleman's time has expired.

Mr. McNerney.

Mr. MCNERNEY. Well, I thank the Chairman and, again, I thank the witness.

Are you familiar with the two bills that Mr. Latta and I have proposed—the Cyber Sense Act and the Enhanced Grid Security Through Public-Private Partnerships Act?

Mr. MENEZES. Yes, sir.

Mr. MCNERNEY. Do you think those bills serve a good purpose?

Mr. MENEZES. We applaud the committee for the leadership that you have shown and I think—has one of them passed already, I believe? In past Congresses?

Mr. MCNERNEY. Right. So——

Mr. MENEZES. And I will say that on the supply chain—you have already seen action, right. You have seen action from NERC in proposing critical infrastructure protection standards. So you see it pending at FERC so certainly your past efforts have generated that activity. It's also generated activity here in this administration because in the fiscal year 2019 request we requested additional moneys to do what your bill is proposing to do.

Mr. MCNERNEY. Do you have any suggestions on improving either one of those two pieces of legislation?

Mr. MENEZES. Again, my suggestions would be as you choose to send direction over—and obligations over to the Department of Energy if you can authorize resources we find that that helps us because otherwise the department typically would be forced to figure out where to get resources that it's currently using for other——

Mr. MCNERNEY. But speaking of resources, the fiscal 2019 budget looks like a 40 percent cut in the electricity delivery and reliability account, which then is split into two further accounts.

So you're saying on the one hand that you need resources and on the other hand the administration is proposing significant cuts in program funding.

So how can they reconcile those notions?

Mr. MENEZES. I think the OE budget cut—I believe it's the case where it shows that we are pulling out almost $96 million and moving it into CESER. So it's creating a new office. But we are still——

Ms. HOFFMAN. We see an increase in CESER budget line for the 2019 request to $96 million.

Mr. MCNERNEY. I saw that, but I mean, I hear that you keep saying we need more resources and yet some of these line items are being significantly slashed.

Mr. MENEZES. Well, can I point out a victory that this office had with the administration?

As many of you know, because of the several trips that we've taken to Puerto Rico, for example, on the emergency response, OK, a very critical part—I know we've been talking about cybersecurity but if you will allow me to talk about that.

Again, when we got over there and looked at our resources, it was surprising. It was surprising to me that all the work that DOE was doing on emergency response in this hurricane season, for example, the resources were, I thought, insufficient.

We asked the White House and they agreed to double the budget of the emergency response, of ISER—our Infrastructure Security Energy Recovery.

Mr. MCNERNEY. So you're saying that in general terms the administration is acting in a way that'll increase your resources. Is that what you're saying?

Mr. MENEZES. In this area. In this area.

Mr. MCNERNEY. In this area?

Mr. MENEZES. Yes, and it's in our fiscal year 2019, to set up CESER. It's all in the congressional justification for it. So——

Mr. MCNERNEY. So, I mean are you——

Mr. MENEZES [continuing]. So we have support in the administration on the topics that we are talking about today.

Mr. MCNERNEY. So in a sense, are you robbing Peter to pay Paul for the CESER?

Mr. MENEZES. No. No, we are not. No, we are moving some existing programs over to CESER just to begin to set up the office and so that was not a—in fact, that's an increase. That is actually an increase.

So, again, together it's going to be $96 million and that is an uptick of about maybe 16 percent, I think, from what it was in fiscal year 2018.

Now, CESER didn't exist—fiscal year 2017. So it's a positive story here.

Mr. MCNERNEY. All right. Mr. Chairman, I am going to yield back.

Mr. UPTON. I would just note that we've got Secretary Perry scheduled to come next month to talk about the budget as well.

Mr. Olson.

Mr. OLSON. I thank the chair. Welcome to our two witnesses.

My first question will be about Hurricane Harvey. I followed your reports on Hurricane Harvey—the situation reports very closely as the storm hit and after the storm hit and the impacts on our energy sector—the Port of Houston and the petrochemical complex.

DOE was a good partner. Worked hand in hand with Governor Abbott, with the local county judges, my county judge, Bob Hebert, Fort Bend County, county judge Matt Sebesta, Brazoria County, county judge Ed Emmett, Harris County. He helped to get waivers they needed and the assistant had to ensure the permits and waivers were issued without delay. That's very important.

You mentioned, Mr. Menezes, that the budget has been doubled now since lessons learned from Harvey for recovery efforts.

What are some lessons learned like that that we could apply in the future, going forward, from Hurricane Harvey? Feel free, both of you, to make comments about that question.

Mr. MENEZES. Well, I am aware that we did an after activity report, I believe. I might defer to Pat. I think she's in possession of that report.

I am not sure if it's finalized or not but certainly we will make it available to all members of the committee.

Pat, do you have specific comments on that?

Ms. HOFFMAN. Yes, thank you very much for the question.

I think I would applaud industry's effort as well in Hurricane Harvey and Irma and Marie and the strong work that they've done.

Some of the lessons learned is as we continue to move forward the industry is on the front line so exchanging coordination of information is critical and absolute for having an effective recovery and restoration process and I think that's where you have seen the success as well as some of the lessons learned. From a department perspective, being able to engage our power marketing administrations, to be continuing to use the strategic petroleum reserve are all important aspects of how the department can help in a restoration process. The waivers and the coordination with industry were always very positive and helpful to support so being proactive in those areas as we continue.

As we look forward on cyber, as we think about that, some of the needs and the issues are really being proactive in looking at threat analysis, continuing to support the mutual assistance program, and I think whether it's hurricanes or cybers, we really want to be able to engage stronger in the mutual assistance program in support of industry.

Mr. OLSON. And you all read my mind. Let's now talk about cyber.

Attacks happen on America every single day in cyberspace. Bad actors have attacked our power industry. They've attacked refineries, chemical plants, pipelines, all across the spectrum.

You mentioned, Mr. Menezes, about AI—artificial intelligence. I formed a caucus here in the House to look at those issues and I have a bill out to get us on board with AI because that's our future to prevent some of these attacks.

My bill just basically says let's partner up with the private to make sure these attacks don't happen through cyberspace and use AI as a weapon. AI is to empower people. It's not to have machines

run our world but it's to empower people with information to make sound decisions when a disaster hits, like a hurricane. And just like you commented about, the bill basically says let's have a true public-private partnership, support the private sector, empower them with the public sector's assistance, make sure we adjust jobs because there's lots of jobs being lost or jobs being created, have facts about jobs. Also bias—there's natural bias can be around information that may be biased—avoid that, and also privacy—big issues.

But how can AI help out with the recovery from Harvey and those you're facing?

Mr. MENEZES. Well, thank you for that question, Mr. Olson.

You raise a very important point. AI will be the future of how strong and resilient we can be because of the ever-growing sophistication of these attacks.

With respect to your bill, again, the administration doesn't have a formal view of it. But as a general rule——

Mr. OLSON. It's good. Trust me.

Mr. MENEZES. As a general rule, all the direction that you can provide to us, particularly in the use of tools that we can use within industry, former Chairman Barton had asked about attacks on the system and we are here representing the department and to be sure, the department is subject to attacks.

It is our industry, however, that typically would be front line because the bad actors would look for soft targets. It might not spend a lot of effort in going after government assets that they think are going to be hard targets.

So they're developing artificial intelligence to probably identify those risk levels. Well, industry is going to be on the front line and so it's very important that we get a set of tools and resources to be able to work with industry and to help industry have the resources and the knowledge and the wherewithal to be able to anticipate, predict, react, respond, and to make their systems more secure.

Mr. OLSON. Amen. Machines to empower people, not take over the world. Thank you for your comments. We're working for this.

I yield back. Thank you, Chairman.

Mr. UPTON. Gentleman's time has expired.

Mr. Tonko.

Mr. TONKO. Thank you, Mr. Chair, and to Secretaries Menezes and Hoffman. Welcome. It's good to have you back again.

I know DOE is taking its role as the sector-specific agency for cybersecurity seriously. But I have a few questions on the reorganization of the Office of Electricity Delivery and Energy Reliability. And, for the record, I am not necessarily opposed to the change but I would like to understand how it might affect DOE functions as we move into the future.

Last month, Secretary Perry announced the creation of the Office of Cybersecurity, Energy Security, and Emergency Response which, as I understand it, will take existing programs from the Office of Electricity.

Can you explain the vision for this cybersecurity office moving forward and do you expect to add new programs or functions to this office over time?

Mr. MENEZES. Thank you for that question. It's a very good question.

When the secretary arrived over at the department, and you have your security clearance, right, you get briefed and your world view changes, and almost immediately it became very apparent that one of the top priorities will be resources for cybersecurity and, again, the physical security—and we were in the hurricane seasons as well and so those three things came together very quickly. Just from an experience point of view.

The department, of course, had a history of dealing with these issues and so we began a process where we evaluated everything within the department, our stakeholders.

We talked to members of Congress and staff. We talked to the appropriators. We talked to OMB and the White House to formulate a process to bring the visibility and enhance the importance of these three topics.

Since this is an initial establishment, the DOE Org Act has given us the authority to do this—but it wouldn't surprise you to find out that our appropriators and others had some very keen views on what assets and what could we do to begin the process.

So I would like to emphasize this is an initial step and so what we did was we identified within the department those successful programs to begin to process to move them over into a new office. So it was to simply begin that process.

So we identified those two, the R&D within OE and the ISER function also within OE. It just happened to be that they're both in OE.

It doesn't diminish what we continue to expect out of OE, the Office of Electricity, and it's just a beginning point for this new office.

Mr. TONKO. And what will happen to other programs from the Office of Electricity?

Mr. MENEZES. What will happen with what?

Mr. TONKO. The other programs from the Office of Electricity.

Mr. MENEZES. Well, they will continue and we will—in a——

Mr. TONKO. In that realm? In that given division?

Mr. MENEZES. No, the Office of Electricity will, of course, help in seeing the transition of them. But the Office of Electricity has other critical functions too that they will continue to do and——

Mr. TONKO. Does that include the non-cyber R&D portfolio focused on grid modernization and storage?

Mr. MENEZES. Yes. Yes. They will continue to do that.

The other thing I want to point out is that one thing that we started at this department is it's a hallmark of this administration at DOE because of our backgrounds is to engage in much more of a collaborative effort between all of the programs.

We are about busting these silos. Now, we are limited to the actual offices due to revenue streams. But as a practical matter, we collaborate. We share responsibilities and you know that we coordinate certainly all of our labs. So what you're seeing over there is a coordinating effort and a collaborative effort so that we can make use of the resources that we currently have to do the things that are important.

Mr. TONKO. Will there be any split of the Office of Electricity staff—the FTEs, or full time equivalents going in another direction or will they stay intact as it is now?

Mr. MENEZES. Well, we are in the process of identifying which employees will ultimately report to or be part of the new office and there's a series of procedures and policies that we have to follow in order to do that. But we are going to be in full compliance with all of the regulations that we need to do.

Mr. TONKO. Well, it's important, I believe, that cybersecurity gets proper consideration in resources. I also believe the work being done by the Office of Electricity on grid modernization, on micro grids and on storage is also critical and I hope that these offices will be working together and not having to compete for resources. I think that's very important.

Mr. MENEZES. You have our commitment from that, sir.

Mr. TONKO. OK. With that, I yield back, Mr. Chair.

Mr. UPTON. Mr. Shimkus.

Mr. SHIMKUS. Thank you, Mr. Chairman.

It's great to have to have you—good to see you again, and welcome to the committee.

So I hate acronyms. So CESER is the Office of Cybersecurity, Energy Security and Emergency Response Management, correct?

Mr. MENEZES. Yes, sir.

Mr. SHIMKUS. When you use CESER that's what you're referring to and that's a new organization within the Department of Energy to address grid resiliency, which can be defined by either concerns of attacks or cybersecurity or the like. Is that fair?

Mr. MENEZES. That is fair, and it will be headed up by an assistant secretary.

Mr. SHIMKUS. You used a good terminology—you want to bust the silos that occur in major bureaucracies so we have people talking to each other.

Mr. MENEZES. Yes, sir.

Mr. SHIMKUS. So, so far so good. I think it's needed. It's something we've talked about for a long time.

So let me address a couple questions, and former Chairman Barton had raised just the whole cybersecurity—how do you define.

So that's the whole issue of what could be points of entry. My colleague, Mr. Tonko, mentioned the micro grids, which kind of are developing in our country and then the question would be cybersecurity of entry through a data control system that then could make instructions to transformers, through generation, through the like.

So that's one way there could be disruption. And isn't that also the reason why we want—which we did in the last Congress, talked about quite a bit—I think you mentioned the fact that we had moved the bill—we do want some communication between our government agencies and the private sector. Why is that important in this debate?

Mr. MENEZES. They're on the front line. It is they're, A, providing the service. They are doing the things that we've come to expect from our energy infrastructure. They own and operate the actual facilities, they develop the software, and they rely on the supply chain, all of which could be vulnerable. And so as the government

agency responsible for that, we need to ensure that they do have the training, they have the know-how.

We share with them information upon which they can identify, train, and respond and recover, ultimately. So they're on that front line, which is not easy. It's a lot more than——

Mr. SHIMKUS. So, they're seeing some front line attacks that they can then talk to you and we can address training and—not remediation but countermeasures, I guess, would be.

Is CESER able to then also talk to our intel communities for higher level cyber concerns that could be then passed on to the private sector and say, hey, watch out for this?

Mr. MENEZES. Correct. In fact, the information sharing and analytical center has developed CRISP, which is the Cybersecurity Risk Information Sharing Program.

Mr. SHIMKUS. Thank you.

Mr. MENEZES. Yes. Just threw out a couple more acronyms your way. And the importance of that is that while the ISAC manages that, it uses information that is shared by our intelligence-counterintelligence that we receive.

I had mentioned previously as members of the NSC, we have resources that some agencies do not have and with special protections in place for classified information we share that information to the extent that we can, and it has been very helpful and useful in identifying threats that without it we still would not necessarily know that our system was even attacked.

Mr. SHIMKUS. Let me go quickly. My time is almost expired. Talking about electromagnetic pulses either intentional or naturally occurring, the hardening of systems, the cost, and the communication with the private sector, I mean, the private sector when we talk about it they just say, oh, the cost is too much—can't do that. And there is some cost, but I think it is a concern that I hope that you all and maybe even this CESER subsection of DOE is talking about.

Mr. MENEZES. Well, I would say that a hallmark of any technology that we develop, any training system, it has to be cost effective. Clearly, we cannot give them information that imposes such a burden that——

Mr. SHIMKUS. But are we talking on EMPs both naturally occurring or bad actors? Is that part of what you're discussing or——

Mr. MENEZES. Yes. CESER does have the energy security part of it so it would include the EMPs as well and the GMDs, if you want another acronym.

Mr. SHIMKUS. Thank you. My time has expired.

Mr. UPTON. Mr. Loebsack.

Mr. LOEBSACK. Thank you, Mr. Chairman, for holding this important hearing and I do appreciate both of you being here as well—the witnesses. Thank you so much.

I don't think that we can argue with the fact that it's absolutely critical that we do ensure the safety of our energy infrastructure and in the 21st century we all know that a very critical emerging threat that's been talked about today is cyberattacks and we've got to just work as hard as we can to make sure that we protect that energy infrastructure.

I am very proud to work with Chairman Upton. We actually can do some things on a bipartisan basis in this committee and I think we've done a lot, but to make sure that we get adopted eventually and implemented H.R. 5175, the Pipeline and LNG Facilities Cybersecurity Preparedness Act. So I want to thank the chair for working with me on that, and vice versa. It's great.

I do think it's absolutely critical that we make progress to ensure the cybersecurity and safety of our natural gas and LNG facilities and I believe that this bill is a step in the right direction.

Physical threats to pipelines and energy infrastructure do remain a significant threat, as everyone on this committee knows and you folks know. But these days our pipeline system is increasingly technologically sophisticated as we get new pipelines put in place and that does, I think, probably increase our vulnerability in some ways to cybersecurity attacks. And for the life of me, since I speak a little Spanish and even more Portuguese, I cannot figure out yet how to pronounce your name—why it's only two syllables.

Mr. MENEZES. It's Americanized Portuguese.

Mr. LOEBSACK. Yes, I am aware of that.

Mr. MENEZES. You were right on that. And so we've apparently had the middle E become silent. So it's Menezes.

Mr. LOEBSACK. Thank you for explaining that. Mr. Menezes. Thank you so much. Thanks for being here today.

As we mentioned, DOE has to play a critical role in ensuring the safety and security of this infrastructure can you elaborate a little more about the level of vulnerability of our pipeline system to cyberattacks? You have spoken about that some this morning already but can you elaborate even more, within the context of an open hearing, at any rate?

Mr. MENEZES. Right, and so I will keep it general.

Perhaps the vulnerability on the pipelines exist because it's a transportation system at its sense and it—probably the control mechanisms, the communication systems, and the operations systems, they may not be as fully integrated, say, as a fully operating electricity company in all sectors, for example, in the—and so as a consequence it may be the assumption that because they're more simplified, if you will, you might not have to develop technologies to make them as resilient as any other point of entry.

So as they are improving their efficiencies they are bringing in new softwares and new devices and, again, the result is you see the flow of product. But as they become more sophisticated, we need to ensure that what they put in has the resiliency programmed in at the front end——

Mr. LOEBSACK. Right.

Mr. MENEZES [continuing]. So that it's resilient, and that's going to be the key. So——

Mr. LOEBSACK. Because I was kind of shocked actually at an earlier hearing when I found out that there isn't a lot of Federal involvement when it comes to pipelines in the first place. There's sort of oversight after they're already in place but there's precious little involvement as they're going in. I think that's one area where there can be more involvement to make sure that these things are put in properly and that they are secure.

Mr. MENEZES. Yes. We are doing what we can in our role for the oil and natural gas subsector coordinating council and we do have monthly meetings with the group and we have quarterly meetings as well with the larger group that is co-led by DOT and DHS and we do bring in all those other agencies. So we have a structure within the existing authorities to try to address that.

Mr. LOEBSACK. Yes.

Mr. MENEZES. There's a lot of information sharing and it's important. You have got to be at the meetings. You have got to be willing to participate. And they are, by the way. I mean, they are.

Mr. LOEBSACK. And just very quickly—my time is running short. Thank you very much. I want to make sure that you folks are prepared as a department in the event that this legislation is passed, be able to put this into effect.

I do have one other question. Maybe you could respond in writing to me if that's possible. We have a lot of existing pipelines now that may not be as subject to cybersecurity threats.

I don't know the answer to that, and maybe you could distinguish in writing for me those that are already in the ground, already exist, versus the newer ones which might be more vulnerable, given the technology, and I would really appreciate an answer to that question, perhaps in writing if that works for you.

Mr. MENEZES. We'll be happy to get back with you on that.

Mr. LOEBSACK. Thank you so much.

Mr. MENEZES. Thank you.

Mr. LOEBSACK. Thanks. Thank you, Mr. Chair, and I yield back.

Mr. UPTON. Mr. Latta.

Mr. LATTA. Well, thank you very much, Mr. Chairman, for holding today's hearing. This is very, very important when we are talking about cybersecurity and also the emergency response.

But before I do, and I know he's stepped out right now, but I just want to recognize Mr. McNerney from California who's been working with me and all the hard work that he's done on the issues, especially with grid security.

Mr. Under Secretary and Ms. Hoffman, thank you very much for being with us today because, again, this is a very, very important topic that we are dealing with today.

In your testimony you noted that securing the electric sector supply chain is critical to the security and resilience of the electrical grid and products must be tested for known vulnerabilities in order to assess risk and develop mitigations.

Would you explain the consequences of having a device or a component in the electric system that poses a cybersecurity vulnerability and, more importantly, do we have the adequate measures right now in place to protect that supply chain?

Mr. MENEZES. Great question, and thank you very much for it.

Our supply chains probably would be our most vulnerable areas and by supply chain it could be any component part that any of our energy partners would rely on. That could make our entire system vulnerable. If point of entry could be on what you think is a routine software program, perhaps to do accounting for a supplier of valves, for example.

OK. So the importance has been noted in a couple of ways. NERC has already proposed CIPs—the critical infrastructure pro-

tection standards—which is pending at FERC to address this very supply chain issue with respect to the agencies that are responsible for developing our mandatory reliability provisions for the electricity grid and this administration in fiscal year 2019 has requested additional money so that we, with our labs and our experts, can similarly test these products for their vulnerabilities and we can mitigate those vulnerabilities. So we can make the whole system stronger by really addressing those most vulnerable, if you will.

Mr. LATTA. Also in your testimony you referenced the budget proposal to invest in testing supply chain components and systems and under the Cyber Sense bill seeks to authorize a related program focused on identifying and promoting cybersecure products using the bulk power system.

Again, would you elaborate on the work that the DOE is doing to test the supply chain components and systems and also in a follow-up of that, how does the quality control for supply chains help in ensuring that cybersecurity?

Mr. MENEZES. I will allow Pat has more experience directly on this.

Ms. HOFFMAN. So, through the Electric Sector Coordinating Council and our discussions with industry, the supply chain need has been highlighted as extreme importance and so I appreciate the committee's efforts in this area.

What we are looking at is actually partnering with industry to test and do a pilot program to test several components that are critical in the industry to do a deep dive testing of the components and subcomponents. What the industry would like to understand is all the vulnerabilities so they can assess their risk and the risks that they are facing. So part of what the NERC standards also emphasize is the disclosure of vulnerabilities and the continued testing. One of the things that we want to emphasize is as we are looking at testing of components there may be a new vulnerability or a new threat vector that's discovered tomorrow. So what should be institutionalized is a process for continual improvement in cybersecurity.

As we've talked about the definition of cybersecurity being secure, information technology, secure firmware software, the information side of the industry, we really need to continually test products, continually improve products, just like we would do from a manufacturing point of view.

So that philosophy of continual improvement is absolutely critical and testing with the national laboratories can help identify some of the vulnerabilities and continue to advance the improvement of products.

Mr. LATTA. When you're testing the products, how do you get that information out to the industry? Because just like this past Friday I spoke at one of my electric co-ops in my district—I have the largest number of co-ops in the State of Ohio—and not too far in the past from that I also spoke at another one. But how do you get that information out, especially with these products, to make sure that they know that they're, A, available and, B, that they're tested and they ought to be utilized once they're approved?

Ms. HOFFMAN. So the goal is to get the information out through the supply chain community and I am sure the next panel will talk about that and details of having that disclosure and that collaborative relationship with the industry with the mitigations and the solutions. But the other area is through our national laboratories and through, say, the ISAC program to continue to really identify some of the vulnerabilities but get it out to industry and all the components and all the sectors in the industry.

Mr. LATTA. Yes. Well, thank you very much, and I yield back.

Mr. UPTON. OK. I would recognize Mr. Kinzinger. No, I am sorry—Mr. McKinley.

Mr. MCKINLEY. Well, I wasn't expecting that. Thank you, Mr. Chairman.

Mr. Menezes—or Secretary Menezes, a couple questions quickly, if I could.

Three years ago we had Tom Siebel—he's the CEO of C3 Energy—testify before us about cybersecurity and the grid, and he made a very revealing comment.

He said that just a small group of engineers would be able to shut down the grid on the East Coast in 4 days, and it would shut down the grid between Boston and New York. Did you ever see his testimony or respond back to him on that?

Mr. MENEZES. I did not see it.

Mr. MCKINLEY. The fact that a lot of things have happened and I appreciate your answers back to Barton where you said that we are constantly under attack. And maybe it's worked but I am saying there are groups saying the engineers can do this. They can still get past your system if they want to do that.

So the other thing, and just maybe it was coincidence in 2015 Ukraine was faced with a cyberattack. The Russians apparently are the ones that contributed to that. What have we learned from that? Did we interact with the Ukraine and find out how that was shut down so we could prevent that from happening here?

Mr. MENEZES. Since that occurred before I arrived, I will just——

Mr. MCKINLEY. Just quickly, because I've got a series of more questions. Yes or no, have we interacted with them?

Ms. HOFFMAN. The answer is yes. We worked closely with them. We actually gained some knowledge of the attack. We have had training sessions with industry and analyzing so lots of——

Mr. MCKINLEY. OK. But we've learned something from it.

But then let me go also now go back even further in history. Back in 2007 there was an Aurora generator test that was maybe controversial. Are you familiar with it, Secretary?

Ms. HOFFMAN. Yes, I am very familiar with it.

Mr. MCKINLEY. OK, you are. OK. Because they were able to display that just by entering 21 codes they could blow up a generator and thereby set in motion a blackout in the United States.

What have we done to prevent those 21 codes from being introduced?

Ms. HOFFMAN. So we worked with industry in analyzing the Aurora attack and looking at the focus on relays and the vulnerabilities in that. The industry has looked at mitigation solutions. We've done information sharing with industry.

So it's been an active engagement with the industry.

Mr. MCKINLEY. Have they taken action, implemented things to prevent that from happening with that?

Ms. HOFFMAN. The industry has implemented and has taken action per some of the requests from NERC in doing that.

Mr. MCKINLEY. OK. The third question or second question has to do with vulnerability because you talk about emergency, and we have a report here from New England saying that they're not going to have enough gas if there's an emergency situation that's coming up and they say that because during the cold weather they're having to divert that gas to homes and so there's not going to be gas for power plants.

We've experienced that in West Virginia. We had a black start plant that had to shut down during the Polar Vortex and just this last winter was told that they were on day to day—they may have to shut down as well.

So I am wondering about in an emergency how are we going to make sure that we have gas available for our power generation, let alone cyberattack? Is there a solution to that?

Mr. MENEZES. Well, we need more infrastructure, to be sure, both what you referenced. The New England ISO, together with NERC, has identified areas in the country where we rely heavily on natural gas for our power generation to ensure our resilience and the reliability of our grid.

It's in those constrained areas where it's important that we try to increase the infrastructure so that we can have adequate supply. That has been the hallmark of this administration so that we have a sufficient diversity of fuels including natural gas.

Mr. MCKINLEY. If I could, Mr. Secretary, but we are relying on Russia for bringing in LNG to New England and now they've unloaded their second tanker on this.

So if we are going to be energy dominant, how are we energy dominant if in an emergency if we are going to rely on a foreign government to provide us a natural resource to be able to provide electricity in New England?

Mr. MENEZES. Well, good question. Well, the President has announced his efforts for the infrastructure bill and contained therein or recommendations on how we can help to site and build, construct, and permit these—in this case, natural gas pipelines to address the issue that you raised.

Mr. MCKINLEY. Right.

Mr. MENEZES. It's not limited to that but it is a component part of that. So it's also a function of working with the States because under federalism the states have a big role to play as to any interstate gas pipelines ——

Mr. MCKINLEY. I understand. I don't want a heavy hand——

Mr. MENEZES. There's so much we can do.

Mr. MCKINLEY. I don't want the heavy hand of the Federal Government stepping in. But there is a concern.

Just in closing quickly, could you tell me what keeps you up at night? What is your biggest concern, from your position?

Mr. MENEZES. Well, in the cybersecurity, clearly. Your worldview changes as you get a security clearance and you get briefed on what's happening.

I think you all have been read into a lot of this stuff. But yes, that causes me to stay awake and, frankly, as we have seen what are becoming common winter events when our system is stressed it seems as though we may be faced with an inadequate supply of what used to be baseload. So the premature closing of what historically has been—whether it's nuclear or clean coal, these facilities are going offline.

We are becoming more reliant on natural gas, which is not a bad thing. But it does have to get through pipelines and we've seen in the cyclone bomb, if you will, on the East Coast we see natural gas actually having price spikes, which forces the operators to go to nuclear, coal, and, believe it or not, oil. So those are the things that keep me up at night.

Mr. MCKINLEY. OK. Thank you very much. I yield back.

Mr. KINZINGER. Thank you, Mr. Chairman. Thank you all for being here.

I know we all recognize the very serious threat we face with cyberattacks. It can be especially difficult as the threats we face are constantly evolving and can vary significantly. Individual bad actors are constantly attempting to obtain bank routing numbers or medical records from everyday Americans—while state actors, for example, North Korea's attack on Sony Pictures or China's break of the OPM files, represent a very different kind of threat. And for a lot of these nonstate actors, a very low barrier of entry.

In the energy sector, we have to prepare for any level of attack, given the innerconnectedness of the grid. Even a relatively small scale attack on a single asset could have serious consequences.

I will ask both of you, just whatever you can do with this. If you can elaborate on how the work the DOE does, like R&D, industry information sharing, and physical hardening of assets to combat cyberattacks, is flexible and able to evolve as the threats change. You might have addressed this to some extent.

Ms. HOFFMAN. Sure. I appreciate the question. We've been actively engaged with industry and we know that the core components of a strong cybersecurity program really looks at building capabilities. And so our goal is to help industry build as much capabilities as possible so our R&D program is focused on supporting that capability development.

So from an information sharing program, let's look at a continuous monitoring or an ability for intrusion detection. It's a capability that the industry needs to have and a support that we've been providing through the risk information sharing program that we've developed with industry.

Other activities is really trying to get ahead of the game and looking at threat analytics but engineering some cyber solutions to prevent and mitigate some of the events that are occurring or the events that could cause damage to the equipment.

One of the things that we want to do is look at continued sharing of programs but also incident response and I think that is the next phase of which we must advance in is supporting the development of incident response capabilities so those tools and capabilities to identify where actors are on the system but also to prevent them from continuing to progress from a cyberattack point of view.

So our R&D program, we also have two strong university programs, one with the University of Illinois and one with the University of Arkansas, to develop the next generation solutions as well as partnerships with the national laboratories, looking at a moving target type activity to think about how could we make the system more dynamic.

Mr. KINZINGER. And to drill down a little bit, it was mentioned, sir, in your testimony that the cyberattack on Ukraine, which the CIA attributes to Russian military hackers, we've experienced a number of attacks by state actors here.

Does DOE plan for these kinds of coordinated attacks differently and what systems are in place to ensure that the DOE is receiving the most pertinent and up to date threat information from our intelligence agencies?

Mr. MENEZES. Right. As Pat Hoffman had testified earlier, the lessons that we learned with respect to the Ukraine.

But I would like to point out that we work with NERC on the GridEx exercises where we have these kinds of situations and we bring industry in, government in, all the stakeholders in, and they participate in a real live situation, if you will, that brings to bear the most sophisticated approaches that we have seen to date.

So it's been ongoing. It had been a success story by all measures. We gain a lot from that. The industry gains a lot from that. I can vouch from industry that you take those lessons learned and you implement them. And they could be as simple as revealing, for example, that you might need satellite phones, for example, because when you lose your power you need to be able to communicate and you need to have enough satellite phones.

So it can be something as simple as that to something much more sophisticated to developing, a more resilient software program, for example.

Mr. KINZINGER. Thank you.

And DOE has a long history of promoting a strong energy workforce and I think we all recognize the need for well-trained cybersecurity professionals in both the private and public sector.

As part of the new announced Office of Cybersecurity, Energy Security, and Emergency Response, does DOE plan to engage in cybersecurity workforce development? For whoever wants to answer that.

Mr. MENEZES. Right, to repeat what we had previously said, the short answer is yes. We currently have in place training programs throughout the process, whether it be at the front end on preparedness. We make sure that you have training to anticipate, identify the new threat vectors, how do you recover. And, of course, what's most important is to have the innovative R&D in place. So while driven primarily by our labs together with industry it's important that we train the workforce, and the workforce is not just in the departments or the governments. It's in the industries themselves and it's not limited to just the big player in the industries but it's all the participants which we have in place right now to cover the large utilities of all sizes whether you're a muni or a co-op.

So we are trying to develop and implement and train and maintain and enhance these programs.

Mr. KINZINGER. Thank you all, and thanks for your service to the country.

I yield back.

Mr. UPTON. Mr. Griffith.

Mr. GRIFFITH. Thank you very much, Mr. Chairman, and thank you, Mr. Under Secretary, for being here. I appreciate all your work on emergency response and Puerto Rico, and I know you're passionate about trying to make everything safer.

I am going to shift gears a little bit. My colleagues have asked some great questions on what we already have and I appreciate that, and my colleague on the other side of the aisle, Congressman Loebsack, touched on this earlier and asked you all to get back with him on whether the new pipelines with more technologies are more vulnerable than older ones already in the ground.

I would hope that you would include me in whatever response you give him because I am interested in that. And we have a new pipeline that's being built in my district and a lot of my constituents are concerned about all kinds of issues. And so I would also ask, and not expecting you to have an answer today, but also ask that you take a look at what can we do as far as making sure that the new pipelines have technology in them that lets us know if there's an earthquake in the area, a collapse somewhere. The faster that people know about it the faster we can respond. Folks are very concerned about possible breaches.

I've mentioned natural disasters but it could also be bad actors from outside. And also I think maybe we need to look and would like your help in figuring out if we need to draft legislation that would get DOE in on the front end, as Mr. Loebsack pointed out, because I am not sure that FERC is looking at, OK, how can we make this pipeline less vulnerable—should we move it away from the more occupied area of a particular—let's say we have a farm. Should we move it away from where the house and the barn are and—to an area that's less likely both to be attacked by bad actors or to create a problem should there be some kind of an issue.

Likewise on that same vein—I am going to give you a second here but I just want to get it all out before I forget something—it would also seem to me that DOE would want to know who had extra capacity and a new pipeline with the right kind of technology could tell you instantly whether or not they had the ability to take on more natural gas at a particular moment should there be a failure in some other area so that we can get that natural gas to where it needs to go by rerouting it possibly. And we've got two coming through Virginia, one through my district, one going through Bob Goodlatte's and other districts.

While we are laying this pipe is the time to put in any new innovations and new thoughts into that, and I am just hoping that DOE has some thoughts and plans. And I will give you an opportunity to respond to that now but also ask that you get back to me on all those thoughts that are important to me intellectually but also important to the constituents in my district—that they want to feel a little bit safer about this pipeline coming through their back yard.

Mr. MENEZES. Well, thank you for the series of questions and the commentary.

Of course, we agree with the issues that you have identified. If I can just take a quick crack at it, if you will, Pat, and then I will defer to you. But, first of all, with respect to developing the technology on the resiliency side of it, first of all, you hit on a key point.

As you know, our system is becoming more and more open. We are actually excited about all the possibilities of getting more inputs on either side of the meter. Individuals will be able to gain input. We are increasing the flexibility of our grid for a variety of good reasons—make it more resilient, more reliable. However, every time we make it smarter it's a new entry—it's a potential new entry. So in my conversations with the lab directors, for example, whom we meet with regularly on this, as they're developing ways to make things more efficient or greater access, more individuals who can get electrons—produce whatever they want when they want it, as an example, I make sure that my message to them is as you develop that new technology, please, at the front end, design it in such a way that it is resilient and it is secure. And so that message is out and they are doing that. So that's on that question.

With respect to the question on the extra capacity to take on more natural gas, I will say that we work with our other partners. I mean, we work with FERC. We work with NERC.

We are aware of the interoperability issues there. We are also aware of other potential issues that might give rise, when you're talking about sharing market information and that kind of thing. So those things have to be looked at and considered carefully.

But the short answer is yes, to the extent that as we are making these improvements and we are spending these resources and we are developing these programs and we are improving technologies, I think you can look at it holistically, if I can use that word, to describe what you were discussing.

And with that, I will pass it to Pat if she wishes to say something.

Ms. HOFFMAN. Just really quick, adding the resiliency looking at four and minus one contingency or single point of failures.

I think also another point that I would like to bring up is you're absolutely right, having the ability to increase the amount of sensors in the system to be able to predict and get ahead of the game as we look at failures as a critical component that we think is an important part of our program in improving resilience.

Mr. GRIFFITH. I appreciate it, and I yield back, Mr. Chairman.

Mr. UPTON. Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman, and I want to thank both of you for being here today. Such an important topic, cybersecurity, particularly as it relates to energy and our energy infrastructure.

I dare say that most people don't really think about the implications of cybersecurity when it comes to infrastructure and the importance of it. So when looking at emerging cybersecurity risk and particularly threats of the highest consequence to energy infrastructure, it seems critical to me that DOE have full visibility on the greatest infrastructure risks and consequences.

Do you believe, Mr. Under Secretary, at this point that DOE has sufficient visibility to day on what those risks and vulnerabilities are?

Mr. MENEZES. Well, we currently have sufficient visibility but it is the future that we need to anticipate. And so today's hearing is about how it is that these increasing threats will require us to have greater visibility and the resources which is why we've set up this office that we affectionately refer to as CESER.

Mr. JOHNSON. Yes.

Mr. MENEZES. So we are doing OK today, as several members have identified. It seems as though while we have the constant threats we've been able to avoid a major catastrophe. But we want to make sure that going forward we have the visibility and the resources. I think Ms. Hoffman would like to say something.

Mr. JOHNSON. Sure.

Ms. HOFFMAN. I think it's important to continue to support the information sharing between industry and the Department of Energy in understanding the number of events that are going out. The critical need, as the under secretary has talked about, moving forward, is that we want to get ahead, we want to see what the next generation threats are. And so that close public-private partnership and information sharing and the flexibility and the freedom for the industry to voluntarily share information with the department is absolutely important.

Mr. JOHNSON. OK. I am encouraged by that answer because I've long held the belief and I still do that this is not an issue that has an ending to it. This is not a race that we are going to run and cross the finish line. As soon as we figure out how to keep the bad guys from getting into our networks, especially in the digital world where everything is connected, as soon as we figure that out, we've got another problem right on the tail end of that.

So I appreciate that there's a forward look and an understanding that that's the case. So what measures can you take to increase visibility of security threats today?

Now, you mentioned some of them. You have created this office. Can you give us some examples of what some of the future look areas are?

Mr. MENEZES. I will take the larger view and I will defer then to Ms. Hoffman on the specifics.

But the creation of the CESER or the establishment of the CESER program is just an initial step and we are taking existing programs and putting it in.

Our vision, though, is much greater and so we want to work with this committee and other members of Congress—the White House, our other agencies—to actually put in place other programs, projects, and the resources to anticipate the increasing threat.

And so that's the big picture and that's why it's important, we think, to set this up and have it under an assistant secretary.

Mr. JOHNSON. OK.

Ms. HOFFMAN. So I would just add three things. It's really active threat investigations, so going after and looking at future threats and tactics and techniques that a bad actor would utilize against the system. So it's really being proactive, moving forward.

It's continuing to support the threat analysis programs such as the CRISP program where we are actively looking at indicators and looking at sharing of information, whether it's an indicator that's discovered by industry or by the Federal Government and allowing that to be shared with industry as quickly as possible. And then it's really getting to the point that we can get to machine-to-machine sharing and we can get proactive whether it's with artificial intelligence, whether it's with other capabilities.

But it's very—I would say going from the current understanding mode to more of a proactive mode are the areas that we want to move forward on.

Mr. JOHNSON. One of the things that—when I was on active duty in the Air Force even as far back as the mid-'90s as the world began to be interconnected and we started talking about things like network-centric warfare and the digital age and what that meant to national security, risk management and risk assessment began to be pushed down in the Department of Defense as part of our overall culture. So it's one thing to have our leaders talking about it.

I know I am over my time. Can you give us 30 seconds on what you're doing to make risk assessment and risk management where cybersecurity is part of the culture in DOE?

Ms. HOFFMAN. Just really quick—we have a risk management tool that we've provided and work with industry on. We have a cyber capabilities maturity model, which is also a risk assessment tool.

The industry is looking at the NIST risk assessment capabilities. So that is being filtered down. But it is a continual process that we want to show in advance. And so there are tools and best practices that the legislation has recognized and it's very important—a success in industry for advancing those capabilities.

Mr. JOHNSON. OK. Well, thank you very much.

Mr. Chairman, thanks for the indulgence and I yield back.

Mr. UPTON. Mr. Long.

Mr. LONG. Thank you, Mr. Chairman, and Mr. Menezes, when you opened this morning you mentioned I believe that the cyber threat from the bad actors, sometimes it boils down to their artificial intelligence attacking our systems and our defense is our artificial intelligence trying to prevent their artificial—can you speak to that for just 30 seconds and, that's a——

Mr. MENEZES. I will let——

Mr. LONG [continuing]. Can of very severe worms, I think.

Mr. MENEZES. I will let Ms. Hoffman answer that one.

Ms. HOFFMAN. So when we talk about cybersecurity, it's really looking at information, technology, and control system technology. But a lot of it is layering computer protections against computer attacks and computer protections, and so you keep layering on different information technology solutions to thwart information-based attacks on the system.

So it becomes an information and a controlled system but a capability of an actor to use that information technology against the industry and so it becomes a very broad attack surface. And so what we need to do is think about what is the right information tech-

nology placement in industry that provides the capability industry requires but doesn't provide that broader attack surface.

Mr. LONG. Kind of reminds me of a friend of mine 40 years ago that had a restaurant and he said that he laid awake half the night trying to figure out how to keep his employees from stealing from him. But the problem was that his employees laid awake the other half of the night trying to circumvent his new system.

So, Mr. Menezes, as we live in an increasingly digitized world with the ever-growing threat of cybersecurity attacks, I think it would be important for the Department of Energy to identify the greatest security risk in order to mitigate potential damage.

How does the Department of Energy prioritize any security risk and how are you working with private energy asset owners to plan for the possibility of cyberattacks?

Mr. MENEZES. Well, our priorities are typically a result of what we are seeing and what we are anticipating. So it's in real time because information that we gathered—both you and Congressman Johnson mentioned the digitalization of our systems and, indeed, we are producing not only more data but more access points as all of our systems become more digitized.

So when we prioritize those things that we are addressing, obviously we have to address those threats that we know as those threats are evolving. That's the first thing. We have to continue everything we've done in the past because they can always revert to prior technology, so we can't ignore that. We build on what we know and then we try to anticipate where we think the next threats are coming from. So we have to make sure that we can respond to what we know and we have to be able to identify those threats.

As I mentioned earlier, we have a lot of hits on our systems. They could appear random. Because of our modeling techniques it could be that we are witnessing new ways that they are trying to figure out ways to gain access to the system.

So we need to make sure that we have that priority in place so we can almost see into the future, if you will, to make our current system resilient to those threats.

Mr. LONG. OK. And you also talk a lot in your testimony about the Department of Energy working with the Department of Homeland Security, Department of Justice, and the FBI on energy sector cybersecurity.

As the sector-specific agency for cybersecurity in the energy sector, what is the Department of Energy's role during a potential cyberattack on the energy infrastructure?

Mr. MENEZES. I will defer to Pat.

Ms. HOFFMAN. So in the event of a cyberattack, first of all, we coordinate very closely with industry in looking at what is happening on the system.

We coordinate the primary function through the National Cybersecurity and Communications Integration Center—the NCCIC at DHS, which is the focal point for cyber coordination in the Federal Government. So we will work with them. We will work with the FBI as well.

We will look at the capabilities that industry has for dealing with this attack, trying to understand what is the root cause of the at-

tack but then also work with industry on providing mitigation measures and any support that's needed.

We would utilize NERC and the ISAC for getting information out to the rest of industry from a prevention and preparedness point of view and that capability is very strong and used, is aware across all the sectors of the industry to pay attention.

Mr. LONG. OK. Thank you.

I have run out of time so, Mr. Chairman, I yield back.

Mr. UPTON. Mr. Walberg.

Mr. WALBERG. Thank you, Mr. Chairman, and thank you for highlighting my legislation, H.R. 5174, as part of this hearing, and I appreciate the panel being here, Mr. Menezes and Ms. Hoffman, and your attention to these concerns.

Back when the Department of Energy was organized as a Cabinet agency back when I was in graduate school in 1977, the largest energy security concern was fuel supply disruptions, not electricity disruptions or cybersecurity, as we are talking about now. As you would expect, the department's Organization Act reflected those concerns. Times have changed and we should be thinking differently now about energy security and emergency preparedness. So I am glad we are doing that here today.

Mr. Menezes, the secretary's efforts to elevate the agency's leadership on emergency and cybersecurity functions are commendable. But I would like to see DOE leadership continue under future administrations. It can't be catch as catch can. We need that continuity.

Do you think it would help to codify DOE's assistant secretary functions into DOE Organization Act?

Mr. MENEZES. Well, thank you for that question, Congressman, and let me take a minute to express our appreciation for working with the committee and its efforts to review our DOE structure and its authorizing statutes.

Your staff and other members work in a very collaborative way to try to identify ways as we seek to realign and modernize the department that you seek to modernize the enabling statutes.

So we support the effort. We appreciate the collaboration and exchange of information and we continue to look forward with you as you move legislation through the process.

Mr. WALBERG. In H.R. 5174, we specify functions to include emergency planning coordination response. Can you talk about your work to elevate these functions in the new office?

Mr. MENEZES. Right. Well, and the secretary announced the setting up of CESER. That is a clear demonstration of his commitment and his organizational vision for the department, to highlight it, to increase the visibility, to coordinate efforts, and to be a source of additional guidance from Congress, the White House, and other agencies. So he's committed to that and he's showing it in a very real and measurable way.

So that's what we are proposing and that's what we are doing. And then we look forward to working with you, the appropriators, others, to ensure that it has the adequate resources it needs to accomplish the goals that we hope it accomplishes.

Mr. WALBERG. Ms. Hoffman.

Ms. HOFFMAN. I would just like to add to what the undersecretary said, that any sort of event that occurs the effective response really is built off of information sharing and coordination.

So in the preparedness when we are conducting exercises, when we are sharing classified threat briefings, when we are coordinating with the intelligence community, it's all critical components of how we support preparedness and so that we are actively coordinating ahead of any event that may occur and that will allow the Federal Government and industry to be very efficient in making sure that we understand the root causes but also the opportunities for mitigations and restoration.

Mr. WALBERG. Good. So, clearly, you will work with us to identify any gaps with—of authority or ambiguities—maybe I should have left that word out—in the system so we can make sure it continues to work.

Mr. MENEZES. Yes, sir.

Mr. WALBERG. Let me ask one more question, Mr. Menezes. Do you believe that elevating cybersecurity functions to a Senate-confirmed assistant secretary level will help intergovernmental and interagency communication as well as multidirectional information sharing with DOE's ability to appropriately and quickly address cyber-related emergencies?

Mr. MENEZES. I do. The key part about being a Senate-confirmed appointee is the accountability that you have to maintain with the two branches of government. You're in the executive branch and you're confirmed by the Senate, and so it forces you to work with Congress and to fully explain yourself to the executive branch.

Secondly, it increases the visibility and the accountability. So as of today, we come up here regularly to testify and so it's a way that we can ensure that we are doing what we said we were going to do and we are doing what you think that we told you that we were going to do, and you can give us instructions as to how we can better do what we need to do.

Mr. WALBERG. Thank you, and you can review the acronyms too, as you come up.

I yield back.

Mr. UPTON. Mr. Duncan.

Mr. DUNCAN. Mr. Chairman, thank you. You saved the best for last, I guess. Maybe.

There's been a lot of talk today about electromagnetic pulse and grid hardening. YSolar flares, coronal mass ejections, CMEs, resulting geomagnetic storm effects are real.

So EMPs could be manmade and be a natural event, and we sort of discount the natural event but just did a little research—1989 we had a huge CME event that knocked out power to 6 million people in northeastern Canada, and we just missed another one this year in 2017 where a huge solar flare happened and the Earth just was not in its path, thank goodness, and thank God we weren't.

But we are not immune to that happening in the future. So too many times when we talk about EMPs, people look at us like we have on a tinfoil hat—that we are talking about some rogue state possibly launching a nuclear weapon in to the atmosphere above the Earth and creating an EMP and knocking out our power grid.

That's a real possibility too when rogue states have nuclear weapons.

So whether it's a natural EMP or whether it's manmade, we've got to be prepared for it and one thing that I talk about a lot in this committee is my alma mater, Clemson University, and they partner with the Savannah River National Laboratory—DOE, regional utilities, and stakeholders to develop the Nation's largest grid emulator, the 20 MVA Duke Energy e-grid and are working on the next phase, a high-voltage transmission scale user facility that can be used to test large-power transformers and other critical transmission assets to develop protection schemes from both cyber and EMP attacks.

It's a prime example of enhancing grid security through public-private partnerships, which is the title of one of the bills we are reviewing today. So I encourage DOE to continue looking for these opportunities, especially since the new Office of Cybersecurity, Energy Security, and Emergency Response. I guess you're going to pronounce that as CESER. Everything in government has an acronym, right?

Can you further discuss what CESER's plans to harden the grid and protect the EMPs are? Either one.

Ms. HOFFMAN. So thank you for the question.

As you are well aware, the department takes an all-hazard approach. So we are looking at a multitude of threats that face the electric grid and the energy industry.

The national laboratories have important testing capabilities. You mentioned one of them. There are several capabilities that we are utilizing from an EMP perspective. We have partnered with the industry in looking at an EMP strategy. We have also worked with EPRI as they're looking at their mitigation and testing plan. We are looking at what the department can do to support EMP testing. As you know, it's a very expensive process to do EMP testing.

Mr. DUNCAN. You mentioned the cost but were you familiar with what Clemson is doing, before today?

Ms. HOFFMAN. Yes, I am familiar with Clemson several other activities in the labs.

Mr. DUNCAN. Have you visited the research facility in Charleston, South Carolina, or has anybody from DOE done that?

Ms. HOFFMAN. I don't know if I've visited that facility but I've visited the——

Mr. DUNCAN. Can I invite you on behalf of my alma mater to visit the drivetrain and test facility in Charleston, South Carolina?

Ms. HOFFMAN. Yes, sir.

Mr. DUNCAN. Both of you?

Mr. MENEZES. Yes, sir.

Mr. DUNCAN. OK.

Let me shift gears real quick. President Trump has talked about a huge infrastructure package and we are talking about within Congress and I guess TNI is working on this package.

When people think about infrastructure they think about roads, bridges, water, sewer, airports, port deepening, et cetera. But grid hardening and our transmission of power supplies, so talking about—I think Morgan Griffith talked about natural gas pipelines and other things. But are elements within DOE, discussing with

the White House and members of Congress, specifically probably TNI Committee—transportation and infrastructure—plans to include grid hardening and cybersecurity as part of the infrastructure package or elements within the DOE having those conversations?

Mr. MENEZES. Well, thank you for the question and pointing out the importance of the issue and the opportunities to work with everyone who's working on the infrastructure bill and who will be working on the infrastructure bill.

To be sure, a resilient strong operating energy system relies on infrastructure and so those component parts should be part of an infrastructure bill to the extent that it's necessary.

The secretary, in fact, is testifying today in the Senate—in the other body, excuse me.

Mr. DUNCAN. On this subject?

Mr. MENEZES. On the other body—on the President's infrastructure bill. And so——

Mr. DUNCAN. So let me just—because my time is running out——

Mr. MENEZES. So energy is a——

Mr. DUNCAN [continuing]. Is this a priority for the White House with regard to an infrastructure package—grid hardening and cyber security as part of the infrastructure package and should it be?

Mr. MENEZES. I know that energy components are a part. I am not sure if the phrase hardening would be in——

Mr. DUNCAN. Let me encourage you to go back to Secretary Perry and go back to your bosses and others in the White House you have conversations with and let's make this a priority in the upcoming infrastructure package.

But I can tell you it's going to be a priority of a number of people here in Congress.

Mr. Chairman, I appreciate it. With that, I yield back.

Mr. WALBERG [presiding]. I thank the gentleman. Seeing that there are no further members wishing to——

Mr. RUSH. Mr. Chairman. Mr. Chairman.

Mr. WALBERG. Mr. Rush.

Mr. RUSH. Before we adjourn, I want to ask unanimous consent to allow me to ask the Under Secretary a couple of questions.

Mr. WALBERG. Without objection.

Mr. RUSH. Mr. Secretary, I understand that the Secretary will be appearing before the committee in the near future to discuss the Department's fiscal year 2019 budget request.

The Department routinely provides detailed budget justification to Congress. But a number of the detailed buy-ins of the fiscal year 2019 request are not available. Does the Department plan to release Volumes II, III, V, and VI prior to the Secretary's appearance before the committee?

Mr. MENEZES. We plan to release it when it's complete. Yes, sir.

Mr. RUSH. Thank you, Mr. Chairman.

Mr. WALBERG. I thank the gentleman.

Again, seeing that there are no further members wishing to ask questions, I would like to thank the panel for being with us today and providing us the answers and probably further questions that we'll have down the road.

Mr. MENEZES. Happy to answer any questions for the record. Thank you.

Mr. WALBERG. Thank you, sir.

We'll change panels here now, and move on with the continuation of the hearing.

[Pause.]

We appreciate the quick changeover here and we want to thank all of our witnesses for being here today and taking the time to testify before our subcommittee.

Today's witnesses will have the opportunity to give opening statements followed by a round of questions from members.

Our second witness panel for today's hearing includes Tristan Vance, Director—Chief Energy Officer, Indiana Office of Energy Development—welcome; Zachary Tudor, Associate Laboratory Director for National and Homeland Security Idaho National Laboratory—welcome; Mark Engel, Senior Enterprise Security Advisor, Dominion Energy—welcome to you; Kyle Pitsor, Vice President, Government Relations, National Electrical Manufacturers Association—welcome you; and Scott Aaronson, Vice President, Security and Preparedness, Edison Electric Institute. Welcome.

We appreciate you all being here today. We'll begin the panel with Mr. Tristan Vance, and you are now recognized for 5 minutes to give an opening statement and I am sure you're well aware of the lighting format.

Welcome. We recognize you.

STATEMENTS OF TRISTAN VANCE, DIRECTOR, CHIEF ENERGY OFFICER, INDIANA OFFICE OF ENERGY DEVELOPMENT; ZACHARY TUDOR, ASSOCIATE LABORATORY DIRECTOR FOR NATIONAL AND HOMELAND SECURITY, IDAHO NATIONAL LABORATORY; MARK ENGELS, SENIOR ENTERPRISE SECURITY ADVISOR, DOMINION ENERGY; KYLE PITSOR, VICE PRESIDENT, GOVERNMENT RELATIONS, NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION; SCOTT AARONSON, VICE PRESIDENT, SECURITY AND PREPAREDNESS, EDISON ELECTRIC INSTITUTE

STATEMENT OF TRISTAN VANCE

Mr. VANCE. Thank you. Thank you, Mr. Chairman, Ranking Member Rush, and members of the subcommittee.

I am Tristan Vance, the Director of the Indiana Office of Energy Development. I also serve as the Chief Energy Officer for the State of Indiana and I am testifying on behalf of the National Association of State Energy Officials—NASEO.

Our testimony is in support of H.R. 5174, the Energy Emergency Leadership Act; H.R. 5175, Pipeline and LNG Facilities cybersecurity Preparedness Act; H.R. 5239, the Cyber Sense Act; and H.R. 5240, the Enhancing Grid Security Through Public-Private Partnership Act.

We appreciate the subcommittee's actions on energy emergency preparedness as demonstrated by the passage of H.R. 3050, which reauthorized appropriations for the U.S. State Energy Program—SEP—and strengthened its emergency and cybersecurity provisions.

Mr. Chairman, Ranking Member Rush, Full Committee Chairman Walden, Ranking Member Pallone, and the original sponsor of the SEP legislation and sponsors of the Dear Colleague letter calling for $70 million for the SEP program, Mr. Tonko and Mr. McKinley, you all deserve special praise for your leadership.

My state energy director colleagues from across the country visited Washington, D.C. in February and strongly encouraged many of your Senate colleagues to act on H.R. 3050.

First, NASEO would like to note the U.S. Department of Energy's exceptional response to last year's hurricanes. The support for energy emergency response from DOE combined with SEP resources, collaboration among states, tribal, and local governments and industry worked to save lives and lessen economic losses.

In particular, the electric and petroleum industries' efforts to restore services were exceptional. Secretary Perry's call for the cybersecurity, Energy Security, and Emergency Response Office, or CESER, would further improve both States' and the Nation's ability to respond to and mitigate the risks of energy supply disruption from all hazards.

NASEO's 2017 bipartisan recommendation to the Trump administration called for such action. In my capacity as a NASEO board member, I co-chaired the NASEO transition task force, which developed this important recommendation. We believe such action will save lives and protect the economy of communities in every region of the country.

The Energy Emergency Leadership Act will elevate this core DOE function and we strongly support the bill. I also want to stress the importance of CESER having a well-defined state energy security program and robust program management resources. A strong DOE state energy emergency partnership such as the one that exists today in the DOE Office of Infrastructure Security and Energy Restoration is critical to respond to emergencies effectively.

Joint state-federal coordination and data sharing is the heart of emergency response. In Indiana, for example, the propane crisis in 2014 needed a rapid response and government's ability to connect stakeholders from three sources in order to keep Hoosiers safe and protect our local economy from potentially devastating poultry industry losses.

While our Nation has not faced a cybersecurity event with significant energy supply impacts, we should adopt the lessons learned from recent natural disasters for our cyber preparedness. We share the subcommittee's concerns and the threat cybersecurity presents to the energy system—electricity, natural gas, and petroleum.

A cyberattack to the energy system during a natural disaster is a horrific scenario. However, we must address such possibilities. For example, the DOE–NASEO–NARUC Liberty Eclipse emergency exercise in 2016 focused on a combined cyber and natural disaster event. These low-cost regional exercises are essential.

We also strongly support H.R. 5239 and H.R. 5240 and believe States can leverage these activities. They build upon the work of utilities, DOE, and the States. For example, in Indiana we created the Indiana Executive Council on Cybersecurity to lead a public-

private partnership and have created a State-led exercise series focused on SCADA systems for electric and water utilities.

Equally important is mitigating energy system risks. For example, states using public-private partnerships such as energy savings performance contracting to upgrade energy systems at mission critical facilities and we are working with DOE's Clean Cities program to add natural gas, propane, and electric vehicles in first responder fleets to enhance resiliency.

NASEO believes the four bills discussed today are a significant step forward on an urgent nonpartisan national security issue. We greatly appreciate the subcommittee's continued leadership on these issues.

Thank you.

[The prepared statement of Mr. Vance follows:]

TESTIMONY OF TRISTAN VANCE, DIRECTOR,

INDIANA OFFICE OF ENERGY DEVELOPMENT;

CHIEF ENERGY OFFICER OF INDIANA, BEFORE

THE U.S. HOUSE ENERGY SUBCOMMITTEE OF THE

COMMITTEE ON ENERGY AND COMMERCE IN SUPPORT OF

LEGISLATION ADDRESSING CYBERSECURITY AND

EMERGENCY PREPAREDNESS

MARCH 14, 2018

**TESTIMONY OF TRISTAN VANCE, DIRECTOR,
INDIANA OFFICE OF ENERGY DEVELOPMENT;
CHIEF ENERGY OFFICER OF INDIANA,
BEFORE THE U.S. HOUSE ENERGY SUBCOMMITTEE OF THE
COMMITTEE ON ENERGY AND COMMERCE IN SUPPORT OF
LEGISLATION ADDRESSING CYBERSECURITY AND
EMERGENCY PREPAREDNESS**

March 14, 2018

Chairman Upton, Ranking Member Rush, and members of the Subcommittee, I am Tristan Vance, Director of the Indiana Office of Energy Development and Chief Energy Officer of Indiana, and I am testifying on behalf of the National Association of State Energy Officials (NASEO) and our 56 governor-designated state and territory energy official members. NASEO submits this testimony in strong support of the two energy security bills and two discussion drafts being considered at today's hearing, including, H.R. 5174, Energy Emergency Leadership Act; H.R. 5175, Pipeline and LNG Facility Cybersecurity Preparedness Act; Discussion Draft Cyber Sense Act; and Discussion Draft Enhancing Grid Security through Public-Private Partnerships Act.

We appreciate the Subcommittee's interest in and actions on the important issue of energy emergency planning, response, and risk mitigation, which was demonstrated with the passage of H.R. 3050 last year. We continue to encourage your colleagues in the U.S. Senate to act on H.R. 3050. The strengthening of state-federal cooperation on energy emergency preparedness and response through the reauthorization of appropriations for the U.S. State Energy Program and the enhanced emergency provisions contained in H.R. 3050 would significantly improve our states' and the nation's energy-related cybersecurity defenses and energy system resilience. The leadership demonstrated on both sides of the aisle on this non-partisan issue is greatly appreciated. Chairman Upton, Ranking Member Rush, Full Committee Chairman Walden,

Ranking Member Pallone, and the original sponsors of the U.S. State Energy Program (SEP) legislation and the sponsors of the appropriations Dear Colleague letter on the Program (calling for $70 million for SEP) Mr. Tonko and Mr. McKinley, all deserve special praise. We have encouraged your Senate colleagues to move the legislation quickly to strengthen our national security.

Before commenting on the bills, we would like to highlight the exceptional work of the U.S. Department of Energy (DOE) in responding to state, territory, and industry needs resulting from the historic hurricanes that devastated Texas, Florida, the Virgin Islands, and Puerto Rico, and impacted many other states last year. The support for state and federal emergency response from DOE's Office of Electricity Delivery and Energy Reliability, and resources from DOE's U.S. State Energy Program, along with collaboration among state energy directors and state utility commissioners, and the tireless efforts of the electricity, natural gas, propane, and petroleum industries saved lives and lessened economic losses by restoring energy services more quickly than would have otherwise been possible. DOE is making a difference and should be commended.

In that regard, Secretary Perry's call for the establishment of a new of Cybersecurity, Energy Security, and Emergency Response (CESER) office is precisely the type of action needed to modernize and improve our states' and the nation's ability to respond to and mitigate the risks of energy supply disruptions from all hazards. NASEO called for the creation of such an office in our bipartisan transition recommendations to the Trump Administration in early 2017. In my capacity as a NASEO Board Member, I co-chaired the NASEO Transition Task Force which

developed this important recommendation. We believe such action will have substantial life-saving and economic value to communities in every region of the country.

The Energy Emergency Leadership Act would elevate and make permanent this core DOE function, and NASEO strongly supports the subcommittee's action. We would also like to take this opportunity to point out the critical importance of making sure this new office has a well-defined and robust State Energy Security Program, adequate staff, and robust program management resources. Without a strong DOE-state energy emergency partnership, such as the one that exists today within the DOE Office of Electricity Delivery and Energy Reliability, the nation and our states will not be prepared to mitigate risks to our energy system and will not respond as effectively during emergencies. The state-federal partnership in cybersecurity and emergency response reflects the interdependent nature of state and federal roles and the new DOE CESER office should be constructed with that fact in mind. We urge you to emphasize the value of a strong State Energy Security program in the DOE CESER office.

The state-focused functions of the current DOE office supporting emergency preparedness and response (DOE's Infrastructure Security and Energy Restoration (ISER) program within the Office of Electricity Delivery and Energy Reliability) makes a tremendous and positive difference in the states' ability to deal with energy emergencies. Of particular value is the systematic sharing of data and analysis during an event.

Information sharing and coordination is at the heart of emergency response. In Indiana, for example, the propane crisis of 2013-14 resulted from a polar vortex and required a rapid response to protect the health and safety of Hoosiers who rely on propane for home heating. Additionally, we had to respond to serious concerns from our poultry industry, one of the largest in the nation, which faced the potential of losing an

entire generation of baby birds (for example, Indiana produces 73% of the nation's ducks for consumption). Baby chickens and ducks need external heat to keep warm, which is generally provided by propane-powered heating systems. Utilizing the state and federal governments' ability to connect key industry stakeholders with deployable resources, and provide information highlighting problem areas, we were able to keep Hoosiers safe and protect our economy from potentially devastating losses. Throughout this emergency, the need to further formalize cross-sector coordination and information sharing was strongly reinforced. We have heard similar feedback from every state that has dealt with energy emergencies over the past several years. While we have not faced a cybersecurity event with these types of impacts, adapting the lessons learned from these weather and market-related events to our cyber preparedness is essential.

We share the subcommittee's high-degree of concern about cybersecurity and its threat to the nation's energy system – electricity, natural gas, petroleum, and energy controls systems. State Energy Directors and utility commissioners are working with DOE, NASEO, and the National Association of Regulatory Utility Commissioners (NARUC) to identify areas of concern, share best practices, and improve information exchange with various energy industry sectors and state and federal agencies. Layering cyber-threats to the energy system (including retail customer interfaces) upon an unfolding natural disaster such as a hurricane, offers a horrific scenario. However, we must plan for, address, and prevent such possibilities. Enhancing regional coordination on energy emergency planning and exercises would be a valuable next step in this area.

For example, last month, NASEO, DOE, and the state emergency officials in the Southeastern United States held a joint workshop to improve state responses and coordination with industry during petroleum emergencies that could result from hurricanes and cyber-related events. Similarly, State-federal

cooperation on preparedness, such as the DOE-NASEO-NARUC led Liberty Eclipse energy emergency exercise conducted in December 2016 in Rhode Island, which focused on a combined cyber and natural disaster event, and the federal Clearpath exercises must continue. This is especially important given changes in personnel at the federal, state, and local levels, as well as the private sector. It would be particularly valuable to conduct smaller, low-cost regional exercises and workshops on a more regular basis. A holistic approach to regular regional exercises is essential as no two emergencies are ever identical.

The types of collaborative DOE-state-industry partnerships that improved emergency response during last year's hurricanes are emblematic of those envisioned in both the Discussion Draft Cyber Sense Act and Discussion Draft Enhancing Grid Security through Public-Private Partnerships Act. NASEO strongly supports both discussion drafts and sees tremendous opportunities for states to engage and leverage these voluntary activities with their local industry partners, DOE, and others. Cybersecurity is unlike the threats posed by natural disasters and can be overwhelming to manage. Energy system risks associated with hurricanes, tornados, flooding, earthquakes, and large-scale fires are better defined because of our past experiences and the known geographic scope of such events. Cyber threats have potentially far greater safety and economic impacts. They require multifaceted approaches and a recognition of the need to secure industry information technology infrastructure, as well as customer-owned systems that can serve as an entry point and become the "weak link" in an otherwise secure system. The discussion drafts take practical steps to address these issues and build upon the existing work of utilities, DOE, and the states.

In Indiana, we have created the Indiana Executive Council on Cybersecurity to lead a public-private partnership to enhance the cybersecurity of the state and its critical assets. The Council produces an overview

of Indiana's cybersecurity risks and opportunities, prioritizes those items by importance, and suggests and/or facilitates the implementation of projects designed to achieve the state's objectives. The council is tasked with creating and implementing a comprehensive cybersecurity plan addressing all potential cyber issues. The Council has over 250 advisory members from government (local, state, and federal), private-sector, military, research and development, and academic entities. These members serve across 20 industry-specific committees such as healthcare, finance, elections, and personal identifiable information in addition to the energy, water, and other common focuses of cybersecurity. The issues and solutions discussed in these industry-focused committees can be brought before the entire council in order to implement cross-sector response.

In addition to the Executive Council on Cybersecurity, Indiana has also started a Critical Exercise ("Crit-Ex") series. This is a state-led initiative that has both a table-top exercise and a real-world simulation to test for the penetration on a Supervisory Control and Data Acquisition ("SCADA") system of electric and water utilities. Beginning in 2016 with two federal agencies, eight state agencies, and 15 private sector organizations, the purpose is to determine government expertise on responding to cyber events, identify systemic weaknesses, determine how to protect and curtail further loss of data and functions after an intrusion, and to build partnerships between public sector agencies and the private sector.

Another innovative step to address cybersecurity in the energy sector is workforce development. Ensuring that we encourage college students to hone computer science skills and apply them to the energy sector is one way of improving our nation's security. Recently, DOE took steps to support such action through a cybersecurity contest which both engaged students in the challenges of protecting our energy infrastructure and brought together energy firms that might employ these students when they graduate. The proposed,

voluntary Cyber Sense program is likewise a practical step forward in working with the utility industry and others to continually improve our attention to thwarting cyber threats and vulnerabilities.

Equally important to our emergency response and cybersecurity activities is mitigating energy system risks in key end-use sectors. For example, many states are utilizing Energy Savings Performance Contracting and other public- private partnership infrastructure modernization approaches to upgrade energy systems at mission critical facilities and places of shelter, such as schools, police and fire stations, hospitals, assisted living facilities, fresh water and wastewater facilities, and universities, and to expand access to natural gas in underserved areas. Using cost-effective energy efficiency upgrades, on-site power options such as combined heat and power, micro-grids and distributed generation, and energy storage, as well as transmission and distribution system hardening, we have the opportunity to significantly drive down the risks to our energy system and lessen the impact of significant energy outages resulting from physical and cyber events.

Similarly, states are working with DOE's Clean Cities program to integrate natural gas, propane, and electric vehicles as a part of first responder and critical services fleets to enhance resiliency. This transportation-energy resilience initiative, called iREV, is an innovative way to reduce risk using existing funds and private sector innovation. These types of risk reduction strategies were pioneered by the State Energy Offices, DOE, utilities, and the energy industry. This is an area where modest federal support can unlock private investment.

Historic weather and non-weather energy supply disruption events such as Super Storm Sandy in 2012, the propane crisis in the winter of 2013-2014, three Colonial Pipeline events of 2016, and last year's devastating hurricanes and wild fires all required state-federal-industry mobilization to lessen the serious life, health, and economic impacts on citizens across entire regions of the

nation. During such serious energy emergencies, neither the Federal Government, nor state governments, nor the private sector can resolve these situations alone. Federal and state legal and operational authorities associated with energy emergency response require coordinated and clearly delineated actions to minimize threats to public health and safety, and to restore communities to normal economic activity.

The federal emergency response architecture established by Congress and carried out by the U.S. Department of Homeland Security with other federal agencies recognizes the critical need for direct engagement among federal, state, and local authorities in each infrastructure sector. DOE's federal leadership on Emergency Support Function 12 – Energy (ESF12) combined with state energy office and utility commission ESF12 leadership at the state level are key to addressing all threats and all hazards, improving the resilience of our mission critical facilities, and quickening the pace of energy system restoration.

NASEO sees the four bills being discussed today as a significant step forward on an urgent, non-partisan national security issue. These are problems that cannot be solved by the government or the private sector alone. We greatly appreciate the Subcommittee's continued leadership on these critical energy security issues.

Thank you for the opportunity to testify.

Contact Information: Tristan Vance, Director, Indiana Office of Energy Development; Chief Energy Officer, State of Indiana; 1 North Capitol Avenue, Suite 900, Indianapolis, IN 46204

Testimony Summary of Tristan Vance, Director, Indiana Office of Energy Development; Chief Energy Officer, Indiana; Before the U.S. House Energy Subcommittee

Chairman Upton, Ranking Member Rush, and members of the Subcommittee, I am Tristan Vance, Director of the Indiana Office of Energy Development; Chief Energy Officer, Indiana, and I am testifying on behalf of the National Association of State Energy Officials (NASEO). Our testimony is in support of H.R. 5174, Energy Emergency Leadership Act; H.R. 5175, Pipeline and LNG Facility Cybersecurity Preparedness Act; and discussion drafts Cyber Sense Act and Enhancing Grid Security through Public-Private Partnerships Act.

We appreciate the Subcommittee's actions on energy emergency preparedness as demonstrated by the passage of H.R. 3050 reauthorizing appropriations for the U.S. State Energy Program (SEP) and strengthening its emergency and cybersecurity provisions. Chairman Upton, Ranking Member Rush, Full Committee Chairman Walden, Ranking Member Pallone, and the original sponsors of the SEP legislation and the sponsors of the *Dear Colleague* letter calling for $70 million for SEP, Mr. Tonko and Mr. McKinley, all deserve special praise. We have encouraged your Senate colleagues to act on H.R. 3050.

First, NASEO would like to note the U.S. Department of Energy's (DOE) exceptional response to last year's hurricanes. The support for state-federal emergency response from DOE, combined with SEP resources, and collaboration among states, tribal and local governments, industry, saved lives and lessened economic losses. Secretary Perry's call for the Cybersecurity, Energy Security, and Emergency Response (CESER) office would further improve the nation's ability to respond to and mitigate the risks of energy supply disruptions from all hazards. NASEO's 2017 bipartisan recommendations to the Trump Administration called for such action. The Energy Emergency Leadership Act would elevate this core DOE function, and we strongly support the bill. We also stress the importance of CESER having a well-defined State Energy Security Program and robust program management resources. Without a strong DOE-state energy emergency partnership, such as the one that exists today, we will not be prepared and will not respond to emergencies as effectively.

State-federal coordination and data sharing is at the heart of emergency response. In Indiana, for example, the propane crisis of 2013-14 required a rapid response and government's ability to connect industry stakeholders with resources to keep Hoosiers safe and protect our local economy from potentially devastating poultry industry losses. While we have not faced a cybersecurity event with these types of impacts, we should adopt these lessons learned to our cyber preparedness. As such, we share the subcommittee's cybersecurity concerns and its threat to the energy system– electricity, natural gas, petroleum, and controls systems. Layering cyber-threats to the energy system upon an unfolding natural disaster is a horrific scenario. However, we must address such possibilities. For example, the DOE-NASEO-NARUC Liberty Eclipse emergency exercise in 2016 focused on a combined cyber and natural disaster event. These low-cost regional exercises are essential.

We strongly support the Discussion Drafts Cyber Sense Act and Enhancing Grid Security through Public-Private Partnerships Act, and believe states can leverage these activities. The drafts build upon the work of utilities, DOE, and the states. For example, in Indiana, we created the Indiana Executive Council on Cybersecurity to lead public-private partnerships, and have started a state-led exercise series focused on the SCADA systems of electric and water utilities.

Equally important is mitigating energy system risks. For example, states are utilizing public-private partnerships such as Energy Savings Performance Contracting to upgrade energy systems at mission critical facilities, and we are working with DOE's Clean Cities to add natural gas, propane, and electric vehicles in first responder fleets to enhance resiliency.

NASEO believes the four bills discussed today are a significant step forward on an urgent, non-partisan national security issue. We greatly appreciate the Subcommittee's continued leadership on these issues.

Contact Information: Tristan Vance, Director, Indiana Office of Energy Development; Chief Energy Officer, State of Indiana; 1 North Capitol Avenue, Suite 900, Indianapolis, IN 46204.

Mr. WALBERG. Thank you.

I recognize Mr. Tudor for your 5 minutes of testimony.

STATEMENT OF ZACHARY TUDOR

Mr. TUDOR. Thank you, Chairman Upton, Ranking Member Rush, Mr. Walberg, and distinguished members of the committee for holding this hearing and inviting Idaho National Laboratory's testimony on the energy sector's cybersecurity and emergency response. I request that my written testimony be made part of the record.

In my role at Idaho National Laboratory, also known as INL, I lead an organization that conducts research for the cyber and physical protection of critical infrastructure with an emphasis on the energy sector.

INL has capabilities that will support the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response, or CESER, in achieving the new leadership role for critical infrastructure protection, consistent with the authorities directed in the FAST Act for assuring the energy sector's capabilities and coordination for cyber and physical protection of emergency response.

Persistent, capable, well-resourced, and highly motivated cyber adversaries are a threat to our Nation's energy sector. These adversaries continue to develop the skills, capabilities, and opportunities for potential compromise of the Nation's energy infrastructure.

The potential consequences of a sophisticated cyberattack create an imperative that Federal agencies, labs, and industries collaborate to build capabilities and develop innovations that reduce the unacceptable risks associated with a cyberattack. DOE, INL, and our other national laboratory partners are providing leadership and resources to assure that the Nation has detective capabilities to reduce these risks. These capabilities include a broad array of science and engineering programs, extensive teams of multidisciplinary national laboratory researches, unique user facilities and test beds for experimentation at scale, and a breadth of collaborative relationships with industry, universities, and Federal agencies.

With regard to reducing cyber risks, INL's Cybercore Integration Center, known as Cybercore, performs research, development, testing, and evaluation of technologies and information products to prevent, detect, and respond to cyber vulnerabilities and intrusions. When shared through public-private partnerships, these solutions create barriers to attack, mitigate the consequences of an attack, and enable rapid restoration of energy sector operations. Specific examples of technology advancement that are reducing risks include, with DOE and other agencies, INL supported the recovery and information sharing in response to the cyberattack on Ukraine's electric grid. After our post-event analysis, INL developed and is conducting unique cyber strike workshops for U.S. asset owners and operators to learn how to protect against similar attacks.

INL developed and completed a pilot study of our consequence-driven cyber-informed engineering methodology, or CCE, with Florida Power and Light. CCE leverages an organization's knowledge and experiences to engineer out the potential for the highest con-

sequence cyber events. Briefings of the study's results were shared with the Section 9 electric utility partners, congressional staffers, and government leaders. A second pilot is currently underway.

INL also is advising the National Security Council on implementing the methodology with a larger set of participants. INL is one of several national laboratories providing technical information and strategic planning guidance to assist CESER leadership to develop infrastructures, capabilities, and processes for reducing cyber and physical risk.

This includes providing principles to establish a research portfolio that delivers impactful solutions and response to cyber and all hazard threats, standards for security-informed design to engineer in cyber physical protections for future grid infrastructure and next generation energy systems, guidance on best practices for coordinating incident response with DHS and other federal and private organizations.

Some examples of INL's current partnerships that are reducing cyber risks are research collaboration with the electric industry partners at the California Energy Systems for the 21st Century Program and Lawrence Livermore National Laboratory is leading to new capabilities for machine-to-machine automated threat response.

DOE's pilot program, Cybersecurity for the Operational Technology Environment, is providing a forum for situational awareness for cyber risks among industry partners and stakeholders. Examples I described demonstrate that DOE and INL are making significant progress in reducing the risks to our energy sector. However, with the increasing capabilities of our adversaries and the increasing complexity of our energy system technologies we will not completely eliminate all risks.

Hence, INL will continue to prioritize initiatives that emphasize the advancement of protection and response capabilities that reduces risks. We do this with the understanding that the U.S. will continue to identify new requirements for technology and innovation, expect solutions through expansive organizational leadership, coordination, and integration, and prioritize funding and focus for research.

I look forward to your questions. Thank you.

[The prepared statement of Mr. Tudor follows:]

STATEMENT OF

MR. ZACHARY D. TUDOR

ASSOCIATE LABORATORY DIRECTOR

NATIONAL & HOMELAND SECURITY

IDAHO NATIONAL LABORATORY

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES

ENERGY AND COMMERCE COMMITTEE

SUBCOMMITTEE ON ENERGY

March 14, 2018

Mr. Zachary D. Tudor, Associate Laboratory Director, Idaho National Laboratory National and Homeland Security Directorate

U.S. House of Representatives Hearing to receive testimony on "DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response"

Chairman Upton, Ranking Member Rush, and distinguished members of the committee, thank you for holding this hearing and inviting Idaho National Laboratory's testimony on the Department of Energy (DOE) cybersecurity and emergency response. I greatly appreciate the opportunity to address this committee and thank the members for your commitments and legislative decisions to assure that our national energy supply is reliable, resilient and protected.

I request that my written testimony be made part of the record.

I am the associate laboratory director for National and Homeland Security at Idaho National Laboratory, also known as INL. INL is one of 17 DOE national laboratories and is DOE's lead nuclear energy laboratory. INL's mission is to conduct research, development and demonstration of solutions that will assure the advancement of nuclear energy, clean energy and critical infrastructure protection technologies – all with the objectives of assuring the energy, economic, and national security of the U.S. In my role at INL, I have the pleasure and responsibility to lead, influence and execute a broad portfolio of research programs which address the cyber and physical protection, and emergency response for critical infrastructure, with an emphasis on the Energy Sector.

In passing the Fixing America's Surface Transportation (FAST) Act in 2015, Congress provided authorities for the DOE to be the Sector-Specific Agency for cybersecurity for the Energy Sector. The impact of your actions and your priorities that called for today's hearing reflects our mutual understanding that our nation faces persistent, capable, well-resourced, and highly motivated cyber adversaries. These adversaries continue to develop the skills, technical capabilities, and opportunities for potential compromise of the equipment, systems, networks, and facilities that constitute our nation's power grid and energy infrastructure. The potentially unacceptable consequences of a sophisticated cyberattack create an imperative for us to do all we can to demonstrably reduce cyber risk.

Beyond cyber, our national grid also is challenged with the complex realities of real-time operations and the accelerated introduction of intelligent and interconnected technologies. These technologies enable: a) integration of bulk power generation with distributed renewables; b) automated management of electricity transmission and distribution systems that support our cities and rural communities; and c) network communications to balance supply and demand, and support recovery during disasters. These innovations are critical to managing a modern and resilient operational environment, yet also increase the risks to the critical control systems throughout the Energy Sector.

After two years in my leadership role with a national laboratory, I have seen first-hand the

critical capabilities DOE is providing for the nation to reduce these risks and execute as the Energy Sector-Specific Agency for protection, coordination and response. These critical capabilities include a broad array of science and engineering programs, extensive teams of multidisciplinary national laboratory researchers, unique user facilities and test beds for experimentation "at scale," and a breadth of collaborative public-private relationships with industry, universities, and federal agencies. Because of these capabilities, DOE will continue to reduce the risks for the Energy Sector and support other federal authorities when their assigned sector has high potential for significant consequences due to the Sector's dependencies upon energy systems (e.g., oil and gas pipelines, transportation fuels, dams, defense manufacturing, etc.)

INL supports the DOE in achieving the intentions of the FAST Act's legislative direction to coordinate with the Department of Homeland Security (DHS), other federal organizations, and critical electric infrastructure stakeholders in *"...providing, supporting, and facilitating technical assistance and consultation for the Energy Sector to identify vulnerabilities and help mitigate incidents..."* We do this through performing cutting-edge energy system research, developing and sharing cyber and physical threat information, and conducting cyber and physical security assessments – all with the objectives of assuring our energy security and reducing risks to our critical infrastructure.

Often, our experts work with industry to implement solutions and provide guidance in partnership with government and private stakeholders who are encountering the realities of keeping real-world systems functioning while defending against significant risks. These "eyes-on-target" experiences allow INL to prioritize better the building of capabilities and focus research on the most relevant challenges. These priorities are continuously validated and updated as a result of discussions with DOE, our research partners, and a wide range of infrastructure stakeholders. Some recent discussions included: a) Chief Information Security Officers (CISOs) and Chief Security Officers (CSOs) from the Section 9 utilities and the California Energy Systems for the 21st Century; b) cybersecurity researchers at universities such as the state of Idaho's three research universities, Texas A&M University, the University of Texas at San Antonio, the University of Tulsa, New Mexico Tech and North Carolina State University; c) peers at national laboratories such as Oak Ridge National Laboratory, Pacific Northwest National Laboratory, and Sandia National Laboratories; and d) senior government officials from DOE, Department of Defense (DoD), and DHS.

With the remainder of today's testimony, I will update you on some of the progress INL continues to make with innovations that have opportunities for immediate and sustainable impact in reducing security risks. I will highlight INL's support, synchronized with other DOE national laboratories, that will enable the success of the new DOE Office of Cybersecurity, Energy Security and Emergency Response (CESER) in achieving its mission to improve the Energy Sector's preparedness for and ability to respond to cyber and physical threats. I also will discuss examples of the partnerships and collaborations that will support the development of coordinated strategies for science and technology research and operational preparedness and response among DOE, DHS, and other stakeholders.

With regard to reducing cyber risks, I, and many of my colleagues at other national laboratories, am keenly focused on sharing threat and vulnerability information with

stakeholders by developing analytical reports and advisories that confirm the status of threats to our power grid and energy infrastructure. Through INL's Cybercore Integration Center, referred to as Cybercore, we perform research, development, testing and evaluation of technologies that can prevent, detect, and mitigate vulnerabilities and intrusions. These technologies can create barriers that minimize attack pathways, mitigate the consequences of an attack, and effectively restore functionality. Cybercore inherently differentiates itself from individual programs and specific products by focusing on holistic emphasis of integrated, engineered solutions focused on cyber-informed technologies and processes, and cyber-prepared people.

Examples of Cybercore and other relevant technology advancements that are reducing risks for energy systems include and are not limited to:

- With DOE and multiagency support, INL experts supported recovery and information sharing following the cyberattack on the electric grid in the Ukraine in 2015 and 2016. As a result of our post-event analyses and discoveries, INL developed and is conducting "Cyber Strike" Workshops for U.S. asset owners and operators to provide awareness and operations training that foster better protection of electrical utilities from similar attacks. During the next few months, with DOE Office of Electricity Delivery and Energy Reliability sponsorship, INL staff will conduct Cyber Strike Workshops for over 400 individuals who work at electrical utilities in Florida, Georgia, and California. This information-sharing effort harnesses INL's proprietary training equipment and face-to-face interactions with our leading researchers and analysts to prepare these private utilities with the tools and techniques to guard against and respond to cyber events. In the future, this outreach will include more energy system stakeholders, including organizations within the oil and gas industry. An example of the typical feedback received from an industry attendee of a Cyber Strike Workshop: *"...It really highlighted the importance of not only having a very solid cybersecurity program, but also the vigilance that is needed from employees to help prevent unwanted intrusion. Everyone said this training was very eye-opening and has changed the way they think about protecting their information in the cyber world..."*

- INL developed and completed an initial pilot study of our proprietary Consequence-driven, Cyber-informed Engineering (CCE) methodology with Florida Power and Light (FPL) through a Cooperative Research and Development Agreement (CRADA). CCE was developed to address the realization that constantly "chasing" threats and vulnerabilities, rather than getting ahead of these problems, is not sufficient to secure our critical systems. CCE is designed to assist asset owners in understanding the most effective and immediate actions they can take to eliminate the opportunity of the "worst-case" cyber-physical impacts from an attack by the most capable cyber adversaries. CCE leverages an organization's knowledge and experiences with their systems and processes to "engineer out" the potential for the highest consequence events. This study was completed to mature the methodology and demonstrate the potential value of CCE to assess vulnerabilities and implement solutions. Briefings of the study's results were shared by a team of researchers and executives from INL and FPL for the Section 9 electric utility partners, and key government leaders. These briefings included separate sessions with U.S. Senate and House of Representative staffers from the energy and

intelligence committees of the Senate, and with the DOE Office of Electricity Delivery and Energy Reliability senior official Pat Hoffman and Assistant Secretary Bruce Walker. A second pilot study of CCE is underway with a military organization, and INL is advising the National Security Council on approaches to implement CCE to a broader set of participants across the U.S.

- Over the last 12 months, INL teamed with DHS in providing technical threat analyses, mitigations, advisories, and field assessments. Hundreds of products and assessments were performed to reduce cyber risks across all 16 critical infrastructure sectors, including Energy, Water and Wastewater, Dams, Commercial Facilities, Government Facilities, Critical Manufacturing, Transportation, and Food and Agriculture. INL supported DHS in the development and advancement of an interagency Aviation Cyber Initiative (ACI) to identify and mitigate cyber vulnerabilities in the nation's aviation systems. Cybersecurity assessments with airlines, airports, and avionics manufacturers have been underway for over two years, including cooperation with the Federal Aviation Administration's Next Generation Air Transportation System (NextGen) cyber risk analysis efforts.

- INL's capabilities also are being applied to provide solutions to a broader range of physical and electromagnetic threats. Recent experimentation conducted through our Laboratory Directed Research and Development projects and DOE-sponsored exploratory science projects provides opportunities for new solutions in: a) protective armor for defending substations against high-caliber ballistic threats similar to what occurred at the Metcalf Transmission Station in California; b) high-fidelity modeling and visualization of grid response and interdependent infrastructure behavior during intermittent renewable generation and natural disasters; and c) transformer survivability during electromagnetic pulse attack or geomagnetic disturbance events.

INL is one of several national laboratories collaboratively contributing technical information and strategic planning guidance to assist DOE leadership in the early stages of developing the structure, capabilities and processes for the DOE Office of Cybersecurity, Energy Security and Emergency Response (CESER). Guidance is focused on the coordinating and integrating research, development, and incident response capabilities among the multiple programs and organizations within the DOE and other federal organizations. Examples include:

- *Providing principles for establishing a CESER RD&D portfolio that delivers impactful solutions in response to cyber and all hazard threats.* These principles can guide CESER in focusing on the development and operationalization of next-generation cyber and situational awareness tools for real-time response by leveraging the cutting-edge energy research for transmission, distribution and storage resulting from the DOE Office of Electricity Delivery and Energy Reliability Grid Modernization Laboratory Consortium.

- *Providing principles for including security-informed design into future grid infrastructure.* CESER will be able to reduce future cyber risks to energy infrastructure by coordinating and integrating "engineered-in" cyber-physical protections into future advanced energy systems (e.g., DOE Office of Nuclear Energy research on advanced reactor designs and

fuel cycle facilities; DOE Office of Energy Efficiency and Renewable Energy programs for electric vehicles connecting to the grid, etc.).

- *Providing guidance on best practices for developing processes and procedures for coordination with incident response* with the DHS U.S. Computer Emergency Readiness Team, the DHS National Cybersecurity and Communications Integration Center Hunt and Incident Response Team, U.S. Cyber Command, etc. Recent recovery efforts in Puerto Rico; responses to the Ukraine grid attack, Nuclear 17, and Palmetto Fusion; and participation in national exercises (e.g., GridEx, Liberty Eclipse, etc.) provide CESER with access to a tremendous pool of expertise to advance the realism and effectiveness of our future efforts for preparedness and response.

INL's track record of successful development and deployment of technical innovations is a result of an emphasis on collaborating, partnering, and sharing of experts and experimental facilities. This approach accelerates the maturation of technologies and methodologies from the conceptual to deployment stages; optimizes the benefits of leveraging investments in expertise, research programs, and technology development infrastructure; and creates effective environments for immediate information sharing of discoveries and emerging threats. Based upon our experiences, we included the formation of new multiorganizational partnerships as a major priority to achieve the Cybercore vision of creating the enduring national capabilities for control systems cybersecurity innovation. Examples of current partnerships that are enhancing national capabilities are:

- INL, Pacific Northwest National Laboratory, and Sandia National Laboratories comprise the three laboratory Cybercore collaboration, CyberPARC (Partnership for Advancing Resilient Controls), which is creating a collaborative environment among the labs to advance the science and engineering of cyber-physical systems to create resilient, self-healing control systems.

- In collaboration with the electric industry partners of the California Energy Systems for the 21st Century Program, INL and Lawrence Livermore National Laboratory are conducting research with machine-to-machine automated threat response (MMATR) concepts and technologies.

- Cybersecurity for the Operational Technology Environment (CYOTE), a DOE-OE pilot project supported by INL, facilitates situational awareness in operational technology (OT) networks, and information sharing and coordination among industry partners and stakeholders, while providing an adaptable forum for development and testing of scientific innovations that have potential to advance grid resilience and security.

The examples I have described demonstrate that DOE and INL are making significant progress in reducing the risks to our nation's energy infrastructure. Although we can minimize but not eliminate the risk, we must redouble our efforts in technology innovation; multiorganizational cooperation, coordination, and integration; and prioritization of funding and focus for research programs. Therefore, I emphasize that based on our current understanding of the threats to our Energy Sector infrastructure, we must aggressively continue to pursue programs to assure our energy, economic and national security. I thank the committee

members for this opportunity to discuss national cybersecurity challenges and to share the burden in creating a path forward that protects the U.S. Thank you.

Mr. WALBERG. Thank you.
Mr. Engels, you're recognized.

STATEMENT OF MARK ENGELS

Mr. ENGELS. Mr. Chairman, Ranking Member Rush, and members of the subcommittee, thank you for the opportunity to testify.

My name is Mark Engels and I am a Senior Enterprise Security Advisor at Dominion Energy. Dominion Energy is one of the largest producers and transporters of energy with a portfolio of approximately 26,200 megawatts of electricity generation, 6,600 miles of electric and transmission and distribution lines, 15,000 miles of natural gas pipeline, and the Cove Point liquefied natural gas facility in Maryland. We operate one of the largest natural gas storage systems in the U.S. with one trillion cubic feet of capacity and serve more than 6 million utility and retail customers.

I've been with Dominion Energy almost 40 years and with a focus on cybersecurity for 19 of those years. As a representative from Dominion Energy, I appreciate the opportunity to provide comments and input to this committee and applaud the committee's focus to advance public-private partnership between the Department of Energy and the oil and natural gas sector.

For Homeland Security Presidential Directive 7, both the Department of Energy, the Department of Homeland Security in coordination with the Department of Transportation function as the sector-specific agencies for natural gas pipelines and LNG. The fact that pipelines have two SSAs comprised of three different federal agencies cannot be understated, especially when it comes to interagency coordination in advance of, during, and post-incident operations. The key to this coordination is maintaining a productive relationships between the energy government coordination councils' two co-chairs—DOE and DHS—and the oil and natural gas sector coordinating council.

The ONGSCC is comprised of owners and operators from 20-plus industry trade associations representing all aspects of the oil and natural gas sector. I encourage DOE and TSA, who has regulatory authority for pipeline security, to develop a memo of understanding that outlines roles and responsibilities for dealing with cyber and physical security of natural gas pipelines and LNG. TSA already has an MOU with the Department of Transportation's Pipeline and Hazardous Materials Safety Administration, or PHMSA, which has responsibility for pipeline safety.

The recent announcement of DOE's new Office of Cybersecurity, Energy Security, and Emergency Response should continue to improve the coordination for pipeline, cyber, and physical security.

The language in H.R. 5175 Section 22 could introduce complexity and confusion when it comes to DOE's involvements with States. Individual pipeline companies, Dominion Energy included, already have longstanding relationships with state emergency response organizations, public utility commissions, and law enforcement for all hazard events. H.R. 5175 directs DOE to focus on advanced cybersecurity applications, pilot demonstrations, develop workforce curricula, and provide mechanisms to help the energy sector evaluate, prioritize, and improve physical and cybersecurity capabilities.

Dominion Energy has worked with DOE and several national labs on a number of efforts that align with the proposed legislation. They include being a peer reviewer for the Department of Energy's Cybersecurity for Energy Delivery Systems Program, participation in workforce and training efforts, Cyber Strike—a hands-on workshop communicating lessons learned associated with the Ukraine grid attacks—and Attack, an approached developed by INL to aggregate and evaluate cyber risk-related information.

Dominion Energy is a member of both the downstream natural gas and electricity information sharing and analysis centers, both of which have benefited from intelligence provided by DOE's Cybersecurity Risk Information Sharing Program, or CRISP. Dominion Energy and other natural gas pipeline companies have worked very closely with TSA and DOE on cyber and physical security to build a partnership based on trust and respect.

The proposed legislation should make sure that roles and responsibilities are clearly defined and understandable by pipeline operators who ultimately have to face the growing threat every day.

Thank you again for the opportunity to provide comments and I will be glad to answer any of your questions.

[The prepared statement of Mr. Engels follows:]

Testimony of

Mark A. Engels

Senior Enterprise Security Advisor

Dominion Energy

Committee on Energy and Commerce

Energy Subcommittee

U.S. House of Representatives

"DOE Modernization: Legislation Addressing

Cybersecurity and Emergency Response"

March 14, 2018

Testimony Summary

Input to HR 5174, the "Energy Emergency Leadership Act", and HR 5175, the "Pipeline and LNG Facility Cybersecurity Preparedness Act".

- **HR 5175 Section 2(1) – Policies and Procedures and HR 5174 Section 2 – Functions Assigned to Assistant Secretaries**

  DOE is the SSA for the natural gas commodity, and DHS (in coordination with DOT) is the SSA for the pipeline infrastructure. The fact that natural gas pipelines have two SSAs, comprised of three Federal agencies, (DOE, DHS, and DOT) cannot be understated, especially when it comes to interagency-coordination – in advance of, during, and post-incident operations.

  The key to this coordination is maintaining a productive relationship between the Energy Government Coordinating Council (EGCC), which is co-chaired by DOE's Office of Electricity Delivery and Energy Reliability (OE) and the DHS National Protection and Programs Directorate (NPPD), and the Oil and Natural Gas Sector Coordinating Council (ONGSCC).

  While natural gas pipeline operators have a general idea about how the relevant Federal agencies associated with pipeline security should work together, HR 5175 would ideally encourage clarification on this issue. In HR 5174, Energy Emergency Leadership Act, the addition of paragraph 12 in the Department of Energy Organization Act, provides clarity and direction as well.

A more expedient approach may be to encourage a Memo of Understanding (MOU) between DOE and TSA that outlines roles and responsibilities for dealing with cyber and physical security for the ONG sector. TSA already has an MOU with the DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) which has responsibility for pipeline safety. Depending on the type of event, the TSA/DOT MOU has been critical in helping operators understand which Federal entity is the lead agency.

- **HR 5175 Section 2(2) – Coordinate Response and Recovery**

  The language in HR 5175 referencing DOE's coordination with States may actually add complexity to a system that already has structure. Individual pipeline companies, Dominion Energy included, have longstanding relationships with State emergency response organizations, public utility commissions and law enforcement for all hazard events, such as weather. Having DOE attempt to coordinate cyber and physical security for pipelines that could include all 50 States may not result in the value intended. This is particularly true for natural gas response and recovery, which is organized around time-tested local and regional coordination.

- **HR 5175 Section 2(3) – Develop Advanced Cybersecurity Applications**

  HR 5175 should ensure adequate resources and funding to continue efforts like the Department of Energy's Cybersecurity for Energy Delivery Systems (CEDS) as well as hardware and software testing via national labs test-beds. Through these programs vendors, academia, labs and industry get involved and ultimately benefits arise from commercialization of products that meet industry requirements.

- **HR 5175 Section 2(4) – Perform Pilot Demonstrations**

  This section is complementary to Section 2(3) but goes further by directing actual demonstrations of technology.

  Asset owners should be involved in the development of testing criteria to ensure the pilot represents, as close as possible, the real world environment in which the technology is intended to operate.

- **HR 5175 Section 2(5) – Develop Workforce Curricula**

  HR 5175 should encourage more training and workforce development similar to *Cyber Strike,* a hands-on workshop sponsored by the Department of Energy and *ATAC,* a methodical approach, develop by Idaho National Laboratory, to aggregate and evaluate cyber-risk related information. Both have proven beneficial to Dominion Energy.

- **HR 5175 Section 2(6) – Provide Mechanisms to Help Evaluate, Prioritize and Improve**

  The Department of Energy's Cybersecurity Risk Information Sharing Program (CRISP) leverages both classified and unclassified signatures to pinpoint activity unique to the Electricity and Oil and Natural Gas (ONG) entities. Any method or approach that encourages more natural gas industry participation would be beneficial to the entire Energy sector.

Testimony

Introduction and Background. Chairman Upton, Ranking Member Rush and members of the Subcommittee, thank you for the opportunity to testify. My name is Mark A. Engels and I'm a Senior Enterprise Security Advisor at Dominion Energy.

Dominion Energy is one of the nation's largest producers and transporters of energy, with a portfolio of approximately 26,200 megawatts of electric generation, 15,000 miles of natural gas transmission, gathering, storage and distribution pipelines and 6,600 miles of electric transmission and distribution lines. We operate the Cove Point liquefied natural gas (LNG) facility in Maryland, one of the largest natural gas storage systems in the U.S. with 1 trillion cubic feet of capacity, and serve more than 6 million utility and retail energy customers.

I have been with Dominion Energy almost 40 years with a focus on cybersecurity for 19 of those years. I'm an active member of the American Gas Association's (AGA) Cybersecurity Strategy Task Force and Natural Gas Security Committee; the Interstate Natural Gas Association of America's (INGAA) cyber and physical security committee; the Edison Electric Institute's (EEI) Security Committee; the Department of Homeland Security's (DHS) Classified Information Forum representing the Energy sector; a peer reviewer for the Department of Energy's (DOE) Cybersecurity for Energy Delivery Systems (CEDS) program; a member of the advisory team for Idaho National Laboratory's (INL) CyberCore Integration Center; and the former chair of the North American Electric Reliability Corporation's (NERC) Cyber Attack Task Force (CATF) and Attack Tree Task Force (ATTF).

On behalf of Dominion Energy, I appreciate the opportunity to provide comments and input to this Committee on HR 5174, the "Energy Emergency Leadership Act," and HR 5175, the "Pipeline and LNG Facility Cybersecurity Preparedness Act." I applaud the Committee's focus on advancing the public/private partnership between the Department of Energy and the Oil and Natural Gas sector. Neither will be successful without the other in addressing the continuous cyber and physical threats faced by our nation's pipelines .

Section 2(1) of HR 5175 directs the Department of Energy to establish policies and procedures to coordinate Federal agencies, States and the Energy sector.

Per the Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD7), DOE is designated as the "Sector-Specific Agency" (SSA) for the Energy sector, which includes production, refining, storage, and distribution of oil and gas, and electric power except for commercial nuclear power facilities. HSPD7 also designates DHS as the SSA for Transportation Systems sector, encompassing mass transit, aviation, maritime, ground/surface, and rail and pipeline systems. HSPD7 further states the Department of Transportation (DOT) and DHS will collaborate in regulating the transportation of hazardous materials by all modes (including pipelines). As the SSAs, DOE and DHS are directed to be "responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment." In the case of natural gas pipelines and LNG, both DOE and DHS (in coordination with DOT) are the SSAs; DOE is the SSA for the natural gas commodity, and DHS (in coordination with DOT) is the SSA for the

pipeline infrastructure. The fact that natural gas pipelines have two SSAs, comprised of three Federal agencies (DOE, DHS, and DOT) cannot be understated, especially when it comes to interagency-coordination – in advance of, during, and post-incident operations. This coordination and acknowledgment of existing authorities – TSA regulatory authority for pipeline security (and associated incidents) and DOT regulatory authority for pipeline safety (and associated incidents) is critical to prevent duplication of efforts and to provide clarity to the owner/operator for effective security communication and outreach to the Federal government.

Additionally, the Homeland Security Act of 2002 directs DHS to be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. DHS is designated to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources.

The key to this coordination is maintaining a productive relationship between the Energy Government Coordinating Council (EGCC), which is co-chaired by DOE's Office of Electricity Delivery and Energy Reliability (OE) and the DHS National Protection and Programs Directorate (NPPD), and the Oil and Natural Gas Sector Coordinating Council (ONGSCC). The ONGSCC is comprised of owners and operators from 20 plus industry trade associations representing all aspects of the ONG sector – drilling, exploration and production, processing, refining, services and supply, transmission, distribution and transportation (including pipelines) for liquid fuel and natural gas.

For many years, DOE's Office of Infrastructure Security and Emergency Response (ISER) has collaborated with the ONGSCC related to cyber and physical security to the mutual benefit of pipeline companies. The recent announcement of DOE's new Office of Cybersecurity, Energy Security and Emergency Response (CESER) should continue to improve the focus on pipeline cyber/physical security and coordination efforts.

A parallel relationship also exists between pipeline companies and the DHS's Transportation Security Administration (TSA). As the regulatory authority for pipeline security, TSA has demonstrated a long history of understanding pipelines and has the expertise to provide oversight to the industry.

In 2011, TSA released *Pipeline Security Guidelines*, which provide guidance on critical and non-critical pipeline asset security. The *Guidelines* were a collaborative effort of ONG asset owners, industry associations and TSA. These *Guidelines* have been the basis for cyber and physical protection implemented across the pipeline community. In 2016, TSA, again working with asset owners, industry associations, and the Department of Homeland Security's Industrial Control System's Cyber Emergency Response Team (DHS ICS-CERT), gathered input to update the *Guidelines* using the National Institute of Standards and Technology's (NIST) Cyber Security Framework as a model. The updated *Guidelines* are scheduled for release in the first half of 2018. Industry also provided input to augment the set of cybersecurity questions used in the Corporate Security Reviews (CSR) conducted by TSA.

Dominion Energy has a close working relationship with both ISER and TSA. In fact, TSA conducted a CSR of our pipeline cyber and physical security program in February, 2018. Also in attendance, at our invitation, were representatives from the General Accountability Office

(GAO), who is actively conducting their own assessment of TSA's cybersecurity capabilities. TSA identified eleven smart practices associated with our cyber and physical security program. But more importantly, they provided four recommendations that Dominion Energy will use to advance our security program. The CSR is an important part of the voluntary and collaborative partnership between TSA and industry. As a result of the partnership model, Dominion Energy has gained valuable insight from agencies with a wide view of the ONG sector.

Recommendation: While natural gas pipeline operators have a general idea about how the relevant Federal agencies associated with pipeline security should work together, HR 5175 would ideally encourage clarification on this issue. In HR 5174, Energy Emergency Leadership Act, the addition of paragraph 12 in the Department of Energy Organization Act, provides clarity and direction as well.

A more expedient approach may be to encourage a Memo of Understanding (MOU) between DOE and TSA that outlines roles and responsibilities for dealing with cyber and physical security for the ONG sector. This will immediately strengthen the relationship between these two key agencies. TSA already has an MOU with the DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) which has responsibility for pipeline safety. The TSA/DOT MOU has been critical to helping operators understand which Federal entity has the lead based on the type of incident (i.e., TSA is lead in the event of security-related incident, and PHMSA in the event of a pipeline safety incident).

Section 2(2) of HR 5175 directs the Department of Energy to coordinate response and recovery by Federal agencies, States and the Energy sector.

Dominion Energy conducts internal exercises to challenge our own staff and leaders. We recognize how important our services are to the health and safety of the public and to national security given the many critically important customers we serve. Our internal incident response plans outline how to engage with the different Federal and State agencies that we are likely to communicate with or from whom we request assistance. Dominion Energy procedures call for the ISER group to be the primary point of contact for our coordination with other Federal agencies such as the DHS, DOD and the FBI. Dominion Energy directly manages the coordination with our State partners through existing relationships.

DOE is very active in industry-led initiatives. For example, INGAA conducted a table-top exercise in April, 2017 involving a cyber and physical attack against a pipeline. Dominion Energy, along with 10 other INGAA members and staff from AGA, FERC, TSA, DOT and DOE participated. It was helpful for industry representatives to better understand the activities Federal agencies would perform during an event.

Dominion Energy also participated in NERC's bi-annual electric grid exercise (GridEX) which took place this past November. In addition, we invited our State Public Utility Commission staff and officials from the Virginia Governor's office to observe. While primarily targeting the electric grid, part of the scenario included malware attacks against natural gas pipelines and physical attacks on compressor stations serving electric generation. These injects allowed participants with natural gas assets to exercise their response plans as well as provide an opportunity for DOE to perform SSA duties for the entire Energy sector.

Dominion Energy plans to provide input to the Regional Integrated Energy Security Planning (RIESP) initiative, which was started in September 2017 by DOE, with assistance from INL and Argonne National Laboratory (ANL). By better understanding regional constructs, best practices, and data used by State governments to plan for response, DOE is looking to encourage greater regional energy security and resiliency planning by States.

Recommendation: The language in HR 5175 Section 2(2) blurs the presently clear distinction with States, actually adding complexity to a system that already has structure. Individual pipeline companies, Dominion Energy included, have longstanding relationships with State emergency response organizations, public utility commissions and law enforcement for all hazard events. Having DOE attempt to coordinate cyber and physical security for pipelines that could include all 50 States may not result in the value intended. This is particularly true for natural gas response and recovery, which is organized around time-tested local and regional coordination.

Section 2(3) of HR 5175 directs the Department of Energy to develop advanced cybersecurity applications and technologies.

In 2012, Dominion Energy was one of four utilities asked by DOE to collaborate on the development of the Cybersecurity Capability Maturity Model (C2M2). It was a great partnership example where industry guided, and DOE listened; exactly the way an effort like this should occur. The effort created a model that has been used by hundreds of electric and natural gas utilities. Dominion Energy has conducted C2M2 assessments against both our

electric and natural gas cybersecurity programs with results presented to our Board of Directors and used to drive improvements. DOE is now engaged in an effort to update the model, again leading by listening to industry for input.

Since 2012, I have been a peer reviewer for DOE's Cybersecurity for Energy Delivery Systems (CEDS) program. This effort has been incredibly important in advancing cybersecurity research and development efforts that have helped pipeline companies. CEDS resources are provided to leading vendors in the industry, academic institutions committed to advancing cybersecurity as well as DOE's national labs. By asking pipeline operators what works and what doesn't, when it comes to operational improvements, dollars are directed to initiatives that have the highest probability of being commercialized and integrated into the nation's natural gas pipeline infrastructure.

Following are two examples of CEDS initiatives that Dominion Energy has been involved with:

- One area that has proven to be a major vulnerability for industry involves Supply Chain threats. It is very difficult, if not impossible, for pipeline companies to have a level of assurance that the components and software integrated into operational infrastructure have the highest degree of integrity. INL has undertaken several initiatives to stand up test environments for Industrial Control Systems (ICS). One such initiative was called RENDER (Risk Evaluation Nexus for Digital Age Energy Reliability). RENDER created a three way sharing arrangement involving the lab, the vendor and the asset owner. Previous projects excluded the asset owner from the equation, creating uncertainty associated with remediation of the vulnerabilities identified by INL. With RENDER, the

asset owner not only could see what vulnerabilities were discovered, but provide input to the vendor about how critical or not the vulnerability was to the asset owner. This allowed the vendor to prioritize corrections that made the most sense to the asset owners.

RENDER targeted ICS used by both natural gas and electric utilities, but was only funded for an initial pilot. As a follow-up to RENDER, ISER is actively pursuing additional test-bed initiatives with multiple national labs that could assist both electric and natural gas utilities. It would not be a certification, but a more comprehensive test of key hardware and software with involvement of asset owners.

- Dominion Energy has taken advantage of DOE's Cybersecurity Procurement Language for Energy Delivery Systems. First published in 2014, the material has been used by our Supply Chain group to enhance the procurement process for our Gas Control Supervisory Control and Data Acquisition (SCADA) system.

Recommendation: HR 5175 should ensure adequate resources and funding to continue efforts like CEDS as well as test-beds for hardware and software testing. Through these programs vendors, academia, labs and industry gets involved and ultimately benefits arise from commercialization of products that meet industry requirements.

Section 2(4) of HR 5175 directs the Department of Energy to perform pilot demonstrations.

This section is complementary to Section 2(3) but goes further by directing actual demonstrations of technology.

Recommendation: Asset owners should be involved in the development of testing criteria to ensure the pilot represents, as close as possible, the real world environment the technology is intended to operate in.

Section 2(5) directs the Department of Energy to develop workforce development curricula.

One of the most effective and beneficial programs Dominion Energy staff participated in is *Cyber Strike*, a hands-on workshop, sponsored by DOE. *Cyber Strike* communicates the lessons learned from the 2015 and 2016 attacks on the Ukraine electric system. Dominion Energy staff from both our natural gas and electric SCADA teams attended workshops giving them practical experience in the type of offensive tactics and techniques they could face from an experienced adversary. Being able to learn from knowledgeable instructors is invaluable to our staff responsible for the safe and reliable operation of our control systems.

A CEDS funded INL initiative, Attack Technology and Characterization (*ATAC*), involved lab threat analysts training Dominion Energy SCADA engineering staff on a methodical approach to aggregate and evaluate cyber-risk related information.

Recommendation: HR 5175 should encourage more training and workforce development similar to *Cyber Strike* and *ATAC*, both of which have proven beneficial to Dominion Energy. To do this, DOE should involve asset owners to determine what programs work best.

Section 2(6) directs the Department of Energy to provide mechanisms to help the energy sector evaluate, prioritize and improve cyber and physical security capabilities.

Information sharing between the public and private sector is a foundational principle that helps the Oil and Natural Gas sector's efforts to address the continuously advancing threats that confront the sector. As will always be the case, there is never enough information, either classified or unclassified, and the information that is available can never be shared fast enough for industry.

The DOE OE has engaged the Energy Sector Information Sharing and Analysis Centers (ISACs), including the Oil and Natural Gas (ONG) ISAC and the Downstream Natural Gas (DNG) ISAC. Recognizing the need for improved information sharing both between industry and government and across the Energy sector, DOE convenes monthly meetings with the ONG ISAC, DNG ISAC, and Electricity ISAC (E-ISAC) to share and discuss cyber threat trends in a classified setting. Dominion Energy is a member of both the DNG-ISAC and the E-ISAC and benefits from intelligence provided by these organizations.

Dominion Energy has also participated in a pilot program, sponsored by DOE, to utilize Secure Video Teleconference (SVTC) capabilities. The purpose is to remotely convene a classified threat briefing for cleared industry representatives and reduce the amount of time it takes for actionable information to reach asset owners.

Along with approximately 30 electric utilities, Dominion Energy is part of DOE's Cybersecurity Risk Information Sharing Program (CRISP). Many of the participants have natural gas assets and automatically share information with the DOE and E-ISAC. This program leverages both classified and unclassified signatures to pinpoint activity unique to the Energy sector. The current CRISP program focuses on business networks, but efforts are also underway at INL to

provide a view into operational networks with a program called Cybersecurity for the Operational Technology Environment (CYOTE).

Recommendation: Any method or approach that encourages greater participation by ONG entities into the CRISP / CYOTE programs will have a positive impact on the entire Energy sector.

Conclusion: Dominion Energy and other natural gas pipeline companies have worked very closely with TSA and DOE on cyber and physical security to build a partnership based on trust and respect. This framework works because different organizations "stay in their swim lanes" and bring to the effort their specific area of expertise. DOE's coordination function is valuable in responding to a crisis and making available Federal resources to address the event. This support could come in the form of harnessing the considerable cybersecurity capabilities of the national labs, whose offensive and defensive threat analysts are world class, coordinating with DHS ICS-CERT for control system expertise or bringing to bear comprehensive knowledge of pipeline operations from TSA.

The proposed legislation should make sure that roles and responsibilities are clearly defined and understandable by pipeline operators who ultimately have to face the growing threat each and every day.

Thank you again for the opportunity to provide comments and input to this Subcommittee and I will be glad to answer any questions. Dominion Energy and I look forward to working with you on these important issues.

Mr. WALBERG. Thank you.
Mr. Pitsor.

STATEMENT OF KYLE PITSOR

Mr. PITSOR. Good afternoon, Mr. Chairman, Ranking Member Rush, members of the subcommittee. Thank you for the opportunity to testify on such an important topic today, the physical and cybersecurity of our Nation's electric system.

My name is Kyle Pitsor, Vice President of Government Relations for National Electrical Manufacturers Association, representing about 350 manufacturers of electrical equipment and medical imaging technologies. NEMA and our member manufacturers have made cybersecurity a top priority. As the manufacturers of essential grid equipment, NEMA companies are a key line of defence against both physical and cyberattacks in the electricity transmission and distribution system.

We understand that a secure product supply chain is inherent to a secure grid and cybersecurity aspects should be built into, not bolted onto manufacturers' products whenever possible. Manufacturers also understand that managing cybersecurity supply chain risk requires a collaborative effort and open lines of communication among electric utility companies, Federal and State and local governments, and suppliers of the full spectrum of grid systems and components, both hardware and software.

I would like to mention briefly some of the industry-wide efforts NEMA and its members have pursued to establish best practices for supply chain and manufacturer cybersecurity hygiene and then make a few comments on the Cyber Sense Act and the Enhancing Grid Security Through Public-Private Partnership Act.

In 2005, the electrical industry took a step toward improving supply chains' security of manufacturers' products by publishing a technical best practices document that laid out the steps for securing supply chains.

NEMA published a white paper on cybersecurity, supply chain best practices for manufacturers that addresses supply chain integrity through four phases of a product's life cycle: the manufacturing, delivery, operation, and end of life of a product. This month in March, NEMA members have approved a new technical document detailing industry best practice cyber hygiene principles for electrical manufacturers to implement in their manufacturing and engineering processes. The document raises a manufacturer's level of cybersecurity sophistication by following seven fundamental principles that are outlined in my statement.

With the above-mentioned two industry developed and cybersecurity best practices documents in mind, I will make a few comments about two of the bills under consideration today. First of all, with respect to the Cyber Sense Act, NEMA member manufacturers support voluntary cyber evaluation of products used in the transmission, distribution, storage, and end use of electricity. However, the specific requirements of any such program need to be carefully designed in close collaboration with manufacturers and other stakeholder groups and developed via an open and transparent process.

We recommend that any cybersecurity evaluation program abide by a set of principles that we've outlined in our written statement. With respect to the Enhancing Grid Security Through Public-Private Partnership Act, NEMA supports the concepts included in the draft legislation. With respect to Section 2, NEMA agrees that voluntary technical assistance efforts should be available to provide electric utilities with information and resources to effectively prepare for and combat both physical and cybersecurity threats.

We also agree that this technical assistance should be provided in close collaboration with State governments and public utility regulatory commissions as well as with equipment manufacturers. Including manufacturers in the training and technical assistance efforts will ensure that products are installed and maintained as intended to limit the risk of cyberattack resulting from the possible misuse of a product.

NEMA also supports the recommendations included in Sections 3 and 4 of the legislation. One additional outage index that we recommend be included in Section 4(b) of the draft legislation is the Momentary Average Interruption Frequency Index. Momentary outages cost U.S. electricity consumers over $60 billion in 2014 and account for more than half of all power outages. Inclusion of this index, we believe, will improve the interrupter cost estimate information produced by the Department of Energy.

In conclusion, NEMA and member company manufacturers recognize that cybersecurity risks are constantly evolving and changing and requires a shared responsibility by all stakeholders.

NEMA looks forward to working with you as a resource to this committee as you continue your work to address cybersecurity concerns in the energy sector.

Thank you, and I look forward to any questions.

[The prepared statement of Mr. Pitsor follows:]



TESTIMONY OF

KYLE PITSOR
VICE PRESIDENT, GOVERNMENT RELATIONS
NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

HEARING ON
DOE MODERNIZATION: LEGISLATION ADDRESSING
CYBERSECURITY AND EMERGENCY RESPONSE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON ENERGY

MARCH 14, 2018

SUMMARY OF TESTIMONY

Manufacturers are developing and following cybersecurity best practices. NEMA has published two industry-developed cybersecurity documents detailing best practices for electrical manufacturers, "NEMA CPSP 1-2015: Supply Chain Best Practices,"[1] and "NEMA CPSP 2-2018, Cyber Hygiene."[2] Government agencies should rely on industry-developed standards and documents, where available and applicable.

Government and private industry should work together to address security challenges. NEMA supports collaboration between the private sector and the Department of Energy, the National Institute of Standards and Technology, the Department of Homeland Security, and other federal and state agencies to promote cybersecurity best practices.

Electrical manufacturers support voluntary cybersecurity evaluation of products used in the transmission, distribution, storage, and end-use of electricity. Manufacturers and electricity companies should be involved in establishing the criteria for any such program via an open and transparent process.

NEMA supports the concepts included in the *Enhancing Grid Security through Public-Private Partnerships Act*. We encourage the Committee to broaden the list of outage indices in Section 4(b) to include Momentary Average Interruption Frequency Index (MAIFI), the average number of momentary power interruptions experienced by a utility customer in a given year. Momentary outages cost U.S. electricity customers $60 billion in 2014.

[1] Available online at http://www.nema.org/supply-chain-best-practices
[2] Available May 2018 at http://www.nema.org

Chairman Upton, Ranking Member Rush, and Members of the Subcommittee:

Thank you for the opportunity to testify in front of you today on such an important topic—the physical and cybersecurity of our nation's electric system.

My name is Kyle Pitsor, and I am the Vice President of Government Relations at the National Electrical Manufacturers Association (NEMA). NEMA is a trade association representing nearly 350 electrical equipment and medical imaging manufacturers that make safe, reliable, and efficient products and systems. Our combined industries account for 360,000 American jobs in more than 7,000 facilities covering every state. Our industry produces $106 billion shipments of electrical equipment and medical imaging technologies per year with $36 billion exports.

NEMA and its Member companies provide products and systems for use in several infrastructure sectors, energy being one of them. We understand that a focused effort by our manufacturers is required to support the electrical infrastructure essential to national and economic security. However, the responsibility for protecting our nation's electric grid must be shared among the private sector, end-users, and government agencies like the Department of Energy, Department of Homeland Security, and the Department of Commerce's National Institute of Standards and Technology.

NEMA and our Member manufacturers have made cybersecurity a top priority. As the manufacturers of essential grid equipment, NEMA companies are a key line of defense against both physical- and cyber-attacks on the electricity transmission and distribution system. We understand that a secure product supply chain is inherent to a secure grid, and that cybersecurity aspects should be built into, not bolted onto, manufacturers' products whenever possible. Manufacturers also understand that managing cybersecurity supply chain risk requires a

collaborative effort and open lines of communication among electric utility companies, federal, state, and local governments, and the suppliers of the full spectrum of electric grid systems and components—both hardware and software.

I would like to mention briefly some of the industry-wide efforts NEMA and its Members have pursued to establish best practices for supply chain and manufacturers' cybersecurity hygiene. I will then make a few comments on the *Cyber Sense Act* (H.R. 5239) and the *Enhancing Grid Security through Public-Private Partnerships Act* (H.R. 5240) under consideration today.

Manufacturers are developing and following best practices

NEMA, as a standards development organization, has been discussing mutually shared cybersecurity principles with our partners in the electric utility industry for almost a decade. Supply chain disruption and compromise are major concerns for the electric utility industry, and both electric utilities and manufacturers recognize that addressing these concerns requires close collaboration.

Supply Chain Security

In 2015, the electrical industry took a step toward improving the supply chain security of manufacturers' products by publishing a technical best practices document that laid out the steps for securing supply chains. NEMA convened industry experts to identify technical guidelines that electrical equipment manufacturers can implement during product development to minimize the possibility that bugs, malware, viruses or other exploits could be used to negatively impact product operation. On June 25, 2015, NEMA published a white paper on cybersecurity supply

chain best practices for manufacturers, "NEMA CPSP 1-2015: Supply Chain Best Practices." The report is available online at http://www.nema.org/supply-chain-best-practices.

The document addresses supply chain integrity through four phases of a product's life cycle:

- **Manufacturing**: Analysis during manufacturing and assembly to detect and eliminate anomalies in the embedded components of the product's supply chain;
- **Delivery**: Tamper-proofing to ensure that the configurations of the manufactured devices have not been altered between the production line and the operating environment;
- **Operation**: Methods by which a manufactured device enables asset owners to comply with security requirements and necessities of the regulated environment;
- **End-of-life**: Decommissioning and revocation processes to prevent compromised or obsolete devices from being used as a means to penetrate active security networks.

U.S. manufacturers are implementing the recommendations included in this report to protect their supply chains from, among other things, counterfeit, re-labeled, used, and grey market products that could cause security and safety risks.[3]

Cybersecurity Hygiene

On March 7, 2018, NEMA Members approved a new technical document, "NEMA CPSP 2-2018, Cyber Hygiene," detailing industry best practice cyber hygiene principles for electrical manufacturers to implement in their manufacturing and engineering processes.[4] The guideline

[3] http://www.eaton.com/Eaton/ProductsServices/Electrical/ThoughtLeadership/Anti-Counterfeiting/index.htm#tabs-2
[4] This document will be published in May 2018, and will be available for download at www.nema.org

document addresses raising a manufacturer's level of cybersecurity sophistication by following seven fundamental principles:

- **Segmenting networks**: Designing data networks that logically and/or physically separate manufacturing systems' data flows from business or public networks;
- **Understanding data types and flows**: Understanding what data should flow through a network, where that data typically goes, and what or who should have access to it;
- **Monitoring devices and systems**: Providing the ability to monitor the health and security of devices and systems using existing, well-known, standard software protocols;
- **User management**: Restricting access to networks to only properly authenticated and authorized users;
- **Hardening devices**: Identifying potential threats and protecting hardware from unauthorized access (e.g., by removing unnecessary software from computers, encrypting confidential and sensitive data, etc.);
- **Updating devices**: Regularly patching and updating devices to protect against evolving vulnerabilities; and
- **Providing a recovery plan and/or escalation process**: Developing a plan to follow in the event that a vulnerability is identified, including incident detection and recording, classification and initial support, investigation and diagnosis, resolution and recovery, incident closure, monitoring the progress of the incident resolution, and a communication plan to inform affected parties about the status of the resolution.

Government and private industry should work together to address challenges

While industry is moving forward with a focus on cyber-security, there are opportunities for the private sector and government to work together.

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* is an example of a successful collaboration between industry and government to develop a voluntary, flexible framework to promote cybersecurity protection for multiple types of infrastructure, including the electric grid.[5] The NIST *Framework* should be referenced by the Department of Energy and other agencies as they work with private industry to promote cybersecurity best practices. It is important that the Department of Energy not reinvent or duplicate the tremendous work already accomplished by NIST; rather, DOE should collaborate with NIST to promote cybersecurity in the energy sector.

Electricity Information Sharing and Analysis Center (E-ISAC)

Another opportunity for public-private cooperation is to allow representation from electric grid equipment manufacturers as full participants in the Electricity Information Sharing and Analysis Center (E-ISAC), managed by the North American Electric Reliability Corporation. The E-ISAC is the principal information- and analysis-sharing gateway for the electricity industry.[6]

[5] https://www.nist.gov/cyberframework
[6] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf

Cyber Sense Act* and *Enhancing Grid Security through Public-Private Partnerships Act

With the above-mentioned industry-developed and -supported cybersecurity best practices in mind, I will make a few comments on two of the bills under consideration today—the *Cyber Sense Act* and the *Enhancing Grid Security through Public-Private Partnerships Act*.

Cyber Sense Act (H.R. 5239)

NEMA Member manufacturers support voluntary cybersecurity evaluation of products used in the transmission, distribution, storage, and end-use of electricity. Not doing so could permit unsecure equipment to be installed, potentially compromising the electric system. However, the specific requirements of any such program need to be carefully designed in close collaboration with manufacturers. We recommend that any cybersecurity evaluation program abide by the following principles:

- Evaluation procedures and requirements should be developed via an open and transparent process with sufficient opportunity for participation and input from the private sector, including electrical manufacturers and electric utilities;
- Electric grid product manufacturers and approved third-parties should be permitted to conduct Cyber Sense evaluation, in accordance with agreed upon evaluation procedures;
- Evaluation procedures and requirements should rely on industry-developed standards and best practices where available and applicable;
- Procedures should avoid reliance on "single point of time" evaluation as a primary determining factor, as the nature of these risks are constantly changing and the

previously described best practices outline continuously evolving system features that require continuous commissioning and patching;

- Sensitive information should be handled with appropriate care to prevent premature or unauthorized disclosure, including system attributes as well as the details of the specific evaluation requirements and information of the results beyond a summary; any disclosure of these types of details undermines the process by providing what could amount to a roadmap for entities attempting to negatively impact the system;
- The scope of the program should be clear and the products to be tested should be decided upon with industry participation;
- The program should account for how products are intended to be installed and operated (e.g., some products are intended to be installed behind layers of security, a concept referred to as "defense-in-depth," and it would be inappropriate to test those products in the same manner as products that are intended to connect directly to the public internet);
- The program should account for the fact that once products are sold, manufacturers often don't know where their products are put into use, how they have been installed, or how they are being operated; asset owners should maintain a system for tracking products;
- Upon the discovery of any vulnerability, manufacturers should be immediately notified and provided an opportunity review the findings and provide feedback to the Department of Energy;

Enhancing Grid Security through Public-Private Partnerships Act (H.R. 5240)

NEMA supports the concepts included in the *Enhancing Grid Security through Public-Private Partnerships Act*.

With respect to Section 2, "Program to Promote and Advance Physical Security and Cybersecurity of Electric Utilities," NEMA agrees that voluntary technical assistance efforts should be available to provide electric utilities with information and resources to effectively prepare for and combat both physical and cybersecurity threats. We also agree that this technical assistance should be provided in close collaboration with state governments and public utility regulatory commissions, as well as with equipment manufacturers. Including manufacturers in training and technical assistance efforts will ensure that products are installed and maintained as intended to limit the risk of a cyberattack resulting from possible improper use of a product.

NEMA also supports the recommendations included in Section 3, "Report on Cybersecurity and Distribution Systems," and Section 4, "Electricity Interruption Information." One additional outage index that should be included in Section 4(b) is Momentary Average Interruption Frequency Index (MAIFI). MAIFI is the average number of momentary (< 5 minutes) power interruptions experienced by a utility customer in a given year. Momentary outages cost U.S. electricity customers $60 billion in 2014, accounting for more than half the cost of all power outages.[7] Certain electrical equipment is sensitive to fluctuations in electricity voltage and frequency, which can cause significant disruptions for customers.[8] For example, some owners of distributed generation resources (like rooftop solar photovoltaic systems) have reported that their systems periodically shut off as a precaution when the system inverter senses

[7] http://grouper.ieee.org/groups/td/dist/sd/doc/2016-09-02%20LBNL%202016%20Updated%20Estimate-Nat%20Cost%20of%20Pwr%20Interruptions%20to%20Elec%20Custs-Joe%20Eto.pdf

[8] http://www.elp.com/articles/powergrid_international/print/volume-20/issue-6/features/utility-industry-targets-growing-concern-momentary-outages.html

voltage and frequency disruptions on the grid; while inverter manufacturers are working on systems that can safely "ride through" these disruptions, a better solution would be to decrease these momentary grid disruptions.[9,10] In industrial applications, momentary outages and voltage/frequency fluctuations can impact the performance of electric motors, necessitating the need to restart industrial processes, which results in expensive downtime. Additionally, with more people working from home, momentary outages are also having an impact on teleworkers; without the protection of an uninterruptible power supply, computers might shut down while teleworkers are editing documents, for example.

Conclusion

NEMA and NEMA Member companies recognize that cybersecurity risks are constantly evolving, and we want to thank the Committee for hosting this very important hearing. As you move forward in considering these bills, we urge you to ensure that manufacturers and electric utilities are consulted start-to-finish, and that industry best practices and standards are used wherever feasible. NEMA looks forward to working with and being a resource for the Committee as you continue your work to address cybersecurity concerns within the energy sector.

Thank you for your attention, and I look forward to answering any questions you might have concerning my testimony.

[9] https://www.ferc.gov/whats-new/comm-meet/2016/072116/E-11.pdf
[10] http://www3.dps.ny.gov/W/PSCWeb.nsf/96f0fec0b45a3c6485257688006a701a/def2bf0a236b946f85257f71006ac98e/$FILE/EPRI%20Fact%20Sheet.pdf

Mr. WALBERG. Thank you.
I now recognize Mr. Aaronson.

STATEMENT OF SCOTT AARONSON

Mr. AARONSON. Thank you, Mr. Chairman, Ranking Member Rush, and members of the subcommittee. I appreciate the opportunity to testify here today. For EEI's member companies, which includes all of the Nation's investor-owned electric companies, securing the energy grid is a top priority. I appreciate your invitation to discuss this important topic on their behalf.

The electric power industry, which includes investor-owned electric companies, public power utilities, and electric cooperatives, supports more than 7 million American jobs and contributes $880 billion annually to U.S. gross domestic product—about 5 percent of the total. That 5 percent is truly the first 5 percent, responsible for generating and delivering the energy that powers our economy and our way of life.

Our members own and operate some of the Nation's most critical infrastructure and they take that responsibility seriously. EEI's member companies prepare for all hazards—physical and cyber events, naturally occurring or manmade threats, and severe weather of every kind. To address multiple threats, our companies take what's known as a defense in-depth approach with several layers of security. I would like to highlight three main areas of focus: standards, partnerships, and response and recovery.

First, standards—through a process created by Congress the electric power sector is subject to mandatory enforceable critical infrastructure protection, or CIP, regulatory standards for cyber and physical security. Through these standards, the bulk power system enjoys a baseline level of security. Standards are important, but with intelligent adversaries operating in a dynamic threat environment, regulations alone are insufficient and must be supplemented.

That brings me to the second area of focus, which is partnerships, which you have heard a lot about today. You heard it from DOE and you will hear it from this entire panel—security is a shared responsibility. None of us can do this alone. To be successful in this environment, industry and government must partner, and as you heard earlier, we are.

I am here this morning in my role as EEI's Vice President for Security and Preparedness but I am also privileged to be a Member of the Secretariat for the Electricity Subsector Coordinating Council. The ESCC is comprised of CEOs of 22 electric companies and nine major industry trade associations representing the full scope of electric generation, transmission, and distribution in the United States and Canada.

Through partnerships like the ESCC, government and industry leverage one another's strengths. This partnership manifests itself in many ways including deployment of government technologies, like CRISP, which you have heard about, multidirectional information sharing, drills and exercises, and facilitating cross-sector coordination.

What makes the ESCC effective is CEO leadership across all segments of the industry. This structure provides resources, sets priorities, drives accountability. Furthermore, CEOs serve as a draw to

other senior counterparts in industry sectors and in government. The unity of effort driven by industry working with government has produced significant tangible results.

Finally, the third area of focus is response and recovery. The electric power sector is proud of its record on reliability but outages do occur. The past year has made one thing abundantly clear—we can't protect everything from everything all of the time and investments help companies restore power and be prepared. Our industry invests more than $120 billion each year to make the energy grid stronger, smarter, cleaner, more dynamic, and more secure. In addition, the industry's culture of mutual assistance unleashes a world-class workforce amidst the toughest conditions to restore power safely and effectively.

Today, we have supplemented that traditional response in recovery with a 21st century edition—cyber mutual assistance. So far, more than 140 entities are participating in the program, covering more than 80 percent of U.S. electricity customers. That brings me to the bills before the subcommittee today. We appreciate both Congress and the Trump administration's support of the electric power sector.

Just as EEI's member companies evolve to meet new threats, our government partners continuously improve their posture through these new initiatives. For example, we applaud DOE Secretary Perry and his team for establishing DOE's new Office of Cybersecurity, Energy Security, and Emergency Response, or CESER.

Legislation passed by this committee codified DOE's role as the sector-specific agency—thank you—and we believe the elevation of CESER will deepen the relationship between our industry and DOE on issues of cybersecurity and energy grid response initiatives.

In his testimony, Secretary Menezes mentioned DOE's establishment of the supply chain testing facility. We are interested in the details of that program. The subcommittee is also aware that through the NERC/FERC process as mandatory supply chain standard will be implemented soon. The committee should consider those efforts when adopting legislation related to supply chains.

Finally, I would like to mention a report included in the Enhancing Grid Security Through Public-Private Partnerships Act looking at distribution, cyber, and physical security. EEI supports this report because it could address several emerging questions that many in the industry also are asking. What considerations should be made to protect a distribution system that is outside of mandatory NERC CIP standards? How can we secure newer technology that is largely consumer grade but may increase the energy grid's attack surface?

A collaborative risk-based approach to security at the distribution level is essential. This report should drive that approach and consider the many different entities in the distribution grid, electric companies, and others.

Again, I appreciate you holding this hearing. I look forward to answering any of your questions.

[The prepared statement of Mr. Aaronson follows:]

STATEMENT OF SCOTT I. AARONSON

VICE PRESIDENT, SECURITY AND PREPAREDNESS

EDISON ELECTRIC INSTITUTE

BEFORE THE U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON ENERGY

"DOE MODERNIZATION: LEGISLATION ADDRESSING

CYBERSECURITY AND EMERGENCY RESPONSE"

MARCH 14, 2018

Summary

America's electric companies work every day to produce and deliver energy that is reliable, affordable, safe, and increasingly clean for their customers. The energy grid powers our economy and our way of life, so providing reliable service is a responsibility electric companies take very seriously.

Threats to that reliability have changed over time and continue to evolve. So, too, has our approach to security. EEI's member companies prepare for all hazards—that means physical and cyber events, naturally occurring or manmade threats, and severe weather of every kind. Our security strategies are not put in place with one threat in mind. Our companies take a "defense-in-depth" approach with several layers of security strategies, designed to eliminate single points of failure. Finally, since our companies cannot protect every asset from every threat all the time, we must prioritize based on the likelihood and severity of a threat, as well as work to manage consequences by restoring power quickly and safely regardless of why an outage occurred.

There are three main components to the electric power sector's defense-in-depth approach: mandatory and enforceable reliability regulations; industry/government partnerships; and efforts to enhance our response and recovery to incidents.

Security is a shared responsibility. While most critical infrastructure is owned largely by the private sector, government at all levels can and must play a role in protecting it. Through partnerships like the Electricity Sector Coordinating Council (ESCC), government and industry leverage one another's strengths. This partnership manifests itself in many ways, including deployment of government technologies, multi-directional information sharing, drills and exercises, and facilitating cross-sector coordination.

We appreciate both Congress and the Trump Administration's support of the electric power sector. Just as EEI's member companies evolve to meet new threats, our government partners continuously improve their posture through new initiatives, most recently the establishment of the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) at the Department of Energy.

Introduction

Chairman Upton, Ranking Member Rush, and members of the Subcommittee, thank you for the opportunity to testify. My name is Scott Aaronson, and I am Vice President for Security and Preparedness at the Edison Electric Institute (EEI). EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for 220 million Americans and operate in all 50 states and the District of Columbia. For EEI's member companies, securing the energy grid is a top priority. I appreciate your invitation to discuss this important topic on their behalf.

The electric power industry—which includes investor-owned electric companies, public power utilities, and electric cooperatives—supports more than 7 million American jobs and contributes $880 billion annually to U.S. gross domestic product, about 5 percent of the total.

While I am here today in my EEI capacity and am testifying on behalf of our membership, I would like to highlight another thread that ties the electric sector together: the Electricity Subsector Coordinating Council (ESCC). The ESCC is comprised of the chief executive officers of 22 electric companies and 9 major industry trade associations, including EEI, the American Public Power Association (APPA), and the National Rural Electric Cooperative Association (NRECA). This group—which includes all segments of the industry, representing the full scope of electric generation, transmission, and distribution in the United States and Canada—serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level incidents or threats to critical infrastructure.

We appreciate the continued interest the Committee has on grid security. I was pleased to testify before this Subcommittee in February 2017. In addition to addressing the legislation before the Subcommittee, I would like to update the Committee on several items and reiterate a few key themes.

All Hazards: The Electric Power Industry's Approach to Security

America's electric companies work every day to produce and deliver energy that is reliable, affordable, safe, and increasingly clean for their customers. The energy grid powers our economy and our way of life, so providing reliable service is a responsibility electric companies take very seriously.

Threats to that reliability have changed over time and continue to evolve. So, too, has our approach to security. EEI's member companies prepare for all hazards—that means physical and cyber events, naturally occurring or manmade threats, and severe weather of every kind. Our security strategies are not put in place with one threat in mind. Our companies take a "defense-in-depth" approach with several layers of security strategies, designed to eliminate single points of failure. Finally, since our companies cannot protect every asset from every threat all the time, we must prioritize based on the likelihood and severity of a threat, as well as work to manage consequences by restoring power quickly and safely regardless of why an outage occurred.

Defense-in-Depth: Standards, Partnerships, and Response

I would like to highlight three main components to the electric power sector's defense-in-depth approach: mandatory and enforceable reliability regulations; industry/government partnerships; and efforts to enhance our response and recovery to incidents.

Standards. Under the Federal Power Act and Federal Energy Regulatory Commission (FERC) oversight, the electric power sector is subject to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards that include cyber and physical security requirements. Entities found in violation of CIP standards face penalties that can exceed $1 million per violation per day. These mandatory standards continue to evolve using the process created by Congress to allow for input from subject matter experts across the industry and government.

The industry also uses voluntary standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Department of Energy's (DOE's) Cybersecurity Capability Maturity Model (C2M2).

Through these standards, the entire bulk power system enjoys a baseline level of security. Standards are important, but with intelligent adversaries operating in a dynamic threat environment, regulations alone are insufficient and must be supplemented.

Partnerships. Security is a shared responsibility. While most critical infrastructure is owned largely by the private sector, government at all levels can and must play a role in protecting it.

Through partnerships like the ESCC, government and industry leverage one another's strengths. This partnership manifests itself in many ways, including deployment of government technologies, multi-directional information sharing, drills and exercises, and facilitating cross-sector coordination.

This unity of effort driven by industry working with government has produced significant, tangible results. The sector continues to deploy the Cybersecurity Risk Information Sharing Program (CRISP), a public-private partnership that includes industry, DOE, Pacific Northwest and Argonne National Laboratories, and the Electricity Information Sharing & Analysis Center (E-ISAC), which manages the program. More than 75 percent of U.S. electric customers are served by a company that has deployed CRISP, and this program will continue to grow as the information gleaned from its sensors and the associated analysis has proven extremely valuable to identifying and addressing cybersecurity risks.

Response and Recovery. The electric power sector is proud of its record on reliability, but outages do occur. When outages happen, many key investments help companies restore power safely and as quickly as possible. Our industry invests more than $120 billion each year to make the energy grid stronger, smarter, cleaner, more dynamic, and more secure. The deployment of more than 75 million smart meters, covering more than 60 percent of American households, improves resiliency and service for our customers. The industry's culture of mutual assistance unleashes a world-class workforce amidst the toughest conditions to restore power safely; neighbors helping neighbors during the worst of the worst.

Industry-government exercises, such as the biennial GridEx, sharpen the industry's skill set, ensuring that when incidents happen our playbook has been tested before it is put into action. GridEx IV, held in November 2017, brought together more than 6,000 participants representing more than 400 organizations from across the electric power industry and federal and state governments. These drills sharpen not just the unity of effort between electric companies and government agencies, but also practice unity of message to ensure that we speak with one voice to our customers and your constituents during incidents.

Today, we have supplemented that traditional response and recovery with a 21st-century addition: cyber mutual assistance. The same surge capacity that rushes to companies in need during hurricanes, winter storms, and wildfires stands ready to assist and share resources in the face of a potential cyber incident. So far, more than 140 entities including investor-owned natural gas and power companies, cooperatives, municipalities, Canadian power companies, and Regional Transmission Organizations/Independent System Operators (RTOs/ISOs), are participating in the program. These entities cover more than 80 percent of U.S. electricity customers, roughly 75 percent of U.S. domestic natural gas customers, and 74 percent of natural gas distribution pipelines.

Government's Role in Grid Security

As stated above, grid security is a shared responsibility. We appreciate both Congress and the Trump Administration's support of the electric power sector. Just as EEI's member companies evolve to meet new threats, our government partners continuously improve their posture through new initiatives.

For example, we applaud DOE Secretary Perry and his team for establishing DOE's new Office of Cybersecurity, Energy Security, and Emergency Response (CESER). Legislation passed by this Committee codified DOE's role as the sector-specific agency, and we believe the elevation of CESER will deepen the relationship between our industry and DOE on issues of cybersecurity and energy grid response initiatives. H.R. 5174, the Energy Emergency Leadership Act, amends DOE's enabling statute by adding the new function "energy emergency and energy security" for the to-be-appointed CESER Assistant Secretary. We appreciate the clarification that technical assistance and response capabilities are provided "upon request of a...energy sector entity," but encourage the Committee to consider defining energy emergency and energy security.

The Cyber Sense discussion draft is nearly identical to Section 1106 of H.R. 8, the House-passed comprehensive energy bill from last Congress. The bill establishes "a voluntary Cyber Sense program to identify and promote cyber-secure products intended for use in the bulk-power system." As mentioned above, the electric power industry—and specifically our bulk power system assets—are subject to mandatory and enforceable cyber and physical security standards developed by NERC and approved by FERC. Notably, since House passage of the energy bill in December 2015, a supply chain risk management standard was developed by NERC and proposed to be adopted by FERC. While that standard may obviate the need for a program like Cyber Sense, the Committee may consider supporting ongoing efforts at DOE to establish testing facilities that have similar goals and outcomes to the discussion draft.

The discussion draft "Enhancing Grid Security through Public-Private Partnerships Act" contains several notable provisions. Section 2 establishes a DOE program to advance industry cyber and physical security. The section is aimed at smaller companies—and follows work DOE already is doing through initiatives such as the Rural Cooperative Cybersecurity Capabilities Program between DOE and NRECA and APPA's Cybersecurity Cooperative Agreement with DOE. EEI is supportive of the report ordered by Section 3 of the bill. This DOE-led report on distribution cyber and physical security should address several emerging questions that many in the industry also are asking: What considerations should be made to protect a distribution system that is outside of mandatory NERC CIP standards? How can we secure newer technology that is largely consumer-grade, and may increase the energy grid's attack surface?

The number of distribution assets—including distributed energy resources and customer devices "behind the meter"—is growing and can impact the broader electricity system. As deployment increases throughout the electric delivery system, the security of these interconnected devices must be considered to prevent cybersecurity incidents from impacting reliability.

To be clear, the distribution system has been—and should continue to be—regulated locally by state regulatory commissions. As such, it is welcome that state commissions are one of the consulted entities for the report, alongside industry stakeholders. At the same time, there is benefit to uniform standards since these vendors and their devices are sold across state lines. However, mandates should be avoided, as they could be prohibitively expensive for electric companies and their customers. Taken together, it is clear that a collaborative, risk-based

approach to security at the distribution level is essential. This report should drive that approach and consider the many different entities in the distribution grid—electric companies and others.

Conclusion

Thank you again for holding this hearing. I am hopeful that my testimony underscores the industry's commitment to security and our willingness to work with many partners to address all hazards. We look forward to continuing close collaboration with our government partners to meet the evolving threat. We appreciate the bipartisan support that grid security legislation historically has enjoyed in Congress and the work you have done to enhance our security posture. We look forward to working on these legislative proposals and others to meet this most-important mission.

Mr. WALBERG. Thank you. Thanks to the panel for your very efficient use of the 5 minutes time. Maybe it would be an example to myself and my colleagues.

Now privileged to represent the neighbor to the south who guards my border, Mr. Latta.

Mr. LATTA. Well, thank you very much, Mr. Chairman, and I appreciate our panel for being here. And again, this is a really important hearing that we are having today because it affects us all.

Mr. Pitsor, if I could start with my questions with you, if I may, please. In your testimony you state that you support a voluntary cybersecurity evaluation of products used in bulk power systems such as the program described in H.R. 5239 Cyber Sense.

One point you raise is that once products are sold manufacturers often don't know where or how these components are used, installed, or operated. You suggest that asset owners should maintain a system of tracking products. Would you explain in detail why it is important to track these products?

Mr. PITSOR. As we look at evaluation of cybersecurity threats of different components and how they're assembled in the manufacturers, once they have sold a product, they're assembled in the field. They're not necessarily aware of who purchased them and how they were assembled. And so the tracking concept here is to have a database and that could be shared so would be more familiar with where products have been placed, how they've been assembled, how they've been installed, how they've been commissioned. So that if patching is necessary due to a cyber-related event or testing for that product, we would then be able to contact the asset user as to what patches should be installed and how they should be installed.

Mr. LATTA. Let me follow up, when you're talking about the database because in Section 2(b)(2) of the Cyber Sense bill establishes a cybersecurity vulnerability reporting process and related database for products tested and identified as cybersecure under this program.

Would this help address the need for a system for tracking those products by having that, as you just mentioned?

Mr. PITSOR. I think a database would be very helpful in terms of addressing that need, yes.

Mr. LATTA. Thank you.

Mr. Aaronson, if I could ask you, and I think you mentioned in your testimony about when you were out with co-ops, and I know I just was at two of my co-ops. I represent the largest number of co-ops in the State of Ohio.

But if I could ask this question—as the new technologies are becoming increasingly interconnected within our electric grid, new vulnerabilities are emerging across the system including at the distribution level. Currently, the physical or cybersecurity of the bulk power system or the interstate is addressed through the Critical Infrastructure Protection Standards issued by NERC. But the distribution system intrastate is outside the jurisdiction of the mandatory NERC standards and the question is are there implications for this perceived gap in oversight and protection of the cybersecurity of the distribution portion of the Nation's electrical grid?

Mr. AARONSON. So a couple of things to respond to there. As I mentioned in my testimony, we operate one big machine, right, with thousands of owners and operators from really large investor-owned electric companies that EEI represents to co-ops and municipal systems of varying sizes. And so as you know, the ESCC incorporates all of those and we work very closely. I know both APPA and NRECA provided written testimony or written statement for the record. So I would refer to that.

With respect to gaps, and I call them perceived gaps, just because distribution level components are not subject to the Federal CIP standards does not mean that there is not security happening at that level. That said, we do think that anything we can do with respect to components that make up that part of the grid—the intrastate—the distribution level, is going to be an important approach to continue to advance security for all of us.

The other thing I would say about distribution security is we need to prioritize. In security you protect diamonds like diamonds and pencils like pencils, and to be sure, there are diamonds at the distribution level that we need to be aware of. There are components that are crown jewels at the distribution level that we need to be securing. And so approaches like Cyber Sense may allow us to do that and some of the things that Secretary Menezes and Assistant Secretary Hoffman were discussing with respect to really looking closely at those components and drilling down on the most critical, because if you have a hundred priorities you have no priorities—but really finding those most critical components and beating the heck out of them so that we can understand if there are any vulnerabilities in them, again, will make us all more secure.

Mr. LATTA. Well, thank you very much, Mr. Chairman. My time is about to expire and I yield back.

Mr. WALBERG. I thank the gentleman.

Now I am privileged to recognize the ranking member, the gentleman from Illinois—in fact, the district I was privileged to be born in—I quickly add long before you represented the district, Mr. Rush.

[Laughter.]

Mr. RUSH. Mr. Chairman, it's still the best district in the Nation.

Mr. Vance, in your written testimony you noted that DOE held a cybersecurity contest which brought together students competing to address the challenges of protecting infrastructure and firms that might employ the same students after they graduate.

Do you think that on both the public and private sector that we are doing enough to ensure that we have a skilled workforce capable of meeting the challenges we will inevitably face in regards to cybersecurity? And I will invite any other members of the panel to weigh in on some of these issues.

Mr. VANCE. I think what we've been doing in Indiana is specifically trying to bring together the public and private sides together to analyze what some of the weaknesses are, what we are good at, what we are not good at, and as Mr. Aaronson from EEI spoke about just a second ago, I think we need to prioritize and figure out where those diamonds are and where those pencils are.

It's one thing for me and my colleagues in the public sector to sit in a room and try to figure out what we need to focus on. We

are going to miss a lot of things. What we need to do is sit down with the private sector and work through a collaborative process to identify where our weaknesses are and how to strengthen those.

So the bills being discussed today, I think, are four steps in the right direction to help strengthen those partnerships.

Mr. RUSH. Anybody else want to chime in?

Mr. TUDOR. Mr. Rush, thank you for the question.

I agree that public-private partnerships are key to moving these forward and these four pieces of legislation are definitely great steps toward that.

At the Idaho National Lab, we know that the partnerships are the strongest part of our operation, whether it's with vendors, asset owners, with other government agencies and that's the way that we will be able to develop the structures to keep our cyber resilience in our energy systems.

Mr. RUSH. And does anyone have any suggestions on how the Congress could help you to ensure that we have enough skilled workforce other than what's information in these four bills?

Mr. VANCE. I will add, real quick, just to give a little bit more perspective on what we are doing in Indiana. Our approach with our cybersecurity council has been to bring together all the potential industries involved in cybersecurity. So right now, I've got about 250 or so members of that council spanning about 20 different industries with industry subgroups that then things can bubble up through those subgroups into the full committee to address in a cross-sector manner.

So I will give you an example. One of the committees is focused on personal identifiable information because that's something that's not unique to any one specific industry and it really needs to be a topic in and of itself. But it can't just be its own council or committee. It has to be part of a bigger picture because it ties back to energy, water, finance—all these other things.

So what we've been trying to do in Indiana is to build a large council that integrates all these different aspects so it can be addressed in a cross-sector manner across different industries.

Mr. AARONSON. Mr. Rush, I would add, I know you're very committed to workforce development in particular with respect to cyber and I think one of the things that you're hearing both from the previous panel and all of us is this is a shared responsibility.

It's a whole of community issue. I reference in my verbal testimony the cyber mutual assistance program. To us, that is a force multiplier. That is when a company is being attacked their counterparts come from around the country and around the Nation and around North America, frankly, to support them. And so I think that's great for the electricity sector and we are very proud of that. But to be able to work with the National Guard, to be able to work with other sectors, to be able to prioritize restoration when cyber incidents maybe are impacting more than one sector.

We need to look at this again far more holistically. And then from a workforce perspective, we are very proud of the development that we do within our sector through things like the CEWD. It's the Energy Workforce Development—Committee for Energy and Workforce Development is a great example of how we can find those gaps that we have in our workforce and work through edu-

cation, work through public-private partnerships to improve our staffing in our most critical needs.

Mr. RUSH. Thank you, Mr. Chairman. I yield back.

Mr. WALBERG. I thank the gentleman.

I now recognize the gentleman from Virginia, Mr. Griffith.

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

Mr. Tudor, I am going to come to you first but I am going to take what's more or less a point of personal privilege and just say that I saw you sitting throughout that first panel and all those questions on that second row there with a couple of young people who are very well behaved. Are they connected with you?

Mr. TUDOR. Yes, sir. That's my son, Miles, and my niece, Sydney. They're getting a civics lesson today.

Mr. GRIFFITH. Well, not the most riveting of hearings but one that's very important and they have done a great job and I thought they were—you could tell they were doing some stuff back there and I thought they were like my kids, playing on an electronic device. But, apparently, they have a numbers game that they're working on that's all done with their hands and they've been very quiet and very well behaved. So you and your family are to be commended for having such well-behaved children.

That being said, let's get down to business. You make reference to the consequence-driven cyber-informed engineering—CCE methodology. You say this is more about getting ahead of the problems of vulnerabilities and threats rather than chasing them. Can you describe what role this approach may have in strengthening cybersecurity and critical infrastructure?

Mr. TUDOR. Yes. Thank you for that question, sir.

So consequence-driven cyber-informed engineering, or CCE, kind of identifies the problem—that we are constantly seeing new vulnerabilities, new threats every day. So an organization does a risk assessment on a Monday and by Wednesday when new vulnerabilities are discovered, many of the activities described in that risk assessment may be moot.

But if we go back and look at the key consequences of any organization and we take an electric utility at this, if keeping the lights on is their mission but maybe there's several key components that if they were lost may prevent that mission from being carried out. Looking at the engineering methods of those consequences, looking at the way an adversary might go about attacking those infrastructures, using a threat-based methodology and at INL we do a lot of work considering the threat first and we use that mindset when we look at our different mitigations, and then developing mitigations with the asset owner who is a key component of this.

So if we can engineer out those severe consequences, irregardless of the threat or the current risk or a new vulnerability then we believe that that has a chance of maintaining that resiliency over a longer period rather than just addressing new vulnerabilities as they show up.

Mr. GRIFFITH. I appreciate that, and there's a pilot program but it's had very limited deployment. Are you confident this methodology is an effective approach and, if so, what are you trying to examine before deciding whether this program should be expanded?

Mr. TUDOR. Yes, thank you again.

We have conducted one pilot. We are on a second, and I think that as we've been briefing this across Congress, the National Security Council, and others, we've been very encouraged that people do believe that this type of methodology will be able to go forward.

So we are working with the DOE and others to develop some ways to do CCES scale. In our next few pilot engagements we'll be bringing more partners along to provide training for them and they can go out and provide training for others. So we hope to be able to scale out this methodology in the next several years.

Mr. GRIFFITH. I appreciate that.

Mr. Engels, you have got a new pipeline coming near my district, although not through my district, and I asked before about some, for lack of a better term, smart pipe technology. I know you're not expecting that question today and so if you could just get me an answer later as to what you all might be doing in regards to letting us know if there's some kind of a break in the line quicker using some smart technology.

Mr. ENGELS. I will be glad to follow up with you on that.

Mr. GRIFFITH. And likewise, I have a friend who's got a farm where there's going to be a pump station and whatever you all could do to reassure folks that they're being placed in the safest location and likewise if there's any smart technology in there I would appreciate having that information.

Mr. ENGELS. I understand. We'll make sure we follow up.

Mr. GRIFFITH. Thank you. All right.

Mr. Aaronson, you mentioned in your written testimony that approximately 75 percent of U.S. customers are served by a company that participates in cybersecurity risk information sharing program.

Do you have any insight what's going on with the other 25 percent?

Mr. AARONSON. So CRISP is a wonderful technology and the beauty of it is it was something that was actually developed by National Labs. It was piloted for a few years by a small subset of companies—did some proof of concept, and that was then. We'll call it commercialized, although maybe that's not a fair characterization because it is still a public-private partnership with the Department of Energy, the North American Electrical Reliability Corporation through their information-sharing analysis center—I am trying to not use acronyms—and then the companies that deploy it.

What we are looking to do and what the ISAC is planning to do now is to expand the program. So it started with five pilots. It has expanded to more than that, to the 75 percent of customers being represented by a company that has deployed CRISP. The other thing you should note is that information, while it is gleaned from the companies that have deployed the sensors that make up CRISP, the information that is gleaned is actually socialized to the entire electric utility sector.

So while there are sensors on 75 percent of companies, we are going to get a much broader cross-section in the coming years.

Mr. GRIFFITH. I appreciate that. Thank you for the answer. I thank all of you for being here today, and I yield back.

Mr. WALBERG. I thank the gentleman and I recognize the gentleman from California, Mr. McNerney.

Mr. MCNERNEY. I want to thank the chairman and I thank the witnesses. Good testimony and informative.

Mr. Aaronson, in your testimony you pointed out that the EEI members do work to prepare for hazards and cyber or natural events. What are your members doing to prepare for climate change events? Is there a standard or is there some sort of work that needs to be done that's being done?

Mr. AARONSON. So, again, I think we look at this as all hazards, and whether it is an act of war or an act of God, whether it is a natural disaster, whether it's an earthquake, whether it's the wildfires that I know that your district has been impacted by, we are looking at ways we can be more resilient, and a lot of what we do kind of crosses, again, acts of war and acts of God and is more about consequence management. Why the lights were turned off—why there was a power outage becomes a little less relevant and how quickly can we get them restored. And so a lot of our focus is on that response and recovery and resilience component of preparation for all manner of hazards.

Mr. MCNERNEY. OK. Thank you.

Mr. Pitsor, I appreciate your comments on the enhancing grid security through public-private partnerships. You mentioned that you wanted to see a Momentary Average Interruption Frequency Index included in the ICE calculation. How would that improve the calculation? How would that improve the results?

Mr. PITSOR. Well, the MAIFI index represents some nearly 50 percent of all the momentary outages that occur in the U.S. and these are momentary outages that are usually 5 minutes or less. We think that the overall interrupter calculation, if it's missing those 50 percent of the outages, it's not capturing fully the economic costs that are associated by these smaller momentary outages. For instance, electric motors trip off, computers don't have backup power trip off. There are costs associated with that that should be captured in the overall estimator.

Mr. MCNERNEY. OK. You mentioned the Cyber Sense Act. How would your members respond to nonvoluntary requirements for—including cybersecurity in their products?

Mr. PITSOR. We are very supportive of the evaluation testing of electrical equipment. I think the key is going to be what type of equipment we are speaking of—the scope of the testing, what protocols we are testing against, who's paying for that testing, and the follow-on work that will be done to address vulnerabilities that are found in terms of patching, recommissioning, the continuous process that goes on in addressing cyber——

Mr. MCNERNEY. It seems that your members would want to have a set of standards they could link their products to.

Mr. PITSOR. Exactly. Working on supply side standards that I mentioned, a new cyber security index standard and then looking at how we test different products and different configurations against different vulnerabilities. We segment those products because some products, as has been recognized, are behind layers of security. So the testing of those maybe are less than those that have outward-facing connection to the internet. There are different levels of testing that would be required for those products.

Mr. MCNERNEY. Do you have concerns about cuts that are being proposed in the fiscal 2019 budget's impact on cybersecurity or security in general? I guess Mr. Aaronson would be the right person to ask that question of.

Mr. AARONSON. So we appreciate what the Department of Energy has done with respect to CESER and elevating some of these issues. We've worked really closely in particular with the Office of Electricity and their Infrastructure Security Energy Restoration Office, which will ultimately matriculate over the CESER.

This last historic hurricane season and the nor'easters the last several weeks, and with that response from Puerto Rico—so between that, our partnerships with the labs and our partnerships with the sector coordinating council we have really appreciated the ability to work closely with this administration and the previous administration. This has been a priority for Department of Energy for several years now.

Mr. MCNERNEY. So you don't see any sort of a drawback with the cuts that are being proposed?

Mr. AARONSON. At this point, I think the priorities that we care about most have not been impacted in our day-to-day interactions with the department.

Mr. MCNERNEY. Thank you. I yield back.

Mr. WALBERG. I thank the gentleman.

Now I recognize the good doctor and gentleman from Indiana, Mr. Bucshon.

Mr. BUCSHON. Thank you, Mr. Chairman.

Mr. Vance, good to have you here from Indiana.

Mr. VANCE. Thank you.

Mr. BUCSHON. You're welcome. As you know, electric cooperatives serve more than 1.3 million customers in the State of Indiana, primarily those in rural parts of the State, which is southwest Indiana, the Wabash Valley that I represent. An additional 300,000 individuals are served by municipal electric utilities. Both cooperative and municipal utilities are generally much smaller than their investor-owned counterparts.

What are some of the specific challenges that you see these smaller utilities face in terms of defending their assets against cybersecurity threats?

Mr. VANCE. I think the challenge is that a co-op or a municipal utility face are very similar to what an investor-owned utility face because they have the same issues in that every time that you move toward a networked piece of equipment you're exposing yourself to potential cybersecurity attacks.

So in Indiana we've been very aware of including our co-ops and our municipal utilities in our conversations on energy security and cybersecurity. They sit on our cybersecurity council established by the governor.

I think one of the important things we are trying to do in Indiana as we continue exercises is to build those relationships so that we know we have those personal connections and when an energy emergency hits we cannot spend hours searching through a binder of 300 pages trying to figure out what to do.

I think to some extent the movie "Ghostbusters" summed it up well when it said, "Who are you going to call?" You have to know

who you're going to call in those situations. We can't spend hours trying to figure it out.

So we've been including our munis and co-ops in our conversations.

Mr. BUCSHON. Are there financial challenges to making sure that your networks and everything are secure that the State helps with or anything?

Mr. VANCE. There's always finding constraints when it comes to infrastructure. But to the best of my knowledge, I am not aware of any specific constraints with munis and co-ops. But we can get back to you on an answer to that.

Mr. BUCSHON. OK. One of the bills we are discussing, and somebody mentioned this a little while ago, Enhancing Grid Security Through Public-Private Partnership Act specifically requires the Secretary of Energy to take different sizes of and regions served by electric utilities into account when administering cybersecurity programs.

Based on your experience in Indiana, what might this look like?

Mr. VANCE. I think that would be something that we'd be very interested to work with DOE on. What that would look like I am not entirely sure, off the top of my head.

Mr. BUCSHON. Anybody have any comments on any of this stuff? No?

Good. I yield back, Mr. Chairman.

Mr. WALBERG. I thank the gentleman.

Seeing no one else on the panel, I recognize myself for 5 minutes. Thanks to the panel for being here.

Mr. Aaronson and Mr. Vance, I asked some questions to our DOE panel earlier and I would appreciate hearing your answers to them as well. I appreciate the secretary's efforts to elevate the agency's leadership on emergency and cybersecurity functions and I believe they are commendable. But I would like to see DOE leadership continue under future administrations, as I mentioned. Do you think it would help to codify DOE's Assistant Secretary functions in the DOE organization chart?

Either one—Mr. Vance or Mr. Aaronson.

Mr. VANCE. From our perspective, I would have to discuss with my other members of NASEO before I could make a statement one way or the other.

But I would defer to DOE on that.

Mr. WALBERG. OK. Mr. Aaronson.

Mr. AARONSON. I would just simply say I see no problem with that. I think it could be useful, and to Mr. McNerney's question also, I think anything that provides accountability, that elevates something not just within the organization but then visibility as a Senate-confirmed position and across the various verticals within the department that acknowledges these intersector relationships between electric, gas, and other generating capabilities, and then I think anything that can get more resources.

I don't want to be dismissive of your question, Mr. McNerney. I think anything that—more resources so we can do some of these partnerships more, better, faster, and focus on all of the things that are happening in this—with respect to security in the sector is

going to be valuable. So I think codifying it, elevating it, funding it, supporting it are all good outcomes.

Mr. WALBERG. OK. Let me ask, do you believe that elevating the cybersecurity functions to the Senate-confirmed Assistant Secretary level is a positive? Is it necessary?

Mr. AARONSON. I will leave that to policy makers on that, sir. I think it's a positive development though, certainly.

Mr. WALBERG. OK.

Mr. Aaronson, one of the bills we are discussing today is the Enhancing Grid Security Through Public-Private Partnership Act, which directs DOE to provide cybersecurity training and technical assistance for electric utilities that have fewer available resources due to size or region.

The legislation builds upon the existing public-private partnership between DOE, the electric cooperatives, and power utilities.

Could you explain for us the challenges facing certain electric utilities in improving the cybersecurity of their assets?

Mr. AARONSON. Sure. So, again, I would point everybody to the statement by the American Public Power Association and the National Rural Electric Cooperative Association with whom I serve as secretaries on the sector coordinating council with.

So one of the benefits of the sector coordinating council is that we do all come together with common cause, whether they are large investor-owns, smaller investor-owns, cooperatives, municipals, Canadians, independent power generators, the nuclear sector, gas, and on and on and on. So we work really well together on these issues, again, of sort of mutual concern with respect to protection of our infrastructure.

With respect to challenges among the smaller entities, there are workforce challenges. There is the ability to ingest intelligence. There is the ability to implement some of the good information that is coming out of the government and some of the mitigation measures that are recommended. And so anything that we can do as a community—again, whole of community so that it is a rising tide that lifts all boats—ultimately helps all of the infrastructure that we own and operate together.

So we are very supportive of that particular provision for our co-op and municipal brothers and sisters but also for some of other smaller entities that are going to need help implementing the things you all recommend.

Mr. WALBERG. So this Section 2 of H.R. 5240, the Enhancing Grid Security Through Public-Private Partnerships Act, does that strengthen and further these existing public-private partnerships?

Mr. AARONSON. I think it does.

Mr. WALBERG. OK.

Thank you. The gentleman from New York is here, my friend, and we recognize you for 5 minutes for questioning.

Mr. TONKO. Thank you, Mr. Chair, and thank you to our witnesses for being here this afternoon.

Mr. Aaronson, the utility industry has a long tradition and culture of mutual assistance. When a disaster strikes, everyone responds, and I know there are still crews from New York working in Puerto Rico. The industry has a good idea of how to deal with supply disruptions and restorations after a natural disaster. But

cyber is still uncharted territory. When the industry comes together to think about the future of mutual assistance, does that include how you might respond to a cyber incident?

Mr. AARONSON. Very much so.

One of the things that we have done as a sector—and actually I will give a little bit of a timeline because I think it's instructive.

So you will recall the end of 2015 we had both GridEx III, which is a biannual exercise that NERC puts on, and then just a month later there was the attack in Ukraine that had impact on their distribution system. The CEOs of the sector coordinating council got together for a meeting in January of 2016 and asked the question, do we have the surge capacity to deal with either the imagined threats in the GridEx scenario or the real ones that were perceived from the Ukraine scenario? And the answer was sort of, which is never a good answer for chief executives.

And so they told us as the sector coordinating council support staff to go put something together. We put together something known as cyber mutual assistance, and so from that time just a little over 2 years ago we scoped what cyber mutual assistance would look like. We developed a legal structure around it. We developed a play book. We exercised it. We've utilized it, and now 142 companies representing nearly 80 percent of all customers in North America have a company that is a member of the cyber mutual assistance program.

It's in its very nascent stages. Traditional mutual assistance has been around for more than 80 years. But it is a platform that we can begin to surge and support each other in the eventuality of a cyberattack.

Mr. TONKO. And in that collaboration, are there any differences that you would cite that they could make a distinction from the regular emergency planning and response efforts?

Mr. AARONSON. It is in some ways very similar in that the goal is to restore power and one of the things I tell people is the best way to not have cyber vulnerabilities is to not have cyber infrastructure.

So another thing that we are pursuing is to actually be able to operate in a degraded state manually, which is something Ukrainians were able to do and, again, which we have some capacity to do but are going to develop even more so.

With respect to the differences between traditional and cyber mutual assistance, the first one is the obvious one. You're not going to have bucket trucks of cyber linemen driving down the highway to the affected area. But there is the capacity to support each other remotely. There are things that can be done to develop both information sharing in the event of these attacks and the sharing of equipment and the bringing in of noncompromised equipment to support the company that may have had equipment compromised.

Last is with storms, you see them coming and they are regional. And so companies from all over North America will descend, and did certainly this last year, on the affected region. Cyber doesn't know boundaries like that and so that is a consideration for how do you respond—do I want to send my people into a company that's been impacted when I may be next, and that is something that the cyber mutual assistance program is contemplating and addressing.

Mr. TONKO. OK. Thank you very much.

And Mr. Vance, a common theme we are hearing today is how partnerships—those between utilities and between different levels of government—are critical to ensuring that our electric system is reliable, resilient, and prepared for the worst.

Can you give us a sense of the level of cyber expertise at the state and local levels?

Mr. VANCE. We have a number of folks at our Office of Technology who are the co-coordinators of our cybersecurity council who are spending their time on cybersecurity in coordination with our Department of Homeland Security, our Utility Regulatory Commission, and a number of folks across state government.

So we do have some folks who are focused specifically on the cyber issues. This is a relatively recent thing. I think it started in 2016 but it's something we are trying to get up to speed as soon as we possibly can.

Mr. TONKO. Thank you. And your testimony mentioned the importance of a robust state energy security program. What kind of services and resources can DOE provide to our given states?

Mr. VANCE. I think that's something that can be defined as we explore this more. But the first things off the top of my head are more training and exercise.

A lot of this planning and exercise activities—for example, the exercise we did in Rhode Island that mapped a cyberattack on top of a natural disaster—is something that was a very useful exercise, bringing people together and go through these issues and also put a face to who some of these people were at utilities, at DOE, at the states.

So I think more exercise and opportunities to plan regionally are really helpful as well.

Mr. TONKO. Thank you very much.

And seeing that I have no time remaining, I yield back, Mr. Chair.

Mr. WALBERG. I thank the gentleman.

Seeing there are no further members wishing to ask questions, I would like to thank all of our witnesses again for being here today and for the insights you shared with us and considering our questions.

Before we conclude, I would like to ask for unanimous consent to submit the following documents for the record: Number one, a statement from the American Public Power Association and the National Rural Electric Cooperative Association; a cybersecurity update letter from the American Public Power Association; a letter to Department of Energy Secretary Perry; a response letter from the Department of Energy Secretary Perry; a statement from Siemens Energy.

[The information appears at the conclusion of the hearing.]

Mr. WALBERG. And pursuant to committee rules, I remind members that they have 10 business days to submit additional questions for the record and I ask that witnesses submit their response within 10 business days upon receipt of the questions.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 1:04 p.m., the committee was adjourned.]

[Material submitted for inclusion in the record follows:]





Statement for the Record by the

AMERICAN PUBLIC POWER ASSOCIATION (APPA) and the

NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION (NRECA)

Submitted to the

House Energy & Commerce Committee, Subcommittee on Energy

For the March 14, 2018, Hearing:

"DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response"

The American Public Power Association (APPA) and the National Rural Electric Cooperative Association (NRECA) appreciate the opportunity to submit a statement for the record for the House Energy & Commerce Committee's Subcommittee on Energy hearing entitled, "DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response." APPA and NRECA support and agree with the testimony of Scott Aaronson of the Edison Electric Institute.

APPA is the national service organization for not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. Public power utilities account for over 15 percent of all kilowatt-hour sales to over 49 million customers in every state but Hawaii. NRECA is the national service organization representing the national interests of cooperative electric utilities and the consumers they serve. More than 900 not-for-profit rural electric utilities provide electric energy to over 42 million people in 47 states, or 12 percent of electric customers nationwide.

H.R. 5240, The Enhancing Grid Security through Public-Private Partnerships Act

H.R. 5240 directs the Secretary of Energy to establish a program to facilitate and encourage public-private partnerships to promote and advance the physical and cybersecurity of electric utilities. The Secretary of Energy is directed to carry out a program to (1) develop and provide for voluntary implementation of maturity models, self-assessments, and auditing methods for assessing the physical security and cyber security of electric utilities; (2) provide training to electric utilities to address and mitigate cybersecurity supply chain management risks; and (3) increase opportunities for sharing best practices and data collection with the electric sector. In carrying out this program, the Secretary is required to take into consideration different sizes of electric utilities and the regions they serve and to prioritize electric utilities with fewer available resources due to size or region.

H.R. 5240 is modeled after an existing, successful public-private partnership between DOE, APPA, and NRECA to bring greater resources, training, and tools for cyber and physical security to small- and medium-sized electric utilities. DOE's "Improving the Cyber and Physical Security Posture of the Electric Sector" initiative, which is funded by the Office of Electricity Delivery and Energy Reliability's Cybersecurity for Energy Delivery Systems program (CEDS), is the only program where DOE and

industry are jointly focused on addressing the unique cybersecurity needs of small- and mid-sized distribution utilities.

APPA/DOE CEDS Agreement

In June 2016, APPA entered into Cooperative Agreement #DE-OE0000811 with DOE to improve the cyber resiliency and cyber security posture of public power utilities. Mid- to small-sized public power utilities often rely on cybersecurity services that are outside of their control due to organizational structures within a city government system. For example, imagine a town where the head of IT must oversee not only the electric utility, but the city's police and fire departments, the city council, and the public works department. This shared services model is valuable for delivering IT services, but it does not cover the cybersecurity risks that need to be addressed at a public power utility. The Cooperative Agreement provided the funding necessary to help APPA better understand the threats facing these utilities, develop tools to help these utilities assess their own status, and develop resources to help keep these utilities secure. Specifically, APPA has focused on five areas: (1) cyber resiliency and security assessments; (2) onsite vulnerability assessments; (3) security training and resource development; (4) deployment of security technologies; and (5) implementation of information sharing mechanisms.[1]

In the first two years of the Cooperative Agreement, more than 400 utilities participated in Cooperative Agreement-related activities. These include development and implementation of a Baseline Assessment Survey; the Cybersecurity Scorecard – a tool that "right-sizes" for smaller utilities the cyber maturity models developed by National Institute of Standards and Technology (NIST) and DOE; table top exercises; and presentations, awareness videos, and written materials. By the end of the second year of the Cooperative Agreement we will have conducted 24 onsite vulnerability assessments. APPA has also begun developing the online platform to host the Cybersecurity Scorecard, which will provide a report of assessed needs along with a roadmap to develop the business model for creating a cybersecurity program at each public power utility.

APPA is developing plans for year three of the Cooperative Agreement, which concentrates on refining these tools, reaching more utilities, and setting the stage for an ongoing cyber security and cyber resiliency effort responsive to the needs of small- and mid-sized public power utilities.

NRECA/DOE CEDS Agreement

NRECA used funding from DOE Cooperative Agreement #DE-OE0000807 in 2016 to create the Rural Cooperative Cybersecurity Capabilities Program (RC3), which assists cooperatives in advancing their cybersecurity posture. RC3 provides cybersecurity training, services, and tools to help members build stronger cyber cybersecurity programs. A major priority of the RC3 Program is developing a self-assessment maturity model to enable small- and mid-sized utilities to assess and benchmark their cybersecurity capabilities, and to build a culture of security within their organization. This effort builds on existing work using the DOE's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), a Risk Mitigation Guide NRECA developed with funding from the Office of Electricity in 2011, and the NIST Cybersecurity Framework. For the past year, NRECA has been field testing this maturity model in a Self-Assessment Research Program. The Self-Assessment Research Program itself works with the executive team of a cooperative and helps each member of that team take a hard look at where their cybersecurity efforts are strong and where they can be improved. Through this program, NRECA has provided intensive two-day cybersecurity training to more than 200 executive level staff at 36 small- and mid-sized cooperatives in 13 states, using the self-assessment to assess their current cybersecurity posture and develop a roadmap to ensure continual improvement.

---

[1] See APPA's *Cybersecurity Program Update* for a summary of Year 1 activities and accomplishments.

As NRECA continues its work with cooperatives, we are already seeing measurable progress. For example, we are documenting improvements in securing network access, strengthening physical security, and integrating cybersecurity awareness into negotiations with third-party vendors. With continued DOE support, NRECA is working to expand this program to more of our members.

The RC3 Program held six Cybersecurity Summits in 2017 that provided staff representing 151 cooperatives cybersecurity training. "Every presentation provided something I could take home to benefit our company," said one attendee. The most valuable aspect of the summits was the opportunity for co-ops to come together and discuss cybersecurity challenges and solutions. With continued support from DOE, NRECA will hold another round of Cybersecurity Summits this year.

In addition, the RC3 Program is developing specialized cybersecurity training resources and programs appropriate for the wide range of cybersecurity expertise that exists within mid- and small-sized utility, creating an information sharing platform for the cooperative community, and increasing access to vulnerability assessment services. Through these efforts, RC3 is helping distribution cooperatives build stronger cybersecurity programs.

Conclusion

Protecting the electric grid from threats that could impact national security and public safety is a responsibility shared by both the government and the electric power sector. Public-private partnerships like those between DOE, APPA, and NRECA are vital to help needed resources reach the smaller utilities in the sector in the most useful manners. We applaud the committee's effort with H.R. 5240 to help ensure these novel programs are maintained and that their impact expands. We look forward to continuing to work with the committee on these issues moving forward.

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

Cybersecurity Program Update



www.PublicPower.org/GridSecurity



Improving Grid Security in Public Power

In June 2016, the American Public Power Association entered into Cooperative Agreement #DE-OE0000811 with the U.S. Department of Energy for a three-year program, with total funding of $7.5 million, to improve the cyber and physical security posture of public power utilities.

In the first year of the program, the Association conducted activities in five areas:

1. Cyber resiliency and security assessments
2. Onsite vulnerability assessments
3. Security training and resource development
4. Deployment of security technologies
5. Implementation of information sharing mechanisms

The Association thanks the more than 150 public power utilities that participated in the program (see list in Appendix A) during year 1 for sharing their expertise.

This update summarizes the Association's accomplishments in year 1, discusses activities for years 2 and 3, and outlines program benefits to public power utilities.

Cyber Resiliency and Security Assessments

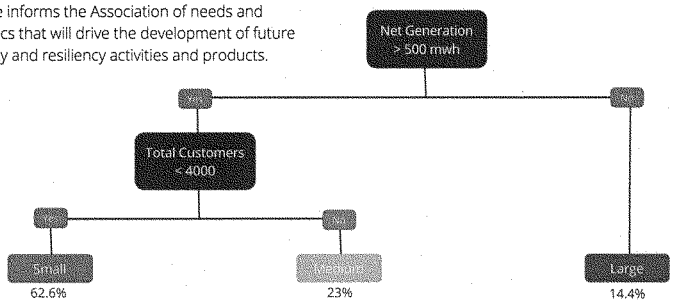
Research and Analysis

To assess the cyber maturity of public power utilities, the Association conducted research to define member demographics and general security capabilities and resiliency. The research results and analysis are captured in the Public Power Baseline Assessment. Criteria were established to categorize small, medium, and large public power utilities for the cybersecurity work.

The baseline informs the Association of needs and demographics that will drive the development of future cybersecurity and resiliency activities and products.

NEXT STEPS

The Association will conduct additional assessments of the security capabilities and needs of small and medium sized public power utilities.



Cluster	Utilities	Customer Count	NERC Registered Entities
Large	290	0 to 1,458,330; Avg. = 49,575	157
Medium	461	4,015 to 408,411; Avg. = 15,156	88
Small	1255	0 to 3,995; Avg. = 1,314	14

Figure 1: Demographics of public power utilities.
Source: Axio Global, Inc.

Note: North American Electric Reliability Corporation registered entities were assumed to have an existing cyber program in place and were not included in this initial assessment.

Public Power Maturity Model: Cybersecurity Scorecard

During the assessment phase of the program, a quick launch self-assessment tool — the Public Power Cybersecurity Scorecard — was created. The scorecard was modeled after the U.S. Department of Energy's electricity subsector Cybersecurity Capability Maturity Model, or C2M2.

The scorecard is designed for small and medium public power utilities that are just starting to evaluate their cybersecurity program. A self-assessment gives a utility the starting point to address cyber risks and informs utility leadership on cyber risk decisions.

In year 1, the scorecard was tested in a user group, which provided feedback. The scorecard will be further tested in year 2 and be made available online.

The scorecard comprises 14 questions which a utility can answer in 45 minutes — compared to the two-day facilitated session needed to complete the C2M2 model. Answers to the scorecard questions can be incorporated into the C2M2 when a utility is ready to use the model.

The 14 questions in the scorecard address these key areas:

- Cyber asset inventory
- Configuration baseline
- Access control
- Vulnerability management
- Threat management
- Cyber risk management
- Cyber event detection
- Cyber incident response
- Operational resiliency
- Monitoring cyber system activity
- Cyber threat and event information sharing
- Supply chain risk
- Workforce management and cyber security training
- Cybersecurity program management

The scorecard gives public power utilities the ability to determine their general cybersecurity posture without extended time and cost commitments.

NEXT STEPS

The Association will encourage its members to use the scorecard to conduct self-assessments of their cybersecurity posture and will undertake further cybersecurity and resiliency activities, including

- Make the scorecard available online
- Obtain an adequate sample size for each utility category to improve benchmarking
- Update the baseline to reflect scorecard responses
- Target categories for cybersecurity program resources and training, based on scores shared voluntarily
- Create profiles for a public power utility based on its demographic cluster and identification of trends for each group
- Incorporate the scorecard answers to the C2M2 and provide a target profile recommendation for a mature cybersecurity program

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.



Security Vulnerability Onsite Assessments

During year 1 of the program, the Association conducted 11 in-depth onsite vulnerability assessments and provided detailed security improvement reports to each utility that participated. Common cybersecurity challenges were identified, such as limited documentation of cybersecurity incident history and the physical security of cyber assets, limited cybersecurity staff, and limited cybersecurity policies and procedures. These challenges will be the focus of the Association's security training and resource development in years 2 and 3 of the program.

It is recommended that public power utilities conduct onsite assessments to receive specific recommendations on enhancements to improve its cybersecurity readiness.

NEXT STEPS

In year 2, the Association plans to conduct 11 additional onsite vulnerability assessments.

The Association will also assess and develop the following:

- Logging and monitoring activities, especially where utilities integrate their information technology (IT) and operations technology (OT) logs
- Simplified assessments on the key areas identified in the scorecard
- Action plans with top priorities highlighted
- Trend analysis to inform future resource development



Security Training and Resource Development

Security Training

In year 1, the Association conducted five 2-day, in-person C2M2 facilitated workshops in various regions of the country. In all, the workshops included 124 participants from 41 public power utilities. The workshops trained participants on how to use the C2M2, understand the characteristics of a mature cyber and physical resiliency program, and benchmark the utility's maturity level.

The Association also conducted 14 tabletop exercises for utility executives as well as IT and OT administrators. These exercises focused on sharing threat information and identified some challenges that will be addressed in year 2 of the program.

Cybersecurity classes were held for executives and IT/OT professionals. The classes were developed by three cybersecurity expert trainers.

For executives, the training sessions discussed tools needed to understand the subject matter and help develop the capability to work with internal and external audiences. For IT/OT personnel, the training sessions discussed a particular security domain and provided background theory as well as tools to design and implement a comprehensive cybersecurity program.

The training is intended to elevate executives' understanding of cybersecurity issues so that they can make decisions on security investment and operational needs, and ensure that IT/OT staff are informed about the latest security tools.

During the year 1 training sessions, many public power utilities acknowledged that they would benefit from additional training on identifying cyber risks and developing a cybersecurity program in their organizations.

NEXT STEPS

The Association will explore and develop low-cost training activities including

- Tabletop exercises — focused on major areas identified in the scorecard — at Association and joint action agency meetings
- Cybersecurity awareness, risk assessments, program and policy development, incident response, information sharing, OT environment cybersecurity, and template development
- Strategies to develop the future cybersecurity workforce
- A public power cybersecurity training certification program
- A Cyber Resilience and Security Incident Playbook, addressing roles and responsibilities in case of a security incident
- A public power cybersecurity summit

Resource Development

During the year 1 workshops and tabletop exercises, public power utilities identified the need for various cybersecurity resources. The Association developed these resources to help public power utilities build their cybersecurity programs.

Managed Cybersecurity Service Provider Catalog: The Association evaluated 48 security services and technology providers to ascertain who can best serve public power utilities and developed the Managed Cybersecurity Service Providers Catalog. Utilities can review the products and services — including subscription services — available to address cybersecurity needs.

The Association does not endorse any of the products or services in the catalog. But utilities can use it to:

- Determine and prioritize their cybersecurity needs
- Review vendor profiles and offerings and obtain contact information
- Discuss offerings with providers and determine if the level of security provided is above, below, or level with requirements

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

Security Training and Resource Development

- Gauge the costs of outsourcing cybersecurity to these companies by asking for detailed quotes, including installation fees and recurring costs
- Select providers based on needs and assessments

Videos: Several videos were produced in year 1 to provide general awareness to public power utilities on cybersecurity risks and the Association's cybersecurity program. Videos are available on a program overview, cybersecurity 101, and cyber risk assessment.

Cybersecurity Information Engagement Plan: The Association developed an engagement plan to be used by public power utilities to inform city officials on cybersecurity issues. The plan will help utilities engage with government officials and other key stakeholders on cyber and physical security issues. One key recommendation of this report is to designate a cybersecurity program lead within the utility to champion a cybersecurity program.

eReliablity Tracker and ICE Calculator Integration: The Association offered an 80% discount on 3-year subscriptions to its eReliability tracking service to encourage small public power utilities to leverage this service. The goal was to give the smallest public power utilities the ability to transition from paper reliability records to automated systems.

The Interruption Cost Estimate or ICE Calculator is designed for electric reliability planners at utilities, or other entities that are interested in estimating interruption costs and/or the benefits associated with reliability improvements.

During year 1, the Association developed new algorithms and integrated the ICE Calculator into the eReliability Tracker. Public power utilities can now use their outage history to make cost-based reliability decisions inside the integrated tracker. Utilities can also see how much a cybersecurity attack would cost their customers. This information can be used to educate local government officials, and obtain cybersecurity funding.

With this advanced tool, utilities can increase security awareness, make security investment decisions, and get tools to institute a documented cybersecurity program.

NEXT STEPS

The Association will develop additional resources, including:

- Resources that address the challenges identified in the scorecard and onsite vulnerability assessments
- Advanced reliability and resiliency reporting algorithms incorporated into the eReliability Tracker and ICE Calculator to create predictive resiliency metrics to assess the potential impact of cyber events
- A cyber asset tracker and management platform with a step-by-step guide on how to identify, track, and maintain utility cyber assets
- Research with National Laboratories and universities on the impact of cyber incidents on reliability, resiliency, and costs to inform cyber technology investments
- The Public Power Cyber Resiliency and Security Roadmap outlining strategy and tactics to develop or enhance a cybersecurity program at a public power utility



Deployment of Security Technology

The Association learned that most small and medium-sized utilities rely on the services of a Managed Security Service Provider (MSSP) to address cyber risks. Discounted subscriptions — through an 80 percent cost share funded by the program — were offered to the N-Dimension N-Sentinel subscription service, which is popular among public power utilities.

Many utilities found even this discounted subscription rate to be a hurdle. The Association found that working with joint action agencies elicited a better response then soliciting individual utilities. Although this form of engagement takes longer, it encourages more deployments and the formation of a more robust regional community. Joint action agencies have more of a stake in the long-term success of the MSSP service deployments.

New technologies and services advance a utility's cyber readiness and expand capability without adding new personnel. However, the utility must maintain the system and act on the cyber threat notifications.

NEXT STEPS

The Association will continue to research and deploy new technologies and services that will help address cyber risk for public power utilities, including:

- Contracting with joint action agencies for MSSP subscription services
- Developing best practices for deployment by exploring the correlation between utility characteristics and demographics (size, number of IT staff employed, and governance or decision-making structure), and delays in the deployment process
- Leveraging controlled social media platforms to develop a sense of community and engagement to discuss the MSSP threat information and utility actions

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.



Implementation of information sharing mechanisms

Secure Information Sharing Mechanisms

Public power utilities, regardless of size, must have easy access to actionable cyber threat information. The Association analyzed the current model of cyber threat sharing through the Electricity Information Sharing and Analysis Center and found that public power utilities need to distill these threat feeds into actionable information.

To overcome this challenge, the Association evaluated information sharing methodologies and technologies that will improve cyber and physical resiliency and security within public power utilities. As part of this research, the Association worked with joint action agencies to encourage all public power utilities to sign up with the E-ISAC.

The research found that

- Public power utilities with the capability to start gathering security event logs should install a Security Event and Information Management (SEIM) solution. At a minimum, security logs should be correlated across the utility.
- Joint action agencies could serve as a centralized repository for their utilities' security logs through the SEIM tools.
- Joint action agencies can filter threat information from E-ISAC to be more actionable for their member utilities.
- When adopting SEIM solutions, it is critical to require the use of standard threat information sharing protocols such as the Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) protocol to ensure interoperability among key stakeholders.
- MSSPs providing SEIM solutions to public power utilities must be able to integrate with a STIX/TAXII solution to create an end-to-end security event log management and threat information sharing process for the industry.

The Association also developed and submitted recommendations to E-ISAC on how to categorize, assess, disclose, and disseminate threat information that is most useful to public power utilities to avoid future threat information fatigue.

The secure information sharing platforms ensure that public power utilities are not overwhelmed by the deluge of information produced by intelligence sources. Eventually, given the ever-increasing volume of data, threat indicator sharing will need to move to an automated platform.

NEXT STEPS

- Continue research with the National Laboratories and universities to pilot a Public Power Secure Information Clearinghouse tool which can provide better real-time information flow among E-ISAC, the Association, and utilities.
- Evaluate other secure information sharing technologies to integrate automated indicator data.

Information Assurance

The Association researched recommended methodologies, best practices, and technologies to improve information assurance for data-in-motion. It developed webinars, a PowerPoint slide deck, and a report on three case studies of information assurance implementation at small, medium, and large public power utilities.

NEXT STEPS

- The Association will work with joint action agencies to research whether aggregation of smart grid deployments at the agencies can ensure data protection.

Questions? Contact Nathan Mitchell, cybersecurity program manager, at NMitchell@PublicPower.org.

Appendix A
Cybersecurity Program Year 1 Participants

Adrian Public Utilities
Alabama Municipal Electric Authority
ALP Utilities
Alton Municipal Utilities
American Municipal Power, Inc.
Atlantic Municipal Utilities
Barbourville Utility Commission
Barnesville Municipal Utilities
Beaches Energy Services
Benson Municipal Utilities
Berea Municipal Utilities
Beresford Municipal Utilities
Boscobel Utilities
Bountiful Power
Bowling Green Municipal Utilities
Breckenridge Public Utilities
Breese
Brigham City
Bristol TN Essential Services
Brookings Municipal Utilities
Bryan Texas Utilities
Cameron
Carthage Water Electric
Central Municipal Power Agency/Services
Central Nebraska Public Power & Irrigation District
Central Utah Water Conservancy District
Chelan County PUD
Chillicothe
City of Albany
City of Charlevoix
City of Columbia
City of Fallon
City of Fulton
City of Higginsville
City of Lakota
City of Lindsborg
City of Marshall
City of McPherson
City of Memphis
City of Moberly
City of Monett
City of Ocala Electric Utility
City of Olivia
City of Paris Combined Utilities
City of Piqua
City of Purcell
City of Salem Electric Department
City of Seguin
City of Staples
City of Vermillion
City of West Plains
City of Williamstown
Clatskanie People's Utility District
CMUA
Coldwater Board of Public Utilities
Columbus Division of Power
Crisp County Power Commission
CUWCD
Delano Municipal Utilities
Denison Municipal Utilities
Denton Municipal Electric
Detroit Lakes Public Utilities
Electric Cities of Georgia
Electrical District No. 3 of Pinal County
ElectriCities of NC
Energy Northwest
Fairview City
Fallon Municipal Electric System
Fellmore City
Flandreau Municipal Utilities
Florida Municipal Power Agency
FMEA
Fort Pierce Utilities Authority
Frankfort Electric & Water Plant Board
Fulton
Gainesville Regional Utilities
Garland Power & Light
Grand Haven
Great Lakes Utilities
Guam Power Authority
Hannibal BPW
Harlan Municipal Utilities
Harrisonville
Hartley Municipal Utilities
Heartland Consumers Power District
Heber Light & Power

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

Appendix A
Cybersecurity Program Year 1 Participants

Henderson Municipal Power & Light
Hillsboro Electric Utility
HMU
Holland Board of Public Works
Homestead Energy Services
Hopkinsville Electric System
Hurricane City Power
Hyrum City Power
Idaho Falls Power
Illinois Municipal Electric Agency
Independence Power & Light
Indiana Municipal Power Agency
Jackson
Jackson Center Municipal Electric System
Kansas City Board of Public Utilities
Kansas Municipal Utilities
Kaysville City
Kentucky Municipal Power Agency
Kentucky Municipal Utilities Association
Kerrville Public Utility Board
Keys Energy Services
Kirkwood Electric
KMU
LADWP
Lake Park Public Utilities
Lakefield Public Utilities
Lakeland Electric
Lakota Municipal Utilities
Lawrenceburg Municipal Utilities
Lebanon Utilities
Lehi City
Lincoln Electric System
LMUD
Lodi Electric Utility
Logan City
Long Island Power Authority
Loup Power District
Lower Valley Energy
Luverne Municipal Utilities
Madison Municipal Utilities
Madisonville Municipal Utilities
Marshall Municipal Utilities
Marshfield Utilities
Mason County PUD #1
MEAG Power
Melrose Public Utilities
Memphis Light, Gas and Water
MEUW
Michigan Public Power Agency
Michigan South Central Power
Michigan South Central Power Agency
Mid-West Electric Consumers Association
Minnesota Municipal Utilities Association
Missouri Joint Municipal Electric Utility Commission
Missouri Public Utility Alliance
Missouri River Energy Services
Monroe City Power
Moorhead Public Service
Murray City
Murray Electric
MYMEAC
Nebraska City Utilities
Nebraska Public Power District
New London Electric & Water Utility
New Ulm
Nixa Municipal Electric System
North Attleboro
North Branch Municipal Water and Light
Northern California Power Agency
Northern Municipal Power Agency
Norwich Public Utilities
NTUA
NYAPP
Odessa
Oklahoma Municipal Power Authority
Omaha Public Power District
Orange City Municipal Utilities
Owatonna Public Utilities
Owensboro Municipal Utilities
Paducah Power System
Parowan
Paullina Municipal Utilities
Pella Municipal Electric Utility
Pierre Municipal Utilities
Piqua Municipal Power System
Platte River Power Authority

Appendix A
Cybersecurity Program Year 1 Participants

Princeton Electric Plant Board
Remsen Municipal Utilities
Rice Lake Utilities
Riverside Public Utilities
Rochester Public Utilities
Rock Rapids Municipal Utilities
Rolla Municipal Utilities
Russellville Electric Plant Board
Sanborn Municipal Utilities
Santee Cooper
Sauk Centre Public Utilities
SDMEA
SESD
Shelby Municipal Utilities
Sikeston BMU
Sioux Center Municipal Utilities
Southern Minnesota Municipal Power Agency
Southwest Public Power Agency
Springfield
Springville City
St. George City
St. James Public Utility
Utah Associated Municipal Power Systems
Valley City Public Works
Village of Sherburne Municipal Utilities
Washington City
Watertown Municipal Utilities
Waverly Utilities
Weber Basin Water Con
West Memphis
Westbrook Public Utilities
Westerville Electric Division
Willmar Municipal Utilities
Wilson
Woodbine Municipal Light & Power
Worthington Public Utilities
WPPI Energy
Zeeland Board of Public Works

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

2451 Crystal Drive
Suite 1000
Arlington, VA 22202-4804
PublicPower.org

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

January 24, 2018

The Honorable Rick Perry
Secretary
U.S. Department of Energy
1000 Independence Ave. S.W.
Washington, DC 20585

Dear Secretary Perry:

Pursuant to authorities Congress provided in the FAST Act in 2015, the Department of Energy (DOE) is the lead Sector-Specific Agency for cybersecurity for the energy sector.[1] As such, DOE is responsible for coordinating with multiple Federal and State agencies, and collaborating with critical infrastructure owners and operators on activities associated with identifying vulnerabilities and mitigating incidents that may impact the energy sector.

To perform these duties effectively, DOE must account for each interrelated segment of the nation's energy infrastructure, including pipelines, which are subject to an array of other federal authorities. In particular, the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) has cybersecurity responsibilities relating to pipelines. Pipeline safety and regulatory responsibilities are also exercised by the Department of Transportation (DOT) and the Federal Energy Regulatory Commission (FERC). Considering the multiple authorities and agencies involved, we write today to seek additional information to assess the quality of coordination among various federal entities relating to cybersecurity of the nation's pipeline system.

To assist with our evaluation, we ask that you coordinate with DHS and provide Committee staff the latest federal threat assessments concerning pipeline infrastructure and include a staff briefing on those assessments and audit programs. In addition, please schedule a briefing and provide written responses to the following by February 12, 2018:

1. Describe the coordination conducted by DOE with DHS, TSA, DOT, FERC, and any other relevant Federal and State agencies as it relates to cybersecurity of pipeline systems.

[1] P.L. 114-94. Section 61003

2. Describe the collaboration conducted with owners and operators of pipeline systems, including the relevant subsector coordinating councils and Information Sharing and Analysis Centers (ISACs).

3. Describe and provide memoranda of understanding or other agreements between DOE and other agencies that have been developed to ensure full and adequate coverage of pipeline systems relating to federal critical infrastructure responsibilities.

4. Describe the federal resources, including personnel, applied to pipeline cybersecurity and vulnerability assessments and related programs.

5. Describe the number, design, and scope of federal audits or assessments to identify vulnerability and cybersecurity risks in pipeline systems.

6. Describe DOE's specific activity and programs concerning cybersecurity in pipeline systems.

We appreciate your prompt attention to this request. Should you have any questions, please contact Peter Spencer of the Majority Committee staff at (202) 225-2927.

Sincerely,

Greg Walden
Chairman

Fred Upton
Chairman
Subcommittee on Energy

Gregg Harper
Chairman
Subcommittee on Oversight
and Investigations

cc: The Honorable Frank Pallone, Jr., Ranking Member

The Honorable Bobby L. Rush, Ranking Member
Subcommittee on Energy

The Honorable Diana DeGette, Ranking Member
Subcommittee on Oversight and Investigations

The Honorable Elaine L. Chao, Secretary
U.S. Department of Transportation

The Honorable Kirstjen M. Nielsen, Secretary
U.S. Department of Homeland Security

The Secretary of Energy
Washington, DC 20585

March 13, 2018

The Honorable Fred Upton
Chairman, Subcommittee on Energy
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your letter requesting input to assess the quality of coordination among the various Federal entities relating to cybersecurity of the Nation's pipeline system. The Department of Energy (DOE) is providing the attached response to your questions.

America's energy supply is essential to our national and economic security. DOE has a vital role in protecting that supply, and I have no higher priority. DOE serves as the Sector Specific Agency for Energy under Presidential Policy Directive 21 and the lead Federal agency for Emergency Support Function (ESF) #12 – Energy under the National Response Framework. As such, I am in the process of establishing the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to elevate these issues commensurate with the seriousness of the threat. This will better position the Department to continue working closely with industry partners, the Department of Homeland Security, the Department of Transportation, and the Federal Energy Regulatory Commission regarding pipeline security and safety initiatives as they relate to resilience and reliability.

I am pleased to report that DOE and DHS provided a briefing to Committee staff on pipeline cybersecurity issues on March 12, 2018 and we are working with the staff to arrange for a more detailed briefing on federal threat assessments concerning pipeline infrastructure. As you consider cybersecurity issues around the oil and natural gas pipeline network, DOE would like to emphasize the connected nature of our energy system as a feedstock to electric generation facilities, fuel assurance, and overall resilience.

Thank you again for your attention to this important subject. If you have any additional questions, please do not hesitate to contact me or Mr. Marty Dannenfelser, Deputy Assistant Secretary for House Affairs, Office of Congressional and Intergovernmental Affairs, at (202) 586-5450.

Sincerely,

[redacted]

Rick Perry

Enclosure

RESPONSE TO HOUSE ENERGY AND COMMERCE LETTER TO SECRETARY PERRY REGARDING PIPELINE CYBERSECURITY

Question 1: Describe the coordination conducted by DOE with DHS, TSA, DOT, FERC, and any other relevant Federal and State agencies as it relates to cybersecurity of pipeline systems.

As the Nation's top 100 pipelines alone supply nearly 84 percent of the Nation's energy[1], pipelines represent a critical part of North America's energy backbone. A coordinated government approach to the cyber and physical security of pipelines, led by the Department of Energy, is essential to ensuring the safe and reliable flow of energy across the U.S.

As the sector-specific agency for the energy sector, DOE works closely with relevant government agencies and oil and natural gas subsector partners on security and resilience including cybersecurity through mechanisms such as through the Oil and Natural gas Sector Coordinating Council and the Energy Government Coordinating Council. As part of the transportation sector, DHS and the Department of Transportation are the co-lead sector-specific agencies for pipeline cybersecurity. DOE works with the Department of Homeland Security (DHS) National Protection and Programs Directorate, the Transportation Security Administration, the U.S. Coast Guard, the Department of Transportation Pipeline and Hazardous Materials Safety Administration, and the Federal Energy Regulatory Commission regarding pipeline security and safety initiatives as they relate to resilience and reliability. Similar to the electric sector, physical and cybersecurity of crude and petroleum pipelines and liquefied natural gas facilities are critical.

The center of gravity for this partnership is the Energy Government Coordinating Council (EGCC)[2], which is co-chaired by DOE and DHS. Through the EGCC, DOE convenes groups listed above, as well as others such as the Federal Bureau of Investigation (FBI), Office of the Director of National Intelligence (ODNI), and Natural Resources Canada (NRCan) to foster a shared national homeland security strategy as it relates to energy infrastructure. This venue provides a useful coordination mechanism to synchronize various collaborations among relevant Federal agencies.

Question 2: Describe the collaboration conducted with owners and operators of pipeline systems, including the relevant subsector coordinating councils and Information Sharing and Analysis Centers (ISACs).

The oil and natural gas (ONG) subsector is a complex system comprised of different segments, including exploration/production, transmission/midstream, and distribution. The protection and resilience of critical ONG infrastructure requires a strong partnership between industry and the Federal Government. The Oil and Natural Gas Sector Coordinating Council (ONG SCC) serves

[1] https://www.tsa.gov/news/releases/2016/07/11/securing-and-protecting-our-nations-pipelines
[2] https://www.dhs.gov/sites/default/files/publications/Energy-GCC-Charter-2014-508.pdf

as the industry counterpart to the EGCC and represents the interests of the complex ONG system – including pipelines.

Proactive collaboration between DOE and the ONG SCC strengthens the development of ONG security strategies, activities, policy, and communication across the energy sector as well as across the ONG subsector to support the Nation's homeland security mission. The ONG SCC is comprised of ONG owners and operators from 23 trade associations, representing a broad industry-wide network across the United States and Canada from all business units – drilling, exploration, production, processing, refining, service and supply, transmission, distribution, and transportation (including pipeline, marine, motor, and rail). As a key part of the energy sector, the Pipelines Sector Coordinating Council serves a dual function as the ONG SCC's Pipeline Working Group.

DOE facilitates three principal-level meetings between the EGCC and ONG SCC each year to discuss strategies and high-level vision for the public-private partnership. Specific physical and cybersecurity as well as resilience projects and initiatives are identified during each of these meetings, and DOE works with the ONG SCC and other partners where appropriate to carry out these activities.

In addition to regular coordination through the ONG SCC, DOE Office of Electricity Delivery and Energy Reliability (OE) has engaged the energy sector ISACs, including the ONG ISAC and the Downstream Natural Gas (DNG) ISAC. Recognizing the need for improved information sharing both between industry and government and across the energy sector, DOE convenes monthly meetings with the ONG ISAC, DNG ISAC, and Electricity ISAC to share and discuss cyber threat trends in a classified setting.

Should a major event occur, DOE will actively engage with the sector to support a safe and timely response. In carrying out DOE's Emergency Support Function (ESF) #12 and Sector-Specific Agency responsibilities, DOE holds regular coordination calls with the ONG SCC and Electricity Subsector Coordinating Council (ESCC) to ensure shared situational awareness and to identify any unmet needs. Additionally, DOE's energy response team leverages the Energy Information Administration's (EIA) subject matter expertise to increase awareness and analyze the regional and national impacts of actual or potential supply chain disruptions. The coordination between EIA and DOE was identified in the National Petroleum Council's 2014 study on industry and government's storm preparation, response, and recovery activities, and DOE's broad coordination role was further codified in the Fixing America's Surface Transportation (FAST) Act of 2015. Collectively, these activities and DOE's other response efforts ensure that the interagency and the Nation's SLTT governments respond to major events effecting the energy sector in a coordinated and appropriate manner.

DOE has also been working with the oil and gas sector for over 10 years to develop advanced technologies to better protect the Nation's energy infrastructure against malicious cyber activity. To coordinate public and private activities and investments, DOE partnered with the energy sector in 2006 and again in 2011 to develop a roadmap and common vision to design, install, operate, and maintain resilient control systems that can survive a cyber incident while sustaining

critical functions. The oil and gas sector played a key role in developing these strategic documents serving on the Executive Steering Committees to ensure the roadmaps fully addressed the industry's major cybersecurity challenges, priorities, and technology gaps. Oil and gas sector representatives included API, AGA, INGAA, BP, Chevron, and El Paso.

Question 3: Describe and provide memoranda of understanding or other agreements between DOE and other agencies that have been developed to ensure full and adequate coverage of pipeline systems relating to federal critical infrastructure responsibilities.

DOE serves as the Sector Specific Agency for Energy under Presidential Policy Directive 21 and the lead Federal agency for Emergency Support Function (ESF) #12 – Energy under the National Response Framework. DOE has established a productive public-private partnership with government partners and the pipeline industry to secure the transport of oil and natural gas. DOE works with the Department of Homeland Security's National Protection and Programs Directorate Office of Infrastructure Protection, DHS's Transportation Security Administration, DHS's United States Coast Guard , DHS's Infrastructure Security Compliance Division, the Department of Transportation's Pipeline and Hazardous Materials Safety Administration and the Federal Energy Regulatory Commission to streamline pipeline security and safety initiatives as they relate to resilience and reliability. Formal agreements have not been necessary to coordinate among agencies lending greater flexibility to adjust to emerging threats as needed. The Energy Government Coordinating Council provides a useful coordination mechanism to synchronize various collaborations among relevant federal agencies.

Question 4: Describe the federal resources, including personnel, applied to pipeline cybersecurity vulnerability assessments and related programs.

DOE-OE leads DOE's efforts to secure the U.S. energy infrastructure against all hazards through cybersecurity research and development and in activities to prepare for, respond to, and recover from major disruptive energy events. In FY 2017, approximately $79.2 million of DOE-OE's resources (combination of program dollars and Federal staff) were dedicated to help achieve this objective. The work performed by OE was done in collaboration with DOE's Office of Intelligence and Counterintelligence, which is responsible for all intelligence and counterintelligence activities throughout DOE, including nearly 30 intelligence and counterintelligence offices nationwide. Given this close connection with the intelligence community, DOE is uniquely postured to provide targeted threat classified and unclassified information to the ONG subsector.

Additionally, DOE's 17 national laboratories represent an unparalleled asset available to DOE. The national labs possess unique instruments and facilities, many of which are found nowhere else in the world. They address large scale, complex research and development challenges with a multidisciplinary approach that places an emphasis on translating basic science to innovation. Several of these labs are leading the development of unique cybersecurity solutions that can be deployed across the pipeline industry to further improve the sector's cyber posture.

Question 5: Describe the number, design, and scope of federal audits or assessments to identify vulnerability and cybersecurity risks in pipeline systems.

In an effort to support ONG companies – including pipelines – in assessing their cybersecurity posture, DOE developed the Cybersecurity Capability Maturity Model (C2M2) in 2012. The model is a tool that may be used by the company to assess the maturity of its cybersecurity program through focusing on the implementation and management of cybersecurity practices associated with the operation and use of information technology and operational technology (OT) assets and the environments in which they operate. With specialized knowledge of the OT cybersecurity environment, DOE ISER is uniquely qualified to support pipeline companies identify and mitigate cybersecurity vulnerabilities through resources like C2M2.

The C2M2 supports the ongoing development and measurement of cybersecurity capabilities within any organization by enabling these organizations to consistently evaluate and benchmark their cybersecurity capabilities, prioritize actions and investments, and support adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The model accomplishes this by providing a common set of industry-vetted cybersecurity practices, grouped into ten domains and arranged according to maturity level.

Pipeline companies and other energy sector organizations can facilitate their own C2M2 assessments, or can turn to other parties to assist them in the one-day facilitations. Private companies as well as industry trade associations, such as the American Gas Association (AGA), have leveraged the model to provide individual assessments to their customers or members, respectively. AGA has additionally sponsored several regional workshops to guide participating natural gas member utilities of all sizes through the model. As the model is designed to allow individual companies or associations to assess their own systems, it is difficult to accurately capture the number of ONG companies, including pipelines, which have undergone a C2M2 assessment.

Several of these companies are now in turn participating in DOE's ongoing efforts to update C2M2 to reflect evolving industry best practices and other updates, including the release of a revised NIST Cybersecurity Framework.

Question 6: Describe DOE's specific activity and programs concerning cybersecurity in pipeline systems.

In addition to the work with the ONG SCC, C2M2, energy sector ISACs, and others previously mentioned, DOE has developed a hands-on workshop for energy sector owners and operators to walk through a simulated cyber-attack on energy control systems. This workshop, called "Cyber Strike," leverages lessons learned from the 2015 and 2016 attacks on Ukraine's electric system to better equip U.S. energy companies with the skills to identify and mitigate similar threats. In 2017, DOE partnered with AGA to deliver a version of this training for over 50 of AGA's natural gas utility representatives. DOE currently has six additional workshops planned for 2018 and is developing additional modules targeted for the ONG audience.

DOE hosts an annual Cyber Defense Competition to address the cybersecurity capability gap. Collegiate student teams engage in interactive, scenario-based events to exercise cybersecurity methods, practices, strategy, policy, and ethics, all focused on the energy sector. The scenario for this year's competition, which takes place on April 6, focuses on the interdependencies between natural gas delivery and electric generation. DOE has engaged with AGA and the Interstate Natural Gas Association of America (INGAA) to facilitate engagement between these talented students and natural gas companies.

DOE also works with the trade associations of the ONG SCC to provide classified threat briefings for cleared sector representatives. Through its ties with the intelligence community, DOE regularly delivers briefings related to emerging cyber and physical threats to energy infrastructure. Additionally, in recognizing the need to explore new ways to improve appropriate access to classified threat information, DOE is conducting a pilot of the Government's Secure Video Teleconference (SVTC) capabilities. This goal of this pilot is to exercise DOE's ability to remotely convene a classified threat briefing for cleared energy sector industry representatives, and reduce the barriers to providing them with the information needed to protect their systems.

Since 2010, DOE has utilized the energy sector cybersecurity roadmaps to guide investments of over $200 million in cost-shared R&D to support the oil and gas sector in building resilient energy control systems. Some major accomplishments include:

Artificial Diversity and Defense Security (ADDSec) – Chevron, Washington Gas Energy Systems and SEL, Inc, partnered with Sandia National Laboratory to develop technologies that allow the traditionally static control system to reconfigure itself unpredictably and thereby impede adversarial reconnaissance by making the control system difficult to map – a critical step toward attack planning. If the adversary does succeed in staging a cyber-attack, the control system can automatically reconfigure to sustain critical functions during the cyber-incident.

Role-Based Access Control (RBAC) - Honeywell developed the RBAC technology for the Experion® Process Knowledge System product suite, an energy delivery control system used extensively within the oil and gas industry. RBAC limits user access to the least needed to perform a given task, which helps reduce the risk of unauthorized access, including inside-threats. This technology accounts for roles that are specific to energy delivery operations, for instance, access required for different operating modes, such as normal, start-up, shut-down, and emergency operations. Partners included Idaho National Laboratory (INL) and the University of Illinois at Urbana-Champaign.

Academic-industry Consortia - DOE partnered with DHS to fund the University of Illinois "Cyber Resilient Energy Delivery Consortium" and the University of Arkansas "Cybersecurity Center for Secure Evolvable Energy Delivery Systems" projects. These multiyear consortiums bring together computer scientists and control system engineers guided by industry advisory boards to develop the foundational science and engineering approaches to enhance oil and gas sector cybersecurity and resiliency.

Vulnerability Analysis of Energy Delivery Control Systems – Idaho National Laboratory conducted test bed assessments of more than seven supervisory control and data acquisition

(SCADA) systems widely used in the energy sector. The resulting report describes common vulnerabilities found in the assessments. The vulnerabilities described in this report were routinely discovered in SCADA assessments using a variety of typical attack methods to manipulate or disrupt system operations. The report was designed to provide recommendations to the SCADA vendor and/or owner to identify and reduce the risk of the associated vulnerabilities in their systems.

Cybersecurity Procurement Language for Energy Delivery Systems - designed to provide baseline cybersecurity procurement language for control systems commonly used in the energy sector including: components of energy delivery systems (e.g., programmable logic controllers, digital relays, or remote terminal units), SCADA systems, and networked energy delivery systems (e.g., a natural gas pumping station). Widespread use of common procurement language can greatly enhance the security of the energy sector supply chain as well as lower life-cycle costs by encouraging vendors to build-in security during the design phase.

Hearing of U.S. House Committee on Energy and Commerce
Subcommittee on Cybersecurity and Emergency Response
DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response

Comments by, Leo Simonovich, VP and Global Head,
Industrial Cyber and Digital Security, Siemens Energy
March 14, 2018

Chairman Upton, Ranking Member Rush, and Members of the Subcommittee:

At a time when the risk of cyberattacks against critical infrastructure is growing exponentially, Siemens applauds the Subcommittee's efforts to better understand all aspects of the topic. In the following comments, I will offer my perspective on the topic as the Global Head for Industrial Cybersecurity and Digital Security at Siemens and share a recent initiative that we are leading with partners in the industrial digital economy.

Siemens and the Growing Cyber-threat to Critical Infrastructure
Siemens is a global technology and manufacturing company that has stood for engineering excellence, innovation, quality, reliability and internationality for nearly 170 years. The company has more than 350,000 employees worldwide in more than 190 countries. In the United States, we employ more than 50,000 people and operate more than 60 manufacturing sites. We supply products and solutions to customers across the entire energy value chain, from oil and gas fields, to the electrical grid, to power generation facilities and transportation infrastructure—along with the software solutions that make it all possible. Siemens has approximately 1,200 cybersecurity experts on staff worldwide, including researchers who continuously challenge the security of our own systems and products before they are sold to customers. Cybersecurity is far from a new topic at Siemens: The first IT Security team at Siemens was established in 1986.

With more than one million devices already connected to our MindSphere Internet-of-Things (IoT) platform, we have first-hand experience with cybersecurity challenges in the age of Industrial IoT. Siemens was the first company to have security integrated in all phases of its industrial product development lifecycle and to be certified by TÜV Süd for this purpose. We also have experience in securing industrial sites by assessing security risks and implementing security measures for our customers based on the IEC62443 standards and Holistic Security Concepts.

Given our deep domain know-how in cybersecurity and the energy sector, Siemens is uniquely positioned to help our customers, governments and society as a whole deal with cyber-threats to critical energy infrastructure. We understand that the stakes have never been higher when it comes to cybersecurity for critical infrastructure—particularly energy systems. In fact, among all industries, energy is the most attacked, and the probability that any energy organization will suffer a cyber-attack is nearly 100%. The number of cyberattacks worldwide continues to grow, with operational technology (OT) becoming a growing target. According to a recent study conducted by the Ponemon Institute, OT cyberattacks now comprise 30 percent of all attacks, with a major impact on productivity, uptime, efficiency and safety. With the rise of cloud, mobile and IoT and now the convergence of IT with OT, critical systems are increasingly

vulnerable to aggressive adversaries and attacks.[1]

This comes at a time when artificial intelligence and big data analytics are revolutionizing the economy, including the energy sector. Billions of devices are being connected by IoT platforms and interacting on a new level and scale. This portends tremendous opportunities for our economy, but with this opportunity comes increased exposure to malicious cyber-attacks.

Fortunately, we also know from the Ponemon study and working with our customers that energy companies recognize that they have a shared concern when it comes to cyber readiness. For example, U.S. oil and gas companies participate in the Oil and Gas Information Sharing and Analysis Center, which collects and synthesizes information and turns it into actionable data about common threats. There is also broad recognition at the corporate board level to address this imperative, reflected in increased cybersecurity spending at these companies. Clearly, there is ample need for collaboration and co-creation to address cybersecurity in the energy sector.

Cybersecurity as an Enabler of the Fourth Industrial Revolution

As the Subcommittee knows, cybersecurity is the basic requirement for protecting critical infrastructure, sensitive data, and maintaining operations in today's world. This means that cybersecurity is more than just a metaphorical safety-belt: It is a critical factor in the success of the digital economy. People, organizations, and even entire societies all over the world need to rely on trustworthy digital technologies. Yet, we cannot expect people to actively support the digital transformation if it cannot be ensured that their data and networked systems are adequately protected according to the current state-of-the-art.

That is why digitalization and cybersecurity are two sides of the same coin and must evolve in parallel. If either one is to work properly, they both have to function seamlessly. That is especially true in an era when digitalization is moving into every area of life. Defects or even outages in the systems that control and network our homes, our hospitals, our factories, our power grids – in fact our entire infrastructure – could have appalling consequences. Modern standards for cybersecurity are an essential prerequisite for people to trust our digitalized world – and it is essential to earn that trust, because digitalization is the linchpin for the future success and prosperity of us all.

This risk can be managed with smart collaboration between industry and government. Our society can and must embrace this digital transformation, or "fourth industrial revolution" as it is often called. People and organizations have to trust digital technologies to be safe and secure; otherwise they cannot accept and embrace the digital transformation. Digitalization and cybersecurity must evolve hand in hand.

To keep pace with continuous advances in the market as well as threats from the criminal world, companies and governments must join forces and take decisive actions. This means making every effort to protect the data and assets of individuals and businesses; preventing damage from people, businesses and infrastructure; and building a reliable basis for trust in a connected and

[1] "The State of Cybersecurity in the Oil and Gas Industry: United States" Sponsored by Siemens and independently conducted by Ponemon Institute LLC.

digital world. Creating a holistic basis of trust can't be achieved by a single company or entity; it must be the result of close collaboration at all levels of society.

A New Charter of Trust for the Digital Economy
Recently, Siemens—along with partners representing some of the largest companies in nearly every sector of the digital economy—committed itself to ten principles to ensure the highest possible level of cybersecurity as this digital transformation unfolds. The partners outlined the key factors we consider essential for establishing a new "charter of trust" between society, governments, business partners and customers. The principles of the charter are listed below. They represent what leaders in the private sector can do to "raise the bar" on cybersecurity across the entire digital economy. As you read the charter, you will notice an overarching theme is a commitment to work collaboratively with governments to address this challenge so that our society can realize the benefits of digitalization. Our company is eager to work with the Subcommittee to share our experience and vision in building greater trust in the digital economy.

Principles for a New Charter of Trust

1. **Ownership for cyber and IT security**: Anchor the responsibility for cybersecurity at the highest governmental and business levels, designating ministries and CISOs; establish clear measures and targets as well as the right mindset throughout organizations –"It is everyone's task".

2. **Responsibility throughout the digital supply chain**: Companies –and if necessary - governments must establish risk-based rules for adequate protection across all IoT layers with clearly defined, mandatory requirements. Ensuring confidentiality, authenticity, integrity and availability by setting baseline standards, such as:

    a. **Identity & access management:** Connected devices must have a secure identity and safeguarding measures that allow only authorized users and devices to use them.

    b. **Encryption:** Connected devices must ensure confidentiality for data storage and transmission purposes, whenever appropriate.

    c. **Continuous protection:** Companies must offer updates, upgrades and patches during a reasonable lifecycle for their products, systems and services via a secure update mechanism.

3. **Security-by-default**: Adopt the highest appropriate level of security and data protection and ensure it is pre-configured into the design of products, functionalities, processes, technologies, operations, architectures and business models.

4. **User-centricity**: Serve as a trusted partner along a reasonable lifecycle –providing products, systems and services as well as guidance based on the customer's cybersecurity needs, impacts and risks.

5. **Innovation and co-creation**: Combine domain know-how and deepen a joint understanding between firms and policymakers on cybersecurity requirements and rules

to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage Public Private Partnerships

6. **Education**: Include dedicated cybersecurity courses in school curriculum, as degree courses in university, professional education and training to lead the transformation of skills and job profiles for the future.
7. **Certification for critical infrastructure and solutions**: Companies –and if necessary - governments must establish mandatory independent third-party certification for critical infrastructure and critical IoT solutions (based on future-proof definitions including e.g. where lives are at risk).
8. **Transparency and response**: Participate in an industrial cybersecurity network to share new insights and exchange early warnings; report incidents beyond today's practice which is focusing on critical infrastructure.
9. **Regulatory framework** : Promote multilateral collaboration in regulation and standardization to set a level playing field matching the global reach of WTO; inclusion of rules for cybersecurity into Free Trade Agreements(FTAs).
10. **Joint initiatives**: Drive joint initiatives including all relevant stakeholders to implement the above principles in the various parts of the digital world without undue delay.

You can learn more about the Charter of Trust at www.charter-of-trust.com. Thank you again for your interest in this topic and willingness to consider Siemens's views.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

April 5, 2018

The Honorable Mark Menezes
Under Secretary
U.S. Department of Energy
1000 Independence Avenue, S.W.
Washington, DC 20585

Dear Mr. Menezes:

Thank you for appearing before the Subcommittee on Energy March 14, 2018, to testify at the hearing entitled "DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. Also attached are Member requests made during the hearing.

To facilitate the printing of the hearing record, please respond to these questions and requests with a transmittal letter by the close of business on Thursday, April 19, 2018. Your responses should be mailed to Kelly Collins, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to kelly.collins@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittees.

Sincerely,



Fred Upton
Chairman
Subcommittee on Energy

cc: The Honorable Bobby L. Rush, Ranking Member, Subcommittee on Energy

Attachments

COMMITTEE ON ENERGY AND COMMERCE
Questions for the Record Responses from Under Secretary for Energy Mark Menezes
DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response."
March 14, 2014

QUESTIONS FROM CHAIRMAN UPTON

Q1. During your appearance before us in January, you mentioned that expectations for DOE's emergency response exceeded its authorities.

Q1a. From your experience to date, are there some additional tools or authorities for DOE that would help improve the ability of the agency's deployment of resources in an emergency?

A1a. The U.S. energy security and emergency response posture has changed since the formation of the Department. New energy security threats have emerged and it is necessary to ensure that we have updated authorities to reflect our new reality. A key area that could enhance DOE capabilities to support security and resilience within the energy sector includes a Federal energy infrastructure prioritization and risk management framework through state and local governments, territories, and tribes to utilize during a multi-state catastrophic incident and to enable strategic investment and programs with energy assurance plans.

Q1b. Was DOE fully prepared to respond effectively to FEMA task orders during the response to the three hurricanes this past year? What can be done to enhance that response?

A1b. Regarding the hurricanes in the contiguous United States, the answer is yes. DOE worked with industry and Federal, state, and local partners to facilitate response and recovery activities. As part of the whole-of-government response to these disasters, DOE deployed response personnel to support state emergency operations centers, FEMA Incident Management Assistance Teams, and regional and national response coordination centers, including several weeks of 24-hour coverage at FEMA's National Response Coordination Center in Washington, DC. DOE responders worked with interagency partners as well as with state government and industry representatives to identify information and resource gaps and inform DOE's engagements to support the restoration efforts.

Regarding Puerto Rico, Hurricane Maria presented an unprecedented challenge to the existing response and funding structures and, as such, departments and agencies are assessing continued improvements to adequately prepare for and recover from disasters. After the storm, DOE coordinated and executed recovery efforts with FEMA, the U.S.

Army Corps of Engineers (USACE), and other agencies to restore power. As with the other hurricanes on the mainland, DOE worked with industry, state, territorial and local partners and deployed its own personnel.

As part of the Department's After-Action Review process, DOE is working to better utilize its capabilities and expertise, to include how these capabilities support each phase from pre-incident preparedness, response, damage assessment, and restoration to long-term recovery.

In addition, DOE, FEMA, USACE, and other partners are establishing a standing Interagency Power Task Force that will serve as a standing coordinating element and, during incidents, transition to a crisis planning component of Emergency Support Function #12.

Q2. DOE works with the Department of Homeland Security, TSA and others to ensure protection of pipelines, but these agencies have other priorities as well. Given its responsibilities in the energy sector broadly, Mr. Menezes, should DOE help make sure there is comprehensive and effective coordination over pipeline security?

A2. Under Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, the Department of Homeland Security (DHS) coordinates the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure, including the integration and coordination of Federal cross-sector security and resilience activities. DOE is designated as the sector-specific agency (SSA) for the energy sector. DHS and the Department of Transportation are the Co-SSAs for the transportation sector, which includes pipelines. DOE supports the established model that places responsibility on DHS to lead comprehensive and effective cross-sector coordination related to the safety and security of the Nation's pipelines. DOE works closely with DHS and other interagency partners to support the private sector in its protection efforts. As the SSA for the energy sector, DOE also co-chairs the Oil and Natural Gas Sector Coordinating Council (ONG SCC) and the Energy Sector Government Coordinating Council (EGCC),

which provide a forum for information sharing between all responsible public and private officials. The ONG SCC also includes a Standing Pipeline Working Group.

Q3. The department's role in energy supply emergencies involves working with state emergency offices. Last year, the House passed legislation, HR 3,050, to enhance DOE's support of state energy assurance planning, including cybersecurity support.

Q3a. I understand you are proposing to elevate and consolidate emergency response functions in a new office-an Office of Cybersecurity, Energy Security, and Emergency Response (CESER). Will the functions in this new office include state energy assurance planning?

A3a. Establishing CESER will enable the Department to strengthen its role as the sector-specific agency for the energy sector under PPD 21, support national security responsibilities, and better address natural disasters and emerging threats. By combining Departmental elements that support response and recovery, DOE will enhance the efficiency and effectiveness of the preparedness cycle for the energy sector for all hazards. Forming one office to support energy stakeholder engagement through planning for and responding to incidents while developing supporting capabilities, training, exercising, and evaluating lessons learned will more directly inform research and development efforts in resilience based on lessons learned from operational activities. Additionally, the important subject matter expertise collected supports the critical role energy plays in national security, and the office will work with all energy sector stakeholders, including states for state energy assurance planning.

Q3b. What are your priorities for continuing to assist state level emergency planning?

A3b. DOE supports local and state resilience planning and emergency preparedness. The Department recognizes that the response to energy sector incidents begins at the state, local, tribal, and territorial (SLTT) levels. As such, DOE routinely engages with state and local emergency management offices and energy assurance officials on a myriad of resilience and energy security initiatives that support their resilience planning efforts.

In February 2016, DOE signed an updated Agreement for Enhanced Federal and State Energy Emergency Coordination, Communications, and Information Sharing with the

National Association of State Energy Officials (NASEO), the National Association of Regulatory Utility Commissioners (NARUC), the National Governors Association (NGA), and the National Emergency Management Association (NEMA). The updated agreement lays the groundwork for information sharing amongst SLTT governments around the country to promote energy resilience and accelerated response. As part of this agreement, DOE and state associations provide training and seminars for Energy Assurance Coordinators, and DOE and the states have developed information sharing protocols and processes to streamline response operations, which are tested through drills and exercises.

DOE also hosted the Liberty Eclipse Energy Assurance Exercise in December 2016 in Newport, RI, with nearly 100 exercise participants from 11 states, private industry, the Department of Homeland Security, the Federal Emergency Management Agency, the Department of Defense, and other interagency partners. During the exercise, participants confronted a fictitious cyber incident that cascaded into the physical sector and discussed the challenges of restoring electrical and fuel systems. The exercise resulted in greater awareness of challenges for cyber incident coordination with states and the need for updating state energy assurance plans. DOE plans to do additional exercises like Liberty Eclipse moving forward.

In 2017, OE worked with NASEO to provide technical assistance to twelve states to update their state energy assurance plans. Later this year DOE will be able to test our plans and information sharing at this year's Clear Path exercise, to be held either in or near Washington, DC, in May. Clear Path VI will build on the successful implementation of the second regionally-focused Clear Path exercise, which occurred during May 2017 and was cited by participants from multiple sectors as crucial to preparing for a nearly-identical real-world event only a few months later: Hurricane Harvey. Clear Path VI will also address the desire to conduct more issue-focused exercises that explore coordination between industry, state, and Federal partners in managing interdependencies within and between infrastructure sectors.

COMMITTEE ON ENERGY AND COMMERCE
Questions for the Record Responses from Under Secretary for Energy Mark Menezes
DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response."
March 14, 2014

Q4. You mention in your testimony that, among the activities that are a priority, will be "early stage activities that improve cybersecurity and resilience to harden and evolve critical energy infrastructure."

Q4a. Would you elaborate some examples of research to create next generation systems, components and devices with "cybersecurity built in"?

A4a. DOE's Cybersecurity for Energy Delivery Systems (CEDS) program works to redesign system architectures to enable energy delivery systems (EDS) to adapt and survive a cyber-attack, while decreasing the cyber-attack surface. CEDS research partnerships are advancing tools and technologies that make EDS resilient against malicious manipulation, integrate cybersecurity as part of the design of power system components, and develop red-teaming techniques specifically tailored to EDS cybersecurity technologies. Here are a few examples of CEDS-supported research partnerships:

- The Los Alamos "Quantum Security Modules for the Power Grid" project leverages the groundbreaking capabilities of quantum communications to generate and manage the encryption keys that guarantee data integrity. This research uses quantum physics principles to reveal in real-time an adversarial attempt to intercept the key exchange. Unlike traditional cryptography solutions, quantum keys pair the benefits of higher security with lower computational complexity.

- Schweitzer Engineering Laboratories Inc. partnered with Sandia National Laboratories and Tennessee Valley Authority to develop the Padlock Project security gateway, which detects tampering with field devices, such as those attached to utility poles, and guards against unexpected cyber-activity. The Padlock Project also integrates the results from the exe-Guard project, which provides for deny-by-default cybersecurity.

- Likewise, CEDS supported a research partnership led by ABB called "Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF)," which enables power grid protective devices to

automatically identify and reject any malicious command that would jeopardize grid stability. CODEF runs a quick physics-based simulation to evaluate how a command would affect grid operations, and then ignores all faulty commands, thereby protecting the system against malware, spoofing, and insider attacks. The prototype was demonstrated in transmission-level operations at the Bonneville Power Administration, and the team is now beginning the process to integrate it into the ABB product lines.

Q4b. What are some of the technologies that will improve the ability to share time-critical data with industry?

A4b. To address the need for timely sharing of threat information as well as the rapid recognition of cyber-attacks against critical energy infrastructure and development of mitigations and to reduce the risk of consequences, DOE supports the Cybersecurity Risk Information Sharing Program (CRISP) and Cybersecurity for the Operational Technology Environment (CYOTE) pilot projects to help improve capabilities. The Energy Sector currently doesn't have a comprehensive capability to share time-critical data with industry; CRISP (focused on information technology [IT]) and CYOTE (focused on operational technology [OT]) are working to address this gap. CRISP and CYOTE are advancing data sharing and analysis capabilities within the energy sector's IT environments, as well as in the complex OT environments where threat monitoring and detection is less widespread.

Q4c. To what extent will the new Office of Cybersecurity, Energy Security, and Emergency Response manage this research?

A4c. Protecting America's energy systems from cyber-attacks and other risks is a top national priority for the Department. The establishment of the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) prioritizes robust cybersecurity programs across the energy sector, with a focus on early-stage activities that improve cybersecurity and resilience to harden and evolve critical grid infrastructure.

CESER programs will continue the Office of Electricity Delivery and Energy Reliability's activities to enhance the resilience (the ability to withstand and quickly recover from disruptions and maintain critical function) and security (the ability to protect system assets and critical functions from unauthorized and undesirable actors) of the U.S. energy infrastructure.

Q5. You reference the budget proposals for the Department to invest in cyber incident response teams.

Q5a. What do you mean when you say "cyber incident response teams?"

A5a. The Department is seeking to continue developing our expertise to establish operational technology cyber incident response teams for our Power Marketing Administrations. These teams could augment the Federal leads for cyber incident response at DHS and FBI by providing subject matter expertise when appropriate and requested.

Q5b. How does this fit with Department of Homeland Security incident response teams?

A5b. Under PPD-41: United States Cyber Incident Coordination, DHS, acting through the National Cybersecurity and Communications Integration Center, is the lead agency for asset response. The SSAs will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure. Under this policy, agencies would coordinate to provide unity of effort. DOE cyber incident response teams are an internal resource for Federally owned energy infrastructure and could contribute specialized knowledge, skills, and abilities to account for the unique combination of energy systems and cybersecurity.

Q5c. What role does coordination play to enhance situational awareness so that efforts can be prioritized?

A5c. Coordination is the foundation of all emergency response efforts and also extends to situational awareness as the data about what is occurring comes from a wide set of stakeholders. This coordination highlights issues occurring and the combination of those events leads to prioritization of addressing the issues.

COMMITTEE ON ENERGY AND COMMERCE
Questions for the Record Responses from Under Secretary for Energy Mark Menezes
DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response."
March 14, 2014

Q6. You make reference to CRJSP-the cybersecurity risk information sharing program—would you explain what this does and how much of the industry it covers?

A6. CRISP analyzes near-real-time IT data from utilities using U.S. intelligence to detect cyber-attacks and threats, and delivers alerts and mitigations back to owners and operators. Participating utilities voluntarily share their IT system traffic, which undergoes classified and unclassified analysis to identify threat patterns and attack indicators across the energy industry. Current CRISP participants provide electricity to about 75 percent of the Nation's electric customers.

Q6a. Are there examples where the program has helped address emerging cyber threats?

A6a. Intelligence analysis of CRISP data alerted operators to threat indicators and identified sophisticated intrusions of electric utilities. CRISP reports supported responses to key attacks in 2017 including WannaCry, CrashOverride/Industroyer, and Petya.

Q6b. What is necessary to expand coverage of the program to cover the full electric sector?

A6b. The FY 2019 Budget Request for Cybersecurity for Energy Delivery Systems (CEDS) supports starting development of a significantly improved information sharing model. The effort will capitalize on the existing CRISP experience and concepts, using the latest available technology, architecture, and innovative partnerships with the energy sector to provide the enhanced cyber protection for the energy sector. The resulting next-generation CRISP will address both IT and OT infrastructure as compared to the existing CRISP, which is IT-centric, and CYOTE, which is OT-centric. The vision is to dramatically increase the footprint across the energy sector infrastructure and to gain a higher level of threat detection capability.

Q6c. Does CRISP apply to the oil and gas sector? If so, what is the coverage?

A6c. The CRISP concept, technology and approach is applicable to the oil and gas sector as a voluntary program, but current CRISP members are primarily from the electric sector. Some of these CRISP members do have gas operations and dialogue is underway to enroll oil and natural gas entities as CRISP participants.

COMMITTEE ON ENERGY AND COMMERCE
Questions for the Record Responses from Under Secretary for Energy Mark Menezes
DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response."
March 14, 2014

Q7. Would you also explain in more detail the Cybersecurity for the Operational Technology Environment (CYOTE) pilot project?

A7. The CYOTE pilot will enable OT data sharing and analysis capability with four pilot utilities for the complex OT environment. This complements the existing CRISP program, which focuses on the security of IT networks. As part of this pilot, DOE is examining how we can work with the electricity sector to leverage U.S. intelligence capabilities to prevent, detect, or delay a cyber-attack on utility OT networks that could disrupt power. A primary objective of this pilot will be to assess whether U.S. intelligence analysis can provide actionable information to utilities to take preventive or corrective measures to reduce OT cyber risks.

Q7a. What would the sectors be where this is and can be deployed?

A7a. CYOTE would be deployed across the Nation's energy sector, including their critical energy infrastructure. The energy sector includes the electricity and oil and natural gas subsectors.

Q8. You mention in your testimony that liability protections for the department, labs, and participating energy sector entities would enable the Department to develop its testing capabilities to understand cybersecurity vulnerabilities. Please elaborate why lack of liability protections might impede your ability to perform this mission?

A8. Effective public-private partnerships are vital to the resilience and security of the energy sector. This collaboration will enable the entities involved to research and test key components of the energy sector, locate vulnerabilities, and recommend mitigations. Currently, this collaboration exists due to trust built through longstanding relationships between DOE, the national laboratories, and energy sector entities.

COMMITTEE ON ENERGY AND COMMERCE
Questions for the Record Responses from Under Secretary for Energy Mark Menezes
DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response."
March 14, 2014

QUESTIONS FROM REPRESENTATIVE GRIFFITH

We have a new pipeline that is already being built in my district and a lot of my constituents are concerned about all kinds of issues.

Q1. Are new pipelines with more technology more vulnerable than the older ones already in the ground?

A1. The cybersecurity of the Nation's pipeline infrastructure is of critical importance. The Department of Homeland Security's (DHS's) National Cybersecurity and Communications Integration Center (NCCIC) provides cybersecurity assistance across all critical infrastructure sectors, including pipelines. DHS's Transportation Security Administration (TSA) Pipeline Security Program is designed to enhance the security preparedness of the Nation's hazardous liquid and natural gas pipeline systems and provides recommended cybersecurity guidelines for pipeline operators. The Department of Transportation's (DOT's) Pipeline and Hazardous Materials Safety Administration (PHMSA) regulates pipeline safety pursuant to 49 C.F.R. §§ 100–199, which includes automated and manual safety requirements for regulated pipelines.

For newer pipelines, operational technologies such as supervisory control and data acquisition (SCADA) and Process Control Systems provide robust communication and computing power to operate physical components such as pumps and compressors along the pipelines. The pipeline systems can be vulnerable to cyber threats if security best practices are not followed or properly deployed. Pipeline security guidelines developed by TSA, the Interstate Natural Gas Association of America, and the American Petroleum Institute are being used by pipeline operators to protect both legacy pipelines and those with newer operation control and monitoring technologies.

Q1a. I would also ask that you look at what we can do as far as making sure that the new pipelines have technology in them that let us know if there's an earthquake in the area or a collapse somewhere. The faster people know about it, the faster we can respond.

A1a. Pipeline operators continuously monitor the status of their pipeline networks. SCADA systems provide real-time information and alert operators to any unexpected changes to

the status of the system, including information that can indicate a ground shift. In seismically active areas and areas subject to ground shift, many operators install ground monitors to provide additional real-time data. PHMSA regulates pipeline safety pursuant to 49 C.F.R. §§ 100–199, which includes automated and manual safety requirements for regulated pipelines.

Q2. I think we also need to look, and would like your help, in figuring out if we need to draft legislation to get DOE on the frontend, because I'm not sure FERC is looking into how to make this pipeline less vulnerable.

A2. DOE has established a public-private collaboration with government partners and the pipeline industry to secure the transport of oil and natural gas. DOE, through the Office of Electricity Delivery and Energy Reliability (OE), works with the DHS National Protection and Programs Directorate (NPPD), TSA, U.S. Coast Guard, and Infrastructure Security Compliance Division, as well as the DOT PHMSA and the Federal Energy Regulatory Commission (FERC) to streamline pipeline security and safety initiatives as they relate to resilience and reliability.

Under Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, DHS coordinates the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure, including the integration and coordination of Federal cross-sector security and resilience activities. DOE is designated as the sector-specific agency (SSA) for the energy sector. DHS and DOT are the co-SSAs for the transportation sector, which includes pipelines. DOE supports the established model that places responsibility on DHS to lead comprehensive and effective cross-sector coordination related to the safety and security of the Nation's pipelines. DOE works closely with DHS and other interagency partners to support the private sector in its protection efforts. As the SSA for the energy sector, DOE also co-chairs the Oil and Natural Gas Sector Coordinating Council (ONG SCC) and the Energy Sector Government Coordinating Council (EGCC), which provide a forum for information sharing between all responsible public and private officials. The ONG SCC also includes a Standing Pipeline Working Group.

COMMITTEE ON ENERGY AND COMMERCE
Questions for the Record Responses from Under Secretary for Energy Mark Menezes
DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response."
March 14, 2014

Q2a. Should we move it away from the more occupied area to one that is less likely to be attacked by bad actors or to create a problem, should there be an issue?

A2a. DOE is not part of the regulatory or permitting process to determine the routes of new pipeline systems. The construction of new interstate natural gas pipelines is regulated by FERC. New pipelines may also be subject to regulatory and permitting requirements from the Department of Transportation, Environmental Protection Agency, Department of Interior, and Department of State, as well as state and local requirements.

Q3. Likewise, it would also seem to me that DOE would want to know who had extra capacity in a new pipeline. With the right kind of technology, it could tell instantly whether or not they had the ability to take on more natural gas at a particular moment should there be a failure in some other area, so that we can get that natural gas to where it needs to go by rerouting it possibly. While we're laying this pipe is the time to put in new innovations and thoughts and I'm hoping DOE has some thoughts.

A3. Pipeline owners and operators are generally aware of any unused capacity on their pipelines as well as where additional product may be needed. As the sector specific agency for the energy sector, DOE works with private and public sector partners to ensure that relevant information about regional fuel supplies is shared so that the private sector can make informed decisions.

