

DOE MODERNIZATION: THE OFFICE OF CYBER-
SECURITY, ENERGY SECURITY, AND EMER-
GENCY RESPONSE

HEARING
BEFORE THE
SUBCOMMITTEE ON ENERGY
OF THE
COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES
ONE HUNDRED FIFTEENTH CONGRESS
SECOND SESSION

SEPTEMBER 27, 2018

Serial No. 115-170



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

U.S. GOVERNMENT PUBLISHING OFFICE

36-776 PDF

WASHINGTON : 2019

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

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. Bobby L. Rush, a Representative in Congress from the State of Illinois, opening statement	4
Prepared statement	5
Hon. Greg Walden, a Representative in Congress from the State of Oregon, opening statement	6
Prepared statement	8
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement	9
Prepared statement	10

WITNESS

Karen Evans, Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, Department of Energy	11
Prepared statement	14
Answers to submitted questions ¹	58

SUBMITTED MATERIAL

Report of the Office of Electricity Delivery and Energy Reliability, Depart- ment of Energy, "Multiyear Plan for Energy Sector Cybersecurity," March 2018, submitted by Mr. Upton ²	
Letter of January 24, 2018, from Mr. Walden, et al., to Rick Perry, Secretary, Department of Energy, submitted by Mr. Upton	46
Letter of March 13, 2018, from Rick Perry, Secretary, Department of Energy, to Mr. Walden, submitted by Mr. Upton	49
Letter of September 26, 2018, from American Public Power Association, et al., to Hon. Paul D. Ryan, Speaker of the House of Representatives, sub- mitted by Mr. Upton	56

¹Ms. Evans did not answer submitted questions by the closing of the record.

²The information has been retained in committee files and also is available
at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108725>.

DOE MODERNIZATION: THE OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

THURSDAY, SEPTEMBER 27, 2018

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

The subcommittee met, pursuant to call, at 10:16 a.m., in room 2322, Rayburn House Office Building, Hon. Fred Upton (chairman of the subcommittee) presiding.

Member present: Representatives Upton, Olson, Barton, Shimkus, Latta, McKinley, Griffith, Johnson, Long, Flores, Mullin, Hudson, Walberg, Duncan, Walden (ex officio), Rush, McNerney, Welch, Tonko, Schrader, Kennedy, and Pallone (ex officio).

Staff present: Samantha Bopp, Staff Assistant; Kelly Collins, Legislative Clerk, Energy and Environment; Margaret Tucker Fogarty, Staff Assistant; Jordan Haverly, Policy Coordinator, Environment; Ryan Long, Deputy Staff Director; Mary Martin, Chief Counsel, Energy and Environment; Sarah Matthews, Press Secretary, Energy and Environment; Drew McDowell, Executive Assistant; Brandon Mooney, Deputy Chief Counsel, Energy; Brannon Rains, Staff Assistant; Mark Ratner, Policy Coordinator; Annelise Rickert, Counsel, Energy; Peter Spencer, Senior Professional Staff Member, Energy; Austin Stonebraker, Press Assistant; Madeline Vey, Policy Coordinator, Digital Commerce and Consumer Protection; Hamlin Wade, Special Advisor for External Affairs; Rick Kessler, Minority Senior Advisor and Staff Director, Energy and Environment; John Marshall, Minority Policy Coordinator; Alexander Ratner, Minority Policy Analyst; and Tuley Wright, Minority Policy Advisor, Energy and Environment.

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

Mr. UPTON. Good morning, everybody.

Today's hearing will enable the subcommittee to consider the current setup and plans for the Department of Energy's new Office of Cybersecurity, Energy Security, and Emergency Response. So the CESER office, as we fondly call it, represents an important new element of the Department with a mission to carry out DOE's energy security and energy emergency functions more effectively.

Throughout this Congress, we have identified key features of departmental modernization. These include the need for sufficient

leadership and coordinated attention across the agency's many programs and operations to get ahead of the risks to our modern energy systems.

To underscore this, we move through committee H.R. 5174, the Energy Emergency Leadership Act, which would establish permanent Assistant Secretary-level leadership over emergency response and cybersecurity functions. While enacting this into law takes time, I commend the Secretary of Energy for assigning this level of leadership under his authority and for creating the CESER office earlier this year.

And we are reminded weekly of the urgency for getting this leadership structure up and running smoothly. The risks are varied and complex. We have devastating weather events and other natural hazards that can deprive communities of energy supplies. We are seeing increasing risk to our energy delivery systems by nation states intent on using cyber controls and vulnerabilities to threaten to leave regions of the Nation without power for perhaps weeks at a time. And the work to be better prepared for these risks and to be responsive when incidents occur is as urgent as ever.

There are critical gaps. And we have learned over the past year that energy supplies through pipeline systems to power our bulk electric system may not fully be coordinated within the electric sector to prepare for or respond to cyber or other risks. So I cosponsored H.R. 5175 to help increase DOE's coordination with other agencies and stakeholders on this front.

The pieces are, in fact, coming together for DOE to confront these risks, and we now have a Senate-confirmed head of the CESER office.

And I am pleased to welcome you this morning.

Assistant Secretary Karen Evans was sworn in about a month ago, but her background in government suggests that she brings some necessary skills to improve coordination across the agency and across the Federal Government.

Prior to her recent work leading the U.S. Cyber Challenge, a private-public partnership to reduce the skills gap in cybersecurity, Ms. Evans served as the top information technology official at OMB during the Bush administration, effectively the Federal Government's chief information officer.

Prior to that, she was the Chief Information Officer at DOE, so she knows the Department pretty well. And I would like to learn today what other pieces are necessary to ensure that the new office can fully carry out DOE's responsibilities.

One important area concerns the Department's role as the specific agency for energy-related emergencies, including cybersecurity threats to our energy systems. It would be helpful to understand CESER's role in carrying out this responsibility and how the Assistant Secretary plans to work with other agencies, especially the Department of Homeland Security. What does DOE bring to the table to enhance the overall Federal effort to guard our energy systems against cyber attacks and provide the resources if those attacks are successful?

In addition, what DOE is learning from recent natural disasters, and what additional steps it plans to take to more effectively respond to energy supply disruptions. We heard in an earlier hearing

with the Under Secretary of Energy that the expectations for what DOE can do in emergency exceeds its authorities. Let's discuss what more DOE can do and work to see if we can address the authorities.

Without question, DOE serves on the front lines in the Federal effort to assure critical energy infrastructure protection from all hazards. It provides the technological, operational, and informational expertise to assist stakeholders and other agencies. I want this hearing to help clarify just what DOE is doing to ensure that we can meet the critical mission.

And with that, I yield to the ranking member of the subcommittee and my friend, Mr. Rush.

[The prepared statement of Mr. Upton follows:]

PREPARED STATEMENT OF HON. FRED UPTON

Today's hearing will enable the subcommittee to consider the current setup and plans for the Department of Energy's new Office of Cybersecurity, Energy Security, and Emergency Response.

The CESER office, as we have come to call it, represents an important new element of the Department, with a mission to carry out DOE's energy security and energy emergency functions more effectively.

Throughout this Congress, we have identified key features of Departmental modernization. These include the need for sufficient leadership and coordinated attention across the agency's many programs and operations to get ahead of the risks to our modern energy systems. To underscore this, we moved through committee H.R. 5174, The Energy Emergency Leadership Act, which would establish permanent assistant-secretary-level leadership over emergency response and cybersecurity functions.

While enacting this into law takes time, I commend the Secretary of Energy for assigning this level of leadership, under his authority, and for creating the CESER office this year.

We are reminded weekly of the urgency for getting this leadership structure up and running smoothly. The risks are varied and complex.

We have devastating weather events and other natural hazards that can deprive communities of energy supplies. We are seeing increasing risks to our energy delivery systems by nation states, intent on using cyber controls and vulnerabilities to threaten to leave regions of the Nation without power.

The work to be better prepared for these risks, and to be responsive when incidents occur is as urgent as ever. There are critical gaps. We have learned over the past year that energy supplies through pipeline systems to power our bulk electric system may not be fully coordinated within the electric sector to prepare for or respond to cyber or other risks. I sponsored H.R. 5175, to help increase DOE's coordination with other agencies and stakeholders on this front.

The pieces are coming together for the Department to help DOE confront these risks. We now have a Senate confirmed head of the CESER office. And I'm pleased to welcome her this morning.

Assistant Secretary Karen Evans was sworn in just 1 month ago, but her background in government suggests she brings some necessary skills to improve coordination across the agency, and across the Federal Government.

Prior to her recent work leading the U.S. Cyber Challenge, a public private partnership to reduce the skills gap in cybersecurity, Ms. Evans served as the top information technology official at OMB during the Bush administration—effectively the Federal Government's Chief Information Officer. Prior to that she was Chief Information Officer at DOE, so she knows the department.

I'd like to learn today what other pieces are necessary to ensure the new Office can fully carry out DOE's responsibilities. One important area concerns the Department's role as a sector specific agency for energy-related emergencies, including cybersecurity threats to our energy systems.

It would be helpful to understand CESER's role in carrying out this responsibility, and how the Assistant Secretary plans to work with other agencies, especially the Department of Homeland Security. What does DOE bring to the table to enhance the overall Federal effort to guard our energy systems against cyber attacks and provide the resources if those attacks are successful?

In addition, what DOE is learning from recent natural disasters and what additional steps it plans to take to more effectively respond to energy supply disruptions? We heard in an earlier hearing with the Under Secretary of Energy that the expectations for what DOE can do in an emergency exceed its authorities. Let's discuss what more DOE can do, and work to see if we can address its authorities.

Without question, DOE serves on the front lines in the Federal efforts to assure critical energy infrastructure protection, from all hazards. It provides the technological, operational, and informational expertise to assist stakeholders and other agencies. I'd like this hearing to help clarify just what DOE is doing to ensure it meets this critical mission.

OPENING STATEMENT OF HON. BOBBY L. RUSH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. RUSH. Well, thank you, Mr. Chairman. And I want to thank you for holding this important and timely hearing. And I want to join with you to welcome Assistant Secretary Evans to the Energy Subcommittee for the very first time.

Mr. Chairman, the issue of cybersecurity is always a permanent component of our mindset among members of this subcommittee, as well as the mindset of the American public, as we have heard of many instances of cyber attacks and cyber probes both domestically and abroad over the past few years.

As recently as April, we heard from the FERC Commissioners that our energy grid is constantly being attacked, almost daily, by state actors as well as by other entities who would try to do us harm.

While we have not yet seen widespread outages due to cyber attacks on our electric grid, it is imperative that we take proactive steps to mitigate the risk of these attacks to the maximum extent possible.

It is my hope, Mr. Chairman, and my expectation that installing Assistant Secretary Evans into her new role as head of the Office of Cybersecurity, Energy Security, and Emergency Response, or CESER, will go a long way in achieving that objective.

As you know, Mr. Chairman, I have worked with my colleague Mr. Walberg of Michigan on a bill that codifies the work that DOE has already been conducting when we introduced H.R. 5174, the Energy Emergency Leadership Act, back in March. I want to acknowledge my friend Mr. Walberg for his leadership on this issue and convey my appreciation to all of my colleagues on both sides of the aisle for their support of the legislation that has passed through both the subcommittee and the full committee earlier this spring.

As you know, Mr. Chairman, H.R. 5174 would basically codify this new position by amending Section 203(a) of the Department of Energy Organization Act and establishing the Assistant Secretary position responsible for cybersecurity and emergency response issues.

The newly created Assistant Secretary will have jurisdiction over all energy emergency and security functions related to energy supply, infrastructure, and cybersecurity. This bill will also authorize the new Assistant Secretary to provide DOE technical assistance as well as support and response capabilities with respect to energy security risks to State, local, or Tribal governments upon request.

Mr. Chairman, this legislation, along with the work that DOE is already doing, will go a long way in helping to protect the Nation's electric infrastructure from hackers who would attempt to disrupt our energy grid and cause untold harm to our economy, our daily lives, and to our overall national security.

However, as a letter my office received yesterday, Mr. Chairman, from the American Public Power Association, the Edison Electric Institute, and the National Rural Electric Cooperative Association urges, we must act in a bipartisan way to get this bill and other legislation addressing cybersecurity concerns out of committee and onto the House floor in a timely manner.

As policymakers, we all want to ensure that we are providing DOE and each of the agencies all of the authorities and resources that they need to comprehensively address the cyber threats that our Nation faces.

So, Mr. Chairman, I look forward to this hearing. I look forward to Assistant Secretary Evans' feedback on this bill as well as some of her top priorities in her new position.

With that, Mr. Chairman, I yield back the balance of my time.
[The prepared statement of Mr. Rush follows:]

PREPARED STATEMENT OF HON. BOBBY L. RUSH

Mr. Chairman, I want to thank you for holding this important and timely hearing, and I want to welcome Assistant Secretary Evans to the Energy Subcommittee for the first time.

Mr. Chairman, the issue of cybersecurity is always prevalent in the minds of members of this subcommittee, as well as in the minds of the American public, as we have heard of many instances of cyber attacks and cyber probes, both domestically and abroad, over the past few years.

Mr. Chairman, as recently as April we heard from the FERC Commissioners that our energy grid is constantly being attacked, almost daily, by state actors, as well as by other entities who would try to do us harm.

While we have not yet seen widespread outages due to cyber attacks on our electric grid, it is imperative that we take proactive steps to mitigate the risk of these types of attacks, to the maximum extent possible.

It is my hope and expectation that installing Assistant Secretary Evans into her new role as head of the Office of Cybersecurity, Energy Security, and Emergency Response, or CESER, will go a long way in achieving that objective.

Mr. Chairman, as you know, I have worked with my colleague, Mr. Walberg of Michigan, on a bill to codify some of the work that DOE has already been conducting when we introduced H.R. 5174, the Energy Emergency Leadership Act, back in March.

I want to acknowledge Mr. Walberg for his leadership on this issue and convey my appreciation to all of my colleagues from both sides of the aisle for their support of the legislation as it passed through the both subcommittee and full committee earlier this spring.

As you know, Mr. Chairman, H.R. 5174 would basically codify this new position by amending Section 203(a) of the Department of Energy Organization Act and establishing the Assistant Secretary position responsible for cybersecurity and emergency response issues.

The newly created Assistant Secretary would have jurisdiction over all energy emergency and security functions related to energy supply, infrastructure, and cybersecurity.

Mr. Chairman, this bill would also authorize the new Assistant Secretary to provide DOE technical assistance as well as support and response capabilities with respect to energy security risks to State, local, or Tribal governments upon request.

Mr. Chairman, this legislation, along with the work that DOE is already doing, will go a long way in helping to protect the Nation's electric infrastructure from hackers who would attempt to disrupt our energy grid and cause untold harm to our economy, our daily lives, and to our overall national security.

However, as the letter my office received yesterday from the American Public Power Association, the Edison Electric Institute, and the National Rural Electric Co-

operative Association urges, we must act in a bipartisan way to get this bill and other legislation addressing cybersecurity concerns out of committee and onto the House floor in a timely manner.

As policymakers, we all want to ensure that we are providing DOE and each of the agencies all of the authorities and resources that they need to comprehensively address the cyber threats that our Nation faces.

So, I look forward to hearing from Assistant Secretary Evans on her feedback on this bill, as well as some of her top priorities in this new position.

And with that, I yield back the balance of my time.

Mr. UPTON. Thank you.

The gentleman's time has expired.

The Chair would recognize the chair of the full committee, the gentleman from Oregon, Mr. Walden, for 5 minutes for an opening statement.

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

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

Today's hearing is an important and timely opportunity to learn about Department of Energy's efforts to protect our Nation's energy infrastructure against cyber threats and physical threats.

Whether it is the constant cybersecurity attacks on our Nation's grid or the physical threats of emergencies such as hurricanes, it is DOE's job to ensure our critical energy infrastructure is secure from all hazards and that energy is delivered to consumers throughout all situations.

Now, Secretary Perry has promised to strengthen the Department's cyber and energy security capabilities. And he followed through with the establishment of a new Office of Cybersecurity, Energy Security, and Emergency Response, known as CESER.

I want to welcome our witness today: Assistant Secretary Karen Evans.

Good to have you here.

She was recently confirmed as head of the CESER office. I had the pleasure of speaking with the Secretary last week, when the administration released its National Cybersecurity Strategy.

So it is good to have you here before the committee.

Protecting our Nation's energy infrastructure is critical to maintaining so much of the American way of life. The reliable supply and delivery of energy is vital to our Nation's economy, our national security, and the public health and welfare of our citizens.

With energy systems now massively digitized and interconnected, we know about the new threats and vulnerabilities that have emerged. So it is a whole-of-government effort. But DOE, in particular, must be vigilant and prepared when it comes to ensuring energy access and delivery through cyber threats, physical threats, and emergencies.

DOE has authority and responsibilities for the physical and cybersecurity of energy delivery systems based upon laws that Congress has passed and that the President has passed and Presidential directives. Congress provided DOE with a wide range of emergency response and cybersecurity authorities, beginning with Department of Energy Organization Act and most recently with the Fixing America's Surface Transportation Act.

As the sector-specific agency for energy, Department of Energy has a crucial coordinating role to play in securing our energy infrastructure.

And I know you know that.

Under Assistant Secretary Evans' leadership, we understand that CESER will work to bolster energy-sector cybersecurity preparedness, coordinate cyber incident response and recovery, and accelerate research, development, and demonstration of more resilient energy delivery systems.

When it comes to energy security and emergency response, this new office with analyze infrastructure vulnerabilities, it will recommend preventive measures, and help other agencies prepare for and respond to energy emergencies. CESER's ultimate mission is to mitigate the risk of energy disruptions. So this includes DOE conducting emergency energy operations during a declared emergency or a situation of national security.

So, when it comes to research, when it comes to development, when it comes to the demonstration of more resilient energy delivery systems, Department of Energy's National Laboratories have incredible, tremendous capabilities that can be brought to bear.

Earlier this year, I had the opportunity to visit DOE's Idaho National Lab, INL, which utilizes cybersecurity researchers in collaboration with a broad range of industries and vendors to develop mitigation techniques and tools. INL also has the unique capability to test cyber and physical security applications on a full-scale electric grid.

And as you know, Madam Secretary, we were able to get some of those experts back here to give us on the committee a classified briefing about the threat and their ability to cope with it.

Our Nation's energy infrastructure is largely privately owned and operated. Because of this, DOE works closely with energy-sector owners and operators to better detect risks and mitigate against them. Specifically, CESER collaborates with government and private-sector partners to develop technologies, tools, exercises, and other resources.

One example of DOE's efforts to strengthen public-private partnerships is through its Clear Path IV regional exercise. In April of 2016, DOE hosted the Clear Path IV energy-focused disaster response exercise in my home State of Oregon. The exercise scenario consisted of a magnitude-9.0 earthquake and subsequent tsunami occurring along the 700-mile-long Cascadia Subduction Zone, which, of course, would cause catastrophic damage.

This 2-day event in Portland and Washington, DC, included roughly 200 participants from Federal, State, and local governments as well as the electric sector and oil and gas industries. This exercise provided valuable insights and recommendations for the energy sector on the government and industry sides to help improve policies, plans, and procedures for energy emergencies.

So today's hearing is of the utmost importance because the reliable and uninterrupted flow of energy impacts every aspect of our daily lives. So I look forward to hearing more about DOE's new CESER office and its role in overseeing cybersecurity, energy security, and emergency response for the energy sector.

And, again, thank you for being here.

And, as a caveat, we have another hearing going on downstairs, so I have to bounce back and forth between the two, as other members may have to do.

And with that, Mr. Chairman, I yield back.
[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Today's hearing is an important and timely opportunity to learn more about the Department of Energy's efforts to protect our Nation's energy infrastructure against cyber threat and physical threats. Whether it is the constant cybersecurity attacks on our Nation's grid or the physical threats of emergencies such as hurricanes, it's DOE's job to ensure our critical energy infrastructure is secure from all hazards, and that energy is delivered to consumers throughout these situations.

Secretary Perry promised to strengthen the Department's cyber and energy security capabilities, and he followed through with the establishment of a new office of Cybersecurity, Energy Security, and Emergency Response, known as CESER. I want to welcome our witness today, Assistant Secretary Karen Evans, who was recently confirmed as head of the CESER office. I had the pleasure of speaking with Assistant Secretary Evans last week when the administration released its National Cybersecurity Strategy. I look forward to hearing more from her on this new strategy and CESER's role in it.

Protecting our Nation's energy infrastructure is critical to maintaining so much of the American way of life. The reliable supply and delivery of energy is vital to our Nation's economy, national security, and the public health and welfare of its citizens. With energy systems now massively digitized and interconnected, new threats and vulnerabilities have emerged. It's a whole of government effort, but DOE, in particular, must be vigilant and prepared when it comes to ensuring energy access and delivery through cyber threats, physical threats, and emergency situations.

DOE has authority and responsibilities for the physical and cybersecurity of energy delivery systems based upon laws that Congress has passed and Presidential directives. Congress provided DOE with a wide range of emergency response and cybersecurity authorities, beginning with the Department of Energy Organization Act, and most recently with the Fixing America's Surface Transportation Act (FAST Act).

As the sector-specific agency for the energy, DOE has a crucial coordinating role to play in securing our energy infrastructure. Under Assistant Secretary Evans' leadership, we understand that CESER will work to bolster energy sector cybersecurity preparedness, coordinate cyber incident response and recovery, and accelerate research, development, and demonstration of more resilient energy delivery systems. When it comes to energy security and emergency response, this new office will analyze infrastructure vulnerabilities, recommend preventative measures, and help other agencies prepare for and respond to energy emergencies. CESER's ultimate mission is to mitigate the risk of energy disruptions. This includes DOE conducting emergency energy operations during a declared emergency or situation of national security.

When it comes to research, development, and demonstration of more resilient energy delivery systems, DOE's National Laboratories have tremendous capabilities that can be brought to bear. Earlier this year, I had the opportunity to visit DOE's Idaho National Lab (INL), which utilizes cybersecurity researchers in collaboration with a broad range of industries and vendors to develop mitigation techniques and tools. INL also has a unique capability to test cyber and physical security applications on a full-scale electric grid.

Our Nation's energy infrastructure is largely privately owned and operated; because of this, DOE works closely with energy sector owners and operators to better detect risks and mitigate against them. Specifically, CESER collaborates with government and private sector partners to develop technologies, tools, exercises, and other resources.

One example of DOE's efforts to strengthen public-private partnerships is through its Clear Path IV regional exercise. In April 2016, DOE hosted the Clear Path IV energy-focused disaster response exercise in my home State of Oregon. The exercise scenario consisted of a magnitude 9.0 earthquake and subsequent tsunami occurring along the 700-mile long Cascadia Subduction Zone, causing catastrophic damage. This two-day event in Portland and Washington, DC, included roughly 200 participants from Federal, State, and local governments as well as electric sector and oil

and gas industries participants. This exercise provided valuable insights and recommendations for the energy sector—on the government and industry sides—to improve policies, plans, and procedures for energy emergencies.

Today's hearing is of the utmost importance because the reliable and uninterrupted flow of energy impacts every aspect of our daily lives. I look forward to hearing more about DOE's new CESER office and its role in overseeing cybersecurity, energy security and emergency response for the energy sector.

Mr. UPTON. Thank you.

The Chair would recognize the ranking member of the full committee, Mr. Pallone, for 5 minutes for an opening statement.

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

Mr. PALLONE. Thank you, Chairman Upton.

I want to welcome Assistant Secretary Evans here today and thank the chairman for holding this important hearing. As a committee, we need a deeper analysis of cybersecurity issues at the Department of Energy so members can truly understand the challenges and threats facing our grid and the energy sector as a whole.

I also continue to believe that the committee should hold a closed-door hearing to look at the cybersecurity risks to our electricity grid. There are classified aspects of this issue that can't be discussed at a public hearing like this, and members should have the opportunity to be briefed on this high-level information in order to ensure we are adequately protecting the grid from threats.

To date, the energy sector has done a good job of guarding consumers against losses caused by a cyber or physical attack. But make no mistake, the threats are out there.

In December 2015, Russian state hackers successfully compromised Ukraine's electrical grid, shutting down multiple distribution centers and leaving more than 200,000 residents without power for their lights and heaters. It was a sophisticated and synchronized attack, and it stands as the only recognized cyber attack to successfully take down a power grid. And we owe it to the American people to ask whether anything about that attack could be replicated here, whether it be the electric system, the gas system or dams, or the railways that carry coal to power plants.

Russia hacked the 2016 election, as we know, and it is clear that the Trump administration is not doing enough to prevent Russia from a repeat performance on election day this November.

So what are we doing to prevent them from attacking our energy sector the way they did our electoral process just 2 years ago? What are we doing to stop Russia from hacking our energy systems the way they hacked Ukraine's grid? And how can we make our energy sector more secure and utility workers more vigilant of cyber and physical security threats? And these are important questions that this committee must ask.

So I am pleased we finally have an Assistant Secretary in place at DOE to oversee cyber threats to our electricity grid, but I am seriously concerned that the Trump administration does not have a senior official in the White House taking the lead on our Nation's cyber defense.

In May, President Trump eliminated the job of National Cybersecurity Coordinator, and 4 months later, there is still no senior official in the administration coordinating a response to the Russian cyber attacks. While DOE's role in cybersecurity is clearly important, a national response to these coordinated attacks cannot be done agency by agency.

And the administration must not use cyber threats to our Nation's grid as an excuse to abuse emergency authorities in the name of justifying subsidies to favored industries or companies. Too often, officials in this administration have touted the notion that the natural gas system is somehow unreliable or not able to fuel electricity production in as secure a manner as coal. And all forms of electric generation and their fuels are vulnerable to disruption, whether manmade or due to extreme weather and other natural events. Coal piles freeze, and trains derail. A dam with a line carrying power from a nuclear plant can be every bit as vulnerable as a natural gas pipeline or a wind turbine. And there are serious threats we should be looking to guard against. But we shouldn't be questioning the security of the system just to boost plants that are not economic in the marketplace.

In early May, the committee passed four bipartisan bills to enhance the Department of Energy's authorities with regard to the cybersecurity of our Nation's energy infrastructure. This includes H.R. 5174, the Energy Emergency Leadership Act, sponsored by Ranking Member Rush and Representative Walberg. And this bill would formally authorize a DOE Assistant Secretary position with jurisdiction over all energy emergency and security functions related to energy supply, infrastructure, and cybersecurity.

Mr. Chairman, I am disappointed that these four bipartisan bills have yet to receive consideration before the House, and I would like to work with you to pass these proposals before the end of the 115th Congress.

So, again, I look forward to the discussion today, Mr. Chairman. I yield back.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

I want to welcome Assistant Secretary Evans here today and thank the chairman for holding this important hearing.

As a committee, we need a deeper analysis of cybersecurity issues at the Department of Energy so Members can truly understand the challenges and threats facing our grid and the energy sector as a whole. I also continue to believe that the committee should hold a closed-door hearing to look at the cybersecurity risks to our electricity grid. There are classified aspects of this issue that cannot be discussed in a public hearing like this, and Members deserve the opportunity to be briefed on this high-level information in order to ensure we are adequately protecting the grid from threats.

To date, the energy sector has done a good job of guarding consumers against losses caused by a cyber or physical attack. But make no mistake: The threats are out there.

In December 2015, Russian state hackers successfully compromised Ukraine's electric grid, shutting down multiple distribution centers and leaving more than 200,000 residents without power for their lights and heaters. It was a sophisticated and synchronized attack, and it stands as the only recognized cyber attack to successfully take down a power grid.

We owe it to the American people to ask whether anything about that attack could be replicated here, whether it be the electric system, the gas system, on dams, or on the railways that carry coal to power plants. Russia hacked the 2016 election,

and it's clear that the Trump administration is not doing enough to prevent Russia from a repeat performance on election day this November. So, what are we doing to prevent them from attacking our energy sector the way they did our electoral process 2 years ago? What are we doing today to stop Russia from hacking our energy systems the way they hacked Ukraine's grid? How can we make our energy sector more secure and utility workers more vigilant of cyber and physical security threats? These are important questions that this committee must ask.

I'm pleased we finally have an Assistant Secretary in place at DOE to oversee cyber threats to our electricity grid. But I am seriously concerned that the Trump administration does not have a senior official in the White House taking the lead on our Nation's cyber defense. In May, President Trump eliminated the job of national cybersecurity coordinator. Four months later, there is still no senior official in the administration coordinating a response to the Russian cyber attacks. While DOE's role in cybersecurity is clearly important, a national response to these coordinated attacks cannot be done agency by agency.

And the administration must not use cyber threats to our Nation's grid as an excuse to abuse emergency authorities in the name of justifying subsidies to favored industries or companies. Too often, officials in this administration have touted the notion that the natural gas system is somehow unreliable or not able to fuel electricity production in as secure a manner as coal. All forms of electric generation and their fuels are vulnerable to disruption, whether manmade or due to extreme weather and other natural events. Coal piles freeze, trains derail. A dam or the line carrying power from a nuclear plant can be every bit as vulnerable as a natural gas pipeline or a wind turbine. There are serious threats we should be looking to guard against, but we shouldn't be questioning the security of the system just to boost plants that are not economic in the marketplace.

In early May, the committee passed four bipartisan bills to enhance the Department of Energy's authorities with regard to the cybersecurity of our Nation's energy infrastructure. This includes H.R. 5174, the Energy Emergency Leadership Act, sponsored by Ranking Member Rush and Representative Wahlberg. This bill would formally authorize a DOE Assistant Secretary position with jurisdiction over all energy emergency and security functions related to energy supply, infrastructure, and cybersecurity. Mr. Chairman, I am disappointed that these four bipartisan bills have yet to receive consideration before the House. I would like to work with you to pass these proposals before the end of the 115th Congress.

Again, I look forward to the discussion today and yield back.

Mr. UPTON. Thank you.

The gentleman yields back.

At this point, we are going to hear from our witness.

We appreciate you sending your testimony up. It will be made part of the record in its entirety. And we will let you have 5 minutes to summarize it, at which point we will ask questions. Thank you. Thanks for being here this morning.

STATEMENT OF KAREN EVANS, ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE, DEPARTMENT OF ENERGY

Ms. EVANS. Thank you.

Chairman Upton, Ranking Member Rush, and members of the committee, thank you for the opportunity to discuss the continuing threats facing our national energy infrastructure.

Focusing on cybersecurity, energy security, and resilience of the Nation's energy systems is one of the Secretary's top priorities. By creating the Office of Cybersecurity, Energy Security, and Emergency Response, also known as CESER, the Secretary clearly demonstrated his priorities and his commitment to achieving the administration's goal of energy security and, more broadly, national security.

Our Nation's energy infrastructure has become a primary target for hostile cyber actors, both state-sponsored and private groups.

The frequency, scale, and sophistication of cyber threats have increased, and attacks can be much easier to launch. Cyber incidents have the potential to interrupt energy services, damage highly specialized equipment, and threaten human health and safety.

The recent release of the President's National Cyber Strategy reflects the administration's commitment to protecting America from cyber threats. The Department of Energy plays a vital role in supporting the security of our Nation's critical energy infrastructure. As a result, energy cybersecurity and resilience has emerged as one of the Nation's most important security challenges, and fostering partnerships with public and private stakeholders will be of the utmost importance for me as the Assistant Secretary of CESER.

Recently, CESER demonstrated the emergency response function through multiple weather events. The hurricanes activated our emergency response plan, while we also addressed the overpressurization of a Columbia Gas natural gas pipeline with the Oil and Natural Gas Subsector Coordinating Council that caused multiple explosions and fires at residential locations in Massachusetts.

However, today, I would like to focus my testimony primarily on the cybersecurity function of the office and how CESER will meet the priorities of the administration and work in conjunction with our Federal agencies, State, local, and Tribal governments, our industry partners, and our National Laboratories.

DOE's role in the energy-sector cybersecurity is established in statute and executive action. In 2015, Congress passed the Fixing America's Surface Transportation Act, specifically naming DOE as the sector-specific agency for cybersecurity for the energy sector.

The creation of CESER elevates the Department's focus on the energy infrastructure protection and will enable a more coordinated preparedness and response to cyber and physical threats and natural disasters with the private sector as well as Federal, State, and local government partners. This includes electricity transmission and delivery, oil and natural gas infrastructure, and all forms of generation.

The Secretary has conveyed that he has no higher priority than to support the national security of our Nation's critical energy infrastructure. The formation of the CESER office enhances the Department's ability to dedicate and focus attention on DOE's SSA responsibilities and will provide greater visibility, accountability, and flexibility to better protect our Nation's energy infrastructure and support asset owners, as well as the overall critical infrastructure response framework as overseen by the Department of Homeland Security.

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

I appreciate the opportunity to appear before this committee 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.
[The prepared statement of Ms. Evans follows:]

**Testimony of Assistant Secretary Karen Evans
Office of Cybersecurity, Energy Security, and Emergency Response
U.S. Department of Energy
Before the
Committee on Energy and Commerce
United States House of Representatives
September 27, 2018**

Introduction

Chairman Upton, Ranking Member Rush, and Members of the Committee, thank you for the opportunity to discuss the continuing threats facing our national energy infrastructure. Focusing on cybersecurity, energy security, and the resilience of the Nation's energy systems is one of the Secretary's top priorities. By creating the Office of Cybersecurity, Energy Security, and Emergency Response (CESER), the Secretary clearly demonstrated his priorities and his commitment to achieving the Administration's goal to energy security and, more broadly, national security.

Our Nation's energy infrastructure has become a primary target for hostile cyber actors, both state-sponsored and private groups. The frequency, scale, and sophistication of cyber threats have increased and attacks can be easier to launch. Cyber incidents have the potential to interrupt energy services, damage highly specialized equipment, and threaten human health and safety. The recent release of the President's National Cyber Strategy (NCS) reflects the Administration's commitment to protecting America from cyber threats. The Department of Energy (DOE) plays a vital role in supporting the security of our Nation's critical energy infrastructure. As a result, energy cybersecurity and resilience has emerged as one of the Nation's most important security challenges and fostering partnerships with public and private stakeholders will be of utmost importance for me as the Assistant Secretary of CESER.

Recently, CESER demonstrated the Emergency Response function through multiple weather events—with the hurricanes activating our Emergency Response Plan while we also, working with federal and industry partners through the Oil and Natural Gas Subsector Coordinating Council, helped address the over pressurization of a Columbia Gas natural gas pipeline that caused multiple explosions and fires at residential locations in Massachusetts.

However, today, I would like to focus my testimony primarily on the cybersecurity function of the office and how CESER will meet the priorities of the Administration and work in conjunction with our Federal agencies, state, local and tribal governments, our industry partners and our national laboratories.

DOE FAST Act Authority

DOE's role in energy sector cybersecurity is established in statute and executive action. In 2015, Congress passed the Fixing America's Surface Transportation (FAST) Act (P.L. 114-94), specifically naming DOE as the Sector-Specific Agency (SSA) for cybersecurity for the energy sector. As set forth in P.L. 114-94, Congress designated DOE as the SSA for cybersecurity for the energy sector. Defined in Presidential Policy Directive 21 (PPD-21), "the term "Sector-Specific Agency" (SSA) means the Federal department or agency designated under this directive 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." PPD-21 states that DHS will "provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure." The FAST Act further mandates that the Secretary of Energy coordinates "with the Department of Homeland Security and other relevant Federal departments and agencies" and collaborating with, among other things, on "providing, supporting, or facilitating technical assistance and consultations for the energy sector to identify vulnerabilities and help mitigate incidents, as appropriate". By creating CESER, the Department's role as this SSA will be strengthened. The Department takes this responsibility seriously.

The FAST Act also gave the Secretary of Energy new authority, upon declaration of a Grid Security Emergency by the President, to issue emergency orders to protect or restore critical electric infrastructure or defense critical electric infrastructure. This authority allows DOE to support energy sector preparations for and responses to natural, physical and logistical events.

CESER

The creation of CESER elevates the Department's focus on energy infrastructure protection and will enable more coordinated preparedness and response to cyber and physical threats and natural disasters with the private sector, as well as federal, state and local government partners. This includes electricity transmission and delivery, oil and natural gas infrastructure, and all forms of generation. The Secretary has conveyed that he has no higher priority than to support the security of our Nation's critical energy infrastructure. The formation of the CESER office enhances the Department's ability to dedicate and focus attention on DOE's SSA responsibilities and will provide greater visibility, accountability, and flexibility to better protect our Nation's energy infrastructure and support asset owners, as well as the overall critical infrastructure response framework overseen by the Department of Homeland Security (DHS).

The CESER office plays an essential role in coordinating government and industry efforts to address energy sector threats. The office is currently composed of two divisions: Infrastructure Security and Energy Restoration (ISER) and Cybersecurity for Energy Delivery Systems (CEDS).

DOE's Roles and Responsibilities for Energy Sector Cybersecurity

In preparation for, and in 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: the 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 is also working with the recently established Tri-Sector Executive Working Group (TEWG) in conjunction with Department of Treasury and DHS along with our industry partners in order to address and manage risks across the energy, telecommunications, and financial sectors. The formation of the TEWG was recommended by the President's National Infrastructure Advisory Council (NIAC) in their August 2017 report titled, "Securing Cyber Assets: Addressing Urgent Cyber to Critical Infrastructure."

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 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.

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.

DOE's Cybersecurity Activities 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.

The Department is focusing cyber support efforts to strengthen energy sector cybersecurity preparedness, coordinate cyber incident response and recovery, and accelerate game-changing research, development, and deployment (RD&D) of resilient energy delivery systems.

Strengthening energy cybersecurity preparedness

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 cyberattacks 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, as well as the broader US intelligence community.

The purpose of CRISP is to share information among electricity subsector partners, DOE, DHS, DOJ, 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 advanced 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 more than 75 percent of continental United States electricity customers. CRISP has clearly demonstrated 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 to monitor traffic 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.

Cybersecurity vulnerabilities of key control systems and operational technology are an increasing concern for the nation's critical energy infrastructure owners and operators. The Cyber Testing for Resilience of the Industrial Control Systems (CyTRICS) program will serve as a central capability for DOE's efforts to increase energy sector cybersecurity and reliability through testing and enumeration of critical electrical components. Further, analysis of test results

will identify both systemic and supply chain risks and vulnerabilities to the sector by correlating collected test data and enriching it with other data sources and methods. DOE will collaborate with government, National Laboratories, and industry to identify key energy sector industrial control systems components and apply a targeted, collaborative approach to these efforts.

Facilitating cyber incident response and recovery

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's Office of Electricity (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.

CESER engages directly with our federal, state, local, tribal, and territorial (SLTT) government partners, as well as 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 the NCCIC and 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. It is critical that the results of the exercises inform our response plans on a continuous basis to close identified gaps in coordination with our industry and government partners through the associated coordinating councils.

Communication capabilities that are survivable, reliable, and accessible, by both industry and government, will be key to coordinating 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 SLTT partners to further shape the types of orders that may be executed under current authorities, while also clarifying how we communicate and coordinate the operational implementation of these orders. Continued coordination with Federal, SLTT, 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.

Accelerating breakthrough RD&D of resilient energy delivery systems

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.

CESER's Cybersecurity for Energy Delivery Systems (CEDDS) R&D program is designed to assist energy sector asset owners by developing cybersecurity solutions for energy delivery systems through a focused, early-stage research and development effort. CESER co-funds industry-led, National Laboratory-led, and university-led projects with SLTT and 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. In a demonstration of our coordination with other federal agencies, two of the university-led collaborations are funded in partnership with DHS Science and Technology.

To select cybersecurity R&D projects, DOE constantly examines today's threat landscape and coordinates with partners, like DHS, to provide the most value to the energy sector while minimizing overlap with existing projects. For example, the Artificial Diversity and Defense Security (ADDSec) project will develop solutions to protect control system networks by constantly changing a network's virtual configuration, much like military communications

systems that rapidly change frequencies to avoid interception and jamming. As a result, ADDSec can harden networks against the mapping and reconnaissance activities that are the typical precursors to a cyberattack.

Another project, the Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF), is designed to anticipate the impact a command will have on a control system environment. If any commands would result in damage to the system or have other negative consequences, CODEF will have the ability to prevent their execution. This type of solution is especially intriguing as it can detect malicious activity regardless of the source, be it an insider threat or an external actor.

The Energy Sector Security Appliances in a System for Intelligent Learning Network Configuration Management and Monitoring project, otherwise known as Essence, is a CEDS-funded endeavor involving the National Rural Electric Cooperative Association (NRECA). Essence started as a concept to build a system that passively monitors all network traffic within an electric utility, and to use machine learning to develop a model of what “normal” is, so that deviations indicative of cyber compromise could be detected instantly and acted on quickly. The envisioned system was built and successfully demonstrated in the first project. Work since then has focused on extending a solid technical prototype into commercially deployable products with solid, committed technical partners with an established presence in the utility market. To date, NRECA has engaged with four partners to offer commercial products based on Essence.

DOE is also working in conjunction with 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 that they have the tools and resources needed to address security challenges. To address risks and manage the risks to an acceptable level, 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

Establishing CESER is the result of the Administration’s prioritization of electric grid security and national security. Our long-term vision will positively impact our national security and economy. As CESER addresses all areas of responsibilities, we are taking the first steps in the transformational change necessary to meet the priority of the Secretary of ensuring the security of our Nation’s critical energy infrastructure.

I appreciate the opportunity to appear before this Committee 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 so much. You are one of the first witnesses that we have ever had that has yielded back some of her time. So thank you. It is a good week.

So, as you know, pursuant to authorities that Congress provided in the FAST Act back in 2015, DOE is, in fact, the sector-specific agency for cyber for the energy sector. And as such, you all are 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.

And as I have listened to a number of different energy-sector firms, they really do believe that there ought to be just one lead cop on the beat. So that is one of the things that we wanted to do when we, on a bipartisan basis, passed the FAST Act.

Can you tell us some of the greatest challenges—as you all are coordinating with other agencies—Homeland Security, others—what difficulties have you had? Have you felt that it has gone pretty well? Do we need to do more? This is something that we want to make sure that you really are the cop on the beat.

Ms. EVANS. Thank you for the opportunity to answer that question. I would say that, based on my tenure to date, which—I am going to remind everybody this is, like, my fourth week.

Mr. UPTON. Yes.

Ms. EVANS. So I have had the opportunity to actually experience this process firsthand, and I have really embraced the priority of the Secretary and all my leadership in the SSA role, which is providing that leadership and making sure that we are the lead person, as you said, the one focal point where the energy sector can come in.

And so I had the opportunity to do that with the hurricanes that came through, and then at the same time we did have that natural gas pipe explosion. So I got to see all of it and was on the calls. And what has happened is, and the way that that works is, we are the lead on those calls when we talk.

Now, it depends on which one we are talking about. So if we are talking about the ones that are being led by the energy sector, they lead that. And so the electricity subsector is led by industry, and we provide information into that, and we actively engage with them on that.

Our staffs all work together. And every night during that hurricane response, we were on with the CEOs of the companies and providing them, from the government standpoint—and DHS was with us, and we had other partners in there as well, so that if questions were asked, we led that response coming from us, and DHS then had the opportunity to provide information from cross-sector so that the energy sector could actually do what it needed to do once we moved into a response mode.

So seeing it firsthand, seeing how it works, seeing that they took the lessons learned from last year, and they applied it to this year's response. There were specific things that happened last year, because of the way that this natural event went, the hurricane went, that it was a one-two type of punch—the event would come and then the flooding—there was specific planning that was done with the industry partners that reflected those lessons learned. And we

had the opportunity, because of the way these calls were done, that we could cross-pollinate across the energy sector.

So it worked well. Right now, I don't necessarily see any gaps, but like I said, I am going to work through this. I am excited to embrace this role. And should we see any gaps, I know I would work with DHS and the other Federal agencies, and we would come forward to our respective committees to ask for that assistance.

Mr. UPTON. So I know that, as we look at these disasters—this committee sent a number of members on both sides of the aisle down to look at Puerto Rico and the Virgin Islands last year after that. And we had members from—obviously, Mr. Kennedy, who was here earlier, and I suspect he will come back, with the natural gas incident that they had up in Massachusetts. And we have members that, for sure, their districts were impacted by Florence in the last 2 weeks. I would imagine that Members reached out to you all. Certainly, their industry partners did.

Any shortcomings that you see right away based on—had you known something, perhaps would you all have acted any differently?

Ms. EVANS. On this go-around, from what has happened?

Mr. UPTON. Yes, so far.

Ms. EVANS. So far, I would say that I have a team that is in place, that the Department has a team that is in place, and I have the honor to actually manage them, that know what they are doing in an emergency response situation. Their responsibilities, our responsibilities as ES-12, when we activate that response plan, they know exactly what they are supposed to do. And when we identify issues that come in through the industry—because they come in multiple ways. Just like you said, they will come in multiple ways. Our leadership would hear something. It comes in. There are multiple meetings that happen.

But the way that the mechanism is set up right now, there is the ability to catch it at multiple levels so that it does not become an issue or that we at least have the appropriate agency working on what those authorities are.

So, for example, in the recovery, one of the things that were being discussed was the ability to use drones. So everybody has them, but there are flight plans that have to be filed, right? And so there was a working group immediately established so our sector knew exactly what was going on in the other sector based on the interaction that happens across with the Emergency Response and the National Response Framework.

So there are multiple levels that happen. Do communications break down? It probably will. And how we need to respond to that and then take that back in to improve it, that is what we are looking at.

And I know that the lessons learned were done from Puerto Rico. And I have seen how they have actually applied those lessons learned through this response and heard those lessons actually being actually implemented by both industry and the government as we were going through the response this go-around.

Mr. UPTON. Thank you.

I yield to Mr. Rush.

Mr. RUSH. Thank you, Mr. Chairman.

Assistant Secretary Evans, as I mentioned in my opening statement, Mr. Walberg and I introduced H.R. 5174, the Energy Emergency Leadership Act, earlier this spring. And our objective was to codify most of the work that the agency is currently undertaking and make sure that we have consistency moving forward regardless of which administration is in office.

Are you familiar with the bill? And if so, do you have any feedback regarding any of its provisions?

Ms. EVANS. Yes, sir, I am familiar with the bill. And I think the feedback and my presence and the establishment of my office supports the idea of what is envisioned by congressional intent. So whatever gets passed by Congress, obviously, I would be responsible for implementing it.

And so, I, again, am supportive of the leadership this committee shows and the support that this committee has and the trust that you have in Department of Energy and the Secretary to accomplish the mission for the energy sector.

Mr. RUSH. I understand, Madam Secretary, that in your previous position you worked as the director of the US Cyber Challenge, an organization that is dedicated to building up the cybersecurity workforce.

From that experience and that perspective, do you have any concerns that you want to share with the committee regarding the Nation's workforce preparedness when it comes to cybersecurity or the threats to our electricity grid?

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? And if not, what are some of the recommendations that you may want to share with us to make sure that we have the capability to address these important issues related to our Nation's security and that centers on the area of workforce development?

Ms. EVANS. I appreciate that question. It is a passion of mine, and I appreciate being able to talk more about cybersecurity workforce issues.

So, as the President released the National Strategy for Cybersecurity, under pillar 2, it specifically talks about the cybersecurity workforce for America as a whole. And as you know, especially in DOE and its industry partners and in the—all of this infrastructure is owned by private industry. So when we start looking at the workforce, one of the biggest things is making sure that the workforce has the basic skills that it needs and then, in this particular sector, the specialized skills as it relates to industrial control systems, SCADA systems, and understanding those.

So there are a lot of initiatives that are under way that are out in private industry that can be leveraged. There is work that specifically DOE was doing, that we were watching from the outside and attempting to leverage that in.

So there is a specific competition. I really believe that you can demonstrate this through competitions. And Congress did pass a workforce act that dealt with allowing to use competitions for people to leverage what they know and to be able to demonstrate it quickly. So CyberForce is a competition that DOE runs with the

National Labs, and it is specifically focused on the industrial control systems and the SCADA systems.

So I am really looking forward to really making that more robust and being able to expand that out for all of us to do. Right now, it is focused specifically on college students, but it needs to expand out more than that, because there are a lot of people that are in this workspace that need to have those skills. They need to be able to demonstrate those, and competitions are a way to be able to do that.

So when you ask me if there are areas where you can improve, our education system and the STEM—and I know we are investing a lot in that—it does one level of knowledge. And what competitions do and what employers need to have and what the Federal Government as a whole needs to have is that the person, when they start on day one, have the ability to show how they would apply that knowledge.

So if you think of it from a science degree, I go to lecture, but then I go to lab. So the competitions allow for that applied knowledge, so that if I am hiring somebody, I know they have the basic set of skills that I need to have, and now what I have to do is train them up for the delta in my industry or in my specific company or, in the case of the Federal Government or DOE, specifically in what we are doing as it relates to cyber emergency response type of capabilities.

So there is a lot of promise, there is a lot of work that is happening in the universities. And I really view my job as not to duplicate that but to leverage a lot of the work that is happening nationally and be able to bring it into the Department of Energy as the sector-specific agency and be able to shine a light on that so that the industry as a whole will be able to take advantage of it.

Mr. RUSH. Thank you.

I yield back, Mr. Chairman.

Mr. UPTON. Thank you.

Mr. Latta?

Mr. LATTA. Well, thank you, Mr. Chairman.

And, Assistant Secretary, thanks very much for being with us today. Appreciate your testimony today.

You might be aware that I chair the Grid Innovation Caucus with my good friend, Mr. McNerney. And we have worked on several pieces of legislation together, and I would like to highlight one in particular, which is the CyberSense Act. And this legislation requires the Department of Energy to establish a voluntary CyberSense program to identify and promote cybersecure products intended in the bulk-power system. And the bulk-power system includes facilities and control systems necessary for operating an interconnected electric energy transmission network.

Would you talk about the work you are already doing on this front and how voluntary programs like this one can help open lines of communications between the private sector and the DOE?

Ms. EVANS. Thank you for the opportunity to talk about our program, called CyTRICS. It is the Cyber Testing for Resilience and Industrial Control Systems. And it is a pilot project to do some of the work and what you intend in that area. And it is to test compo-

ment parts that go into operational technology that is used throughout the energy sector. So we are now starting the pilot.

There are a lot of challenges as we start going through this that aren't necessarily the technical challenges but making sure that we have the voluntary participation from our industry partners as we go through this. We already have some companies that have volunteered to have their products tested.

What we then have to say and how we have to work this out would be: What do we do with those results of the testing? How are we going to share that? How does that fit into an overall risk management framework? How we would roll it up into what we are doing with the C2M2 maturity model that we have so that those results, along with a lot of the other pieces that we are putting together, that a company will be able to look at that and say, OK, here are the products, here are the risks, here is what I have to do to mitigate that risk.

And then the information from these pilots will feed our other research and development efforts so that we can then refine them based on the results that we are getting.

So we really are looking forward and we really are excited about this particular project that we are looking at, because we know that there could be a lot of risks associated with all these different products that are coming into the energy sector, and so we have to make sure that we are aware of what those risks are as we are implementing them.

Mr. LATTI. Well, you talk about trying to get more volunteers in there. How can we encourage more companies to really want to volunteer to be part of that program then?

Ms. EVANS. Well, so they could reach out to our office, in particular, and I am happy—they can come through the sector coordinating councils that they have, because most of them are actively participating in that, and they can volunteer through that as well.

And as we identify and work through the challenges that we have, the idea is then to have a framework. The whole purpose of my office is to take this research and then be able to operationalize it and to be able to take it out into industry so that they can actually use the results of the research and be able to implement it.

And so the more that we can learn about what types of anomalies there might be from different companies, the faster we will be able to develop that framework, and then the faster it will be able to be implemented and out in the infrastructure.

Mr. LATTI. OK.

Well, through this committee's efforts, DOE was established in statute as the lead sector-specific agency for cybersecurity for the energy sector. This new mandate was included in the FAST Act of 2015.

While the lead sector-specific agency mandate is new, DOE has been engaged in this work for many years. What makes DOE equipped to serve as the lead agency?

Ms. EVANS. Well, thank you for that question.

And I would like to say that it is the expertise of the Department as a whole, as well as the ability to leverage the knowledge that is out in the National Labs. And so those are some of the smartest people in the world, and that they work on multiple problem sets

as it relates to the energy sector, they are always thinking about what is over the horizon, what is next, and also trying to fix what is actually happening today.

So I believe that the way that the Secretary's priorities are set up, the experience that is there at DOE, and then leveraging what is happening in the National Labs, that is why you trust us to be the sector-specific agency in this area, and that is why we are providing that leadership.

Mr. Latta. Well, thank you very much.

And, Mr. Chairman, my time is about to expire, and I yield back.

Mr. Olson [presiding]. Thank you.

The Chair now calls upon the gentleman from California, Mr. McNerney, for 5 minutes, sir.

Mr. McNerney. I want to thank the chairman for that.

Mr. Olson. You are welcome. We will see if the Astros beat the Dodgers again this year. So—

Mr. McNerney. We will see.

Ms. Evans, I thank you for testifying. And you have only been there a month, so I understand that that presents challenges.

And I want to follow up on my colleague Bob Latta's comment about the Grid Innovation Caucus. And the purpose of that is really to educate Members of Congress about the challenges and opportunities in the grid, but also to put forth legislation.

Bob mentioned one. I am also going to mention H.R. 5240, the Enhancing Grid Security Through Public-Private Partnerships Act, that provides cybersecurity training to electric utilities and promotes sharing best practices and data collection in the electric sector.

Now, in conversations with utility executives, I have heard that there is a big bottleneck in sharing information, security information, with the utilities because their security people don't have security clearances, and it is taking them a year, year and a half, to get those clearances.

Do you have a plan to expedite the clearances of utility executives and utility security people so that we can get information to them on a timely basis?

Ms. Evans. Well, I appreciate that question on security clearances. And I am going to answer it a little bit differently versus saying that I am going to expedite out the clearance process. Those of you that are involved in that know that that can be quite the challenge, if I were to agree to try to expedite that.

What I really am trying to do and what the vision of this office is is to take information that is informed by intelligence, threat intelligence types of things, things that are classified, overlay it on what is here, and then take it so that it can be actionable out by the utilities.

So you don't necessarily have to have the classified background behind it. A lot of times, especially when you are working out there—and I come from an ops background—you really want to know what you are supposed to do; the why can come a little later on. A lot of times, you have to respond immediately in a situation. You want to know what the actions are that you need to take. That doesn't necessarily have to be classified.

And that is what I view my office as being able to reach out, share that information with our partners, and be able to give them the actions that they need to take that is informed by the government-as-a-whole approach.

Mr. MCNERNEY. OK. That sounds good. How far along are you in that process?

Ms. EVANS. I actually have some things I hope within the next 120 days that I will be able to share with industry directly that they can start taking some action. There are some things I am doing that they should be implemented here shortly, and I think that they will be surprised when they see it. And there are some basic things that they can do now in basic hygiene that, when they see the visualization of that, they are going to be surprised.

Mr. MCNERNEY. Well, I look forward to hearing from the executives and utility people—

Ms. EVANS. Yes. OK.

Mr. MCNERNEY [continuing]. What they think of the plan, and I will be glad to share that with you.

Ms. EVANS. That would be awesome. I am looking forward to working with you on that.

Mr. MCNERNEY. Now, how does CESER monitor or plan to monitor cyber attacks?

Ms. EVANS. So there are several different things that are already under way that CESER is looking at, as far as the infrastructure. The vision that we have for this office, several of the tools that are already in place, several of the projects that they already have—which I am sure you are familiar with CRISP. Also included in my testimony we talked about CYOTE, that particular project.

The way that we look at how we are going to do this is, for example, in the operational technology world, you know exactly how things are supposed to respond. So the idea is to manage by exception. So, as you pick up exceptions, then working and putting together a model, you can put sensitivities to that, and that would then show anomalous behavior.

Based on then feeding it with information that is coming from multiple areas, especially intelligence, we will be able to tell if that is something that is just—so we talked about the supply chain and all these other types of equipment. We will be able to tell by the data if something is actually happening, if somebody is in the network or if it is an equipment malfunction, or what is actually happening, by overlaying this data.

Are we there now? No. We have several of these pieces in place that are—

Mr. MCNERNEY. So you are basically using big data and algorithms, or will be. So that is—

Ms. EVANS. We will be. That is why there are different pieces—

Mr. MCNERNEY. Again, I will look forward to hearing more about that.

And I have time for one more question. You may not have time to answer it. Do you feel confident that our utilities are adequately prepared and protected from Russian and North Korean cyber attacks to prevent massive blackouts or credible enough threats of

massive blackouts to make our Nation vulnerable to cyber blackmail?

Ms. EVANS. So, since you asked me do I feel confident, the answer would be no.

Mr. MCNERNEY. Thank you.

I yield back.

Mr. OLSON. Thank you.

The Chair now calls upon the gentleman from Secretary Evans' home State of West Virginia, Mr. McKinley, 5 minutes, sir.

Mr. MCKINLEY. Thank you, Mr. Chairman.

And I would be remiss if we didn't go back and remind the chairman, when she was being introduced, that she is a good West Virginia native and graduated WVU and is a staunch Mountaineer fan.

Ms. EVANS. Yes, I am.

Mr. MCKINLEY. So thank you. Thank you for coming here to this.

I am curious about a few things primarily dealing with the reliability, because the question you just heard from Congressman McNerney about the capability of meeting the challenges we face. And the President has been wrestling with 202(c) or Defense Procurement Act as a way of addressing that.

Can you give me an update on maybe what is happening in that arena, for everyone to understand that we may be having quite a few power plants shut down prematurely without having 202(c) or the Defense Procurement. So if you could give me a little update, if you could?

Ms. EVANS. I actually can. Thank you for that question. Secretary Perry was speaking yesterday about this exact issue. And what he said was that he does not have anything new to update at this time, that this is still a policy that is being reviewed by the White House.

Mr. MCKINLEY. OK. But building off that—and we talked about the ISO New England, the problems they are having there in getting power, not only the importing—as you are probably familiar, that they are importing from Canada 73 gigawatts of power into New England.

Do you dispute that number? Or do you think that number is—that is the number that has been published, 73 gigawatts. That is essentially—for people to understand what that means, that is about 100 power plants that don't exist in New England, as we rely on importing power from Canada.

Is that about correct, the 73 gigawatts?

Ms. EVANS. I don't have the exact numbers in front of me. I am happy to take that question back and—

Mr. MCKINLEY. If you would, please.

Ms. EVANS. Yes.

Mr. MCKINLEY. Because, we are trying to be energy-independent. And we have a section of the country that has some issues about being able to meet the challenges, whether that is from hacking or internally. So we are depending on now importing.

So let me ask another question, then, with that dependability. And McNerney was just talking about Russia. Isn't it accurate that New England was getting its natural gas this past winter from Russia? From an LNG tanker that was in Boston Harbor?

Ms. EVANS. I don't know the answer to that question, sir, and I would be happy to take that back as well.

Mr. MCKINLEY. Well, I have the answer.

Ms. EVANS. OK. There you go.

Mr. MCKINLEY. So, yes, the answer is yes—

Ms. EVANS. OK.

Mr. MCKINLEY [continuing]. It was.

And so it is a matter—if we are going to be energy-independent and we are going to make sure that we have the power necessary for that New England area, we have two issues: Are we going to continue to import gas from Russia, and are we going to import power from Canada?

So that is why I think it is so important that the White House and others move on this 202(c) or Defense Procurement Act to protect our grid system. Because I think we—reports we have had from National Energy Technology Lab, NETL, have indicated we are prematurely shutting down too many of our coal-fired power plants, and we are headed into a blackout, possibly this winter, as a result of it.

Do you have anything to update us on alternative measures that might prevent that from happening?

Ms. EVANS. No, sir, I don't. But I will take back your concern and elevate it to my leadership so that they know exactly what the issues are that you are bringing up so that I can make sure I can feed into the policy process.

Mr. MCKINLEY. If you would, please, pass that on—

Ms. EVANS. Yes, sir.

Mr. MCKINLEY [continuing]. To Secretary Perry, and tell him where it is coming from.

Ms. EVANS. Yes, sir, I will.

Mr. MCKINLEY. Thank you.

I yield back.

Mr. OLSON. Thank you.

The Chair wants to remind my dear friend from West Virginia, our witness, Secretary Evans, this weekend the Mountaineers are going to Lubbock, Texas, to play the Texas Tech Red Raiders. And my warning is, they have got this symbol; it is called "guns up." They score a touchdown, they get their guns up. You all are going to see a lot of guns up in 60 minutes in Lubbock, Texas.

The Chair now calls—

Ms. EVANS. As you know, I am really constraining myself not to respond to that, but that is OK.

Mr. OLSON. It is football in Texas. Feel free to fire back.

Ms. EVANS. No, that is OK. But we are Big 12. It is good. It is all good. It is OK. We are doing well. Our team is doing well.

Mr. MCKINLEY. Where are they ranked? What, 25th?

Mr. OLSON. Twenty-five versus 12. Get your guns up.

The Chair now calls upon the gentleman from South Carolina, Mr. Duncan, for 5 minutes of questions.

Mr. DUNCAN. Go, Tigers.

Secretary Evans, I first want to thank you for your response to Hurricane Florence. I know there were over a million power outages across the Carolinas, and you and your team were extremely responsive both during the preparation and restoration process.

Duke Energy serves much of my district, and I have heard from them many positive things about your engagement. So I want to applaud you on that.

I also want to thank you, both you and Secretary Perry, for your leadership in creating the new CESER program. Protecting the grid against cyber and EMP attacks should be a priority. Many Americans fear the potential of an attack given the volatility of players such as Iran, Russia, and North Korea.

Over 5 years ago, the U.S. DOE and the industry, with industry matching over 80 percent of the funds, established at Clemson University perhaps the world's largest, most capable electric grid emulator. This 20-megavolt-ampere facility, called the Duke Energy eGRID, is providing a platform for innovating and validating and testing multimegawatt electric grid components in real grid conditions without the risk to the grid.

This capability is needed to facilitate the rapid introduction of new technologies into our Nation's electrical infrastructure. It is also a prime example of public-private partnership working to develop advanced technologies to protect against evolving threats.

The folks at Clemson worked closely with the utilities. Duke is a partner. They worked close with industry, National Labs, and other universities and the DOE to accelerate the marketing of new technologies.

Are you familiar with the eGRID down there in Charleston?

Ms. EVANS. Yes.

Mr. DUNCAN. Have you visited that in North Charleston?

Ms. EVANS. Not yet.

Mr. DUNCAN. OK. I want to invite you to do that. And I invited Secretary Perry as well.

I am concerned with the grid being able to withstand attacks such as an EMP or cyber attacks, supply-chain attacks. And I realize you just started at the DOE, but I am interested to know how the DOE plans to address these important critical issues.

Ms. EVANS. I appreciate the opportunity to answer that question.

I am in the process of looking at many of the things that are in place. This office was set up specifically to deal with those concerns. And Congress has given us that authority, as the sector-specific agency, to really embrace that and to go full-force into that.

My office, in conjunction with other offices within DOE, really are looking at how do we need to do that, what are the right investments as we are going forward, what is the right research and development as we are doing that. There are many projects that are already in place with the National Labs. It is my intention to leverage those results and implement them.

And so I am of the mindset that my office is about the implementation and working with industry to get it implemented and then distributed through industry so that they can benefit from the results of all that research and make sure that it is actionable so that it can go out there so that the grid and our energy sector is resilient and then can withstand—the Secretary has told me that his highest priority and his biggest concern is that, when a natural disaster is happening, that we would also have some type of disruption in the technology and that we would be able to discern be-

tween the two if they are related or if it is our adversaries taking advantage.

And that is what I really look at as the highest priority, to be able to implement that technology and be able to provide that information up through the appropriate mechanisms so that the Secretary and DHS and the administration is properly informed so that they can make those decisions.

Mr. DUNCAN. I used to serve on the Homeland Security Committee, and since I have been in Congress, there have been several attempted attacks on transfer stations, substations, different things. We have gotten lucky, in that supposed attackers didn't realize diesel fuel didn't explode, et cetera.

Those type of physical attacks on our electric grid are very difficult to predict and protect against. We can't monitor every substation and what not. What sort of work is DOE doing in that regard?

And we know all about the cyber stuff, but these are physical attacks. It would just take a simple explosive device and—so have you all thought about that? And what, working with Homeland Security, are you doing about it?

Ms. EVANS. So the short answer is yes. And the ISER group that is in my responsibility does exercises. And so we heard a little bit about the Clear Path IV exercise. The idea is to develop different scenarios around those so that, as it is being executed, what are the responses, have we thought about everything.

And so, when you do those exercises—and there are exercises coming up, like Liberty Eclipse, and there are things we are doing with NERC, as the GridEx. Those exercises, they inform the ability to actually respond. So the idea is, OK, we all have a plan, but you want to exercise the plan before you actually have to do the plan and respond to the plan.

So that is what that group does. The idea is to expand out those exercises. And as we hit the basics, then it is to continue to expand those out so that those lessons learned are there in the response plan and that we share that. That is exactly why we do the exercises with State, local, and our government partners, as well as industry.

And that was the uniqueness of that Clear Path IV, was that industry was involved in that, and it was done out in Washington State. Because it is one thing if you do it in DC; it is another thing if you are doing it across the country and involving all the State and local partners as well as the industry. Because those lessons learned, the communications, the issues that you brought up earlier, if we see gaps, we don't want to be in the actual incident when we are identifying gaps that we need your help with.

Mr. DUNCAN. All right.

Well, my time has expired, but I will remind the committee that things that can affect our grid system can be both manmade and natural, so hardening the grid is important.

With that, I yield back.

Mr. OLSON. Thank you.

The Chair now calls upon the gentleman from New York, Mr. Tonko, for 5 minutes.

Mr. TONKO. Thank you, Mr. Chair.

And, Assistant Secretary Evans, congratulations on your confirmation, and welcome to the committee, and thank you for your testimony.

Obviously, we have not faced the full consequences of a cyber attack on the grid yet, but we do continue to experience major electricity outages and energy disruptions due to natural disasters. I want to ask about what you see as the mission and role of your office in the future.

There has been a lot of emphasis on cybersecurity today, and rightfully so, but it is my understanding that the office is also responsible for emergency response, including those from natural disasters. Is that indeed correct?

Ms. EVANS. Yes, sir.

Mr. TONKO. And earlier this Congress, Assistant Secretary Walker of the Office of Electricity, testified about the work being done by his office in the wake of Hurricane Maria in Puerto Rico. Now, has CESER played a role in the Maria response or preparation against future energy disruptions in Puerto Rico over this past year?

Ms. EVANS. Thank you for the question. And before the CESER office actually was formed, a lot of the functions that we are talking about as the exercise capability that we have as well as the emergency response capability all belonged and were all in one office, which was where Secretary Walker is, in the Office of Electricity. When CESER was formed, those moved over. So my office has cybersecurity, energy security, and emergency response.

So in the case of Puerto Rico and Maria, my office is responsible for the activities that happen when we activate our emergency response, the RES-12 under the National Response Framework. So, for example, this go-around with the hurricanes, it is my office that goes and mans down in FEMA, that goes out to the regions. We have very specific response capabilities, incident response capabilities that we do in natural disasters.

When we move into the recovery phase, and that is what is happening right now down in Puerto Rico, Assistant Secretary Walker continues that effort. He was just down there for the anniversary, was looking at everything that is there, and he is involved in the recovery aspect.

So when you look at how our offices work together and where that separation is, we do the emergency incident response type of capability. We are down there. We are embedded with the States. We work with FEMA. We are over at the national center there, and all the information goes up. When it shifts, where we are right now, that is when it then shifts back to Assistant Secretary Walker's office.

Mr. TONKO. OK. Thank you.

And I know that earlier there were questions about Hurricane Florence. So in this cross-pollination between the two offices, have there been lessons learned or experiences from Maria from the Puerto Rico experience that helped or influenced your responses in some way with Florence?

Ms. EVANS. I would say that based on the way that Assistant Secretary Walker handled that, he has been instrumental in bringing up the CESER office. And his interactions of what he has done

and how I have been able to be brought up to speed so fast is based on those lessons learned of where they clearly see the delineation between the two offices.

So, again, this is a secretarial priority. Assistant Secretary Walker and I really have worked that out. We continue to work it out. But his office is very strategic in looking at how you are doing different things; and then my office, it feeds directly into my office for lessons learned impact, and then we implement from a tactical standpoint.

Mr. TONKO. Thank you.

Robust cybersecurity requires significant financial resources and new and advanced technologies. But we know there are many small utilities with limited resources that might not have the same technical capacity as their larger components. Does DOE have a plan, a technical assistance program or funding available to assist these smaller utilities such as a public power authority, a small public power authority, or a rural cooperative?

Ms. EVANS. I would like to take that question for the record because I am unaware of the specifics, but—and I would like to get back to you on that specific question.

Mr. TONKO. If you would, please. That would be very helpful, because they obviously could be impacted by some very severe disasters, and that assistance would play a major role in their responsiveness.

So thank you again for your response to the questions.

Mr. OLSON. Thank you.

The Chair now calls upon himself for 5 minutes.

And, again, welcome, Secretary Evans. I can assure you there will be no talk about football, Texas Tech versus West Virginia this Saturday. I won't talk much about cybersecurity. That is important, but I do want to focus on natural disasters and specifically hurricanes.

As you know, my home State of Texas is a cornerstone of America's energy production and security. The Greater Houston is a cornerstone of this cornerstone. We produce the bulk of the oil that is refined and used here in America, and we also have a launching port through the number one exporting port in America, the Port of Houston, for this energy to head overseas and change the world.

Hurricane Harvey hit us 13 months ago, hit us twice. It wasn't a windstorm. It wasn't a storm surge. It was a rain event, almost 4 feet over all of southeast Texas in less than 2 days.

I know your organization is new. You have been on the job for 4 weeks, but could you talk about what you have all learned with Harvey, Maria, Irma, and now Florence, what those lessons are? And also, after a storm, do you all do some after-action reporting and include all the players, the State, the government there in the State, the counties, the cities, the first responders, and private parties who are involved in the recovery from these storms? What is your sort of plan there, what you have learned so far?

Ms. EVANS. Thank you for the question. It is my understanding that after-action reports are done. After-action reports were done after last year's Harvey, and I do know that a lot of the lessons learned were specifically discussed on the coordinating calls with our industry partners.

And it was highlighted very early on, specifically, about that this was going to be a one-two punch very similar to Harvey, and that they were more concerned about the flooding and the aftereffects of the hurricane. And so the utilities as they were on the calls, because of those lessons learned, did preposition over 40,000 workers before the flooding happened because they knew what would happen about the roads and how things would be. And so that happened.

Additionally what happened because of things that happened there that they applied this year is there were things that dealt with, once the power company went in, they were looking at one set of power lines, and the telecommunications companies then would go in and they would cut lines because they weren't sensitive.

So what happened this year in this particular case is that information was conveyed. This was lessons learned. So the utility companies told exactly the telecommunications companies where they were going, what the plans were so the telecommunications companies could follow right behind the utility companies. So as the power came up, communications came up. That was a direct lessons learned from Harvey last year.

Mr. OLSON. Well, thanks, I have a question.

You also brought up drones in a hurricane, natural disaster early in this hearing. Drones played a big role in Harvey as the storm hit, quick recovery. For example, the mayor of Missouri City wanted to fly a drone over—he had heard a levee was having problems with a bubble in a big subdivision. It was about to burst. There were rumors it didn't, but he was concerned. He couldn't fly his drone because it was—airspace was controlled by the Coast Guard. It took him 1 day with this levee about to break maybe and flood all these homes to finally be able to fly his drones.

So my question, I know it is not your jurisdiction per se, what is your role in these drones over these disasters? What is DOE's role here? Can they help out Missouri City and have them fly those drones quickly to save people in need in a time of crisis?

Ms. EVANS. So as the sector-specific agency, when especially that was discussed as another lessons learned that happened from last year, that the drones would be critical, and then there is a lot of information that we have from our own modeling that we share with utilities companies.

But that issue was raised early, and because the coordinating councils are cochaired with our industry partner—our industry partners as well as our government partners, as that issue is raised, we have a mechanism then to feed it back in before it becomes a crisis. So the things that you are talking about, there was a working group already established—

Mr. OLSON. Great.

Ms. EVANS [continuing]. Before the incident happened so that they could get approval and be able to use the drones for the recovery mechanism.

Mr. OLSON. The final question is about reliability and emerging threats. In Texas, we have had some blackouts in the past. The big year was 2011. That February we had rolling blackouts because of two power plants in Dallas area had some water pipes frozen, had

to have rolling blackouts. That same August, this extreme heat wave, same thing happened across the State.

As you know, when blackouts happen, even rolling blackouts for a short amount of time, people are exposed to death situations, mostly senior citizens and young kids who can't handle extreme heat or extreme cold, and we have to take this very seriously.

I know they are expecting a thing called the GridEx exercise. Could you talk about your work with industry and NERC on preparing for a grid emergency like we had in Texas in 2011?

Ms. EVANS. I appreciate the question. I know that we have the GridEx exercise. Again, that information feeds back into what DOE does, what—any gaps that they would see in DOE's ability as the sector-specific agency to be able to deal with that. I am actually getting ready to go out to the NERC event and what they are doing with GridEx again this year, so I will be there. I will have first-hand out at that group.

Mr. OLSON. Great.

Ms. EVANS. But there are other things that DOE does that feeds back into what NERC does too as the Electricity ISAC, and so there are tools that we have, there is modeling that we do. We have eagle eye that looks at everything. We also then have the CRISP program that feeds that.

The idea in the long run is to be able to start putting more of this data together so that it can go out through the Energy ISAC that NERC does manage so that they can get that information then down to the utilities. So as you are looking at natural disasters or other types of things, again, I am getting back to we have to give them actionable information that they can share through their partners so that they can take the appropriate actions.

Mr. OLSON. Thank you. My time is expired. Enjoy your time watching the football game from Lubbock, Texas.

Ms. EVANS. Thank you.

Mr. OLSON. The Chair now calls upon the gentleman from Ohio, Mr. Johnson, for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chair.

And, Assistant Secretary Evans, thanks for being with us today. Let me try to dodge my colleague here to make eye contact with you.

Decisions made by different agencies across the Federal spectrum can impact our electric grid and specifically impact how our grid operators, generators, and grid-related devices effectively perform and communicate with one another. For instance, the electric utility industry has added and is continuing to add data and networks along its infrastructure to bolster its reliability.

This continual addition of new technologies and communications networks can fall into multiple agencies across the Federal Government and commission jurisdictions, some of which are not typically involved in the oversight of our electric grid. So that is why I am interested in the Tri-Sector Executive Working Group, which is meant to manage risk across energy, telecommunication, and financial sectors. Can you tell me a bit more about this work?

Ms. EVANS. Yes, sir. I appreciate the question on the Tri-Sector Working Group. We just held our first meeting all together last week. And so the idea behind that, that was a recommendation

that came from the President's working group on that on infrastructure and recognized the complexity of those three and the interdependency.

So from a Federal Government standpoint, you have Department of Transportation, Department of Energy, and Department of Homeland Security representing that. And then we have the utilities, which is also the same group that is leading our Electric Subsector Coordinating Council; and then you have the financial sector, which is also the ISAC for that, which is then JPMorgan is the lead on that as well; and then you have Telecom, which was AT&T.

So we were there. The idea is really to, OK, we need to know what is critical in those areas for what is the basic types of operations we are talking about, the modeling of what it is going to take for the North American grid so that we can deal with these issues and where are the interdependencies, and then utilize that from the government approach back. And, again, that gets back to our original question, if we see that there are any gaps in those authorities, then we will raise those through the appropriate policy mechanism and go to our respective committees.

Mr. JOHNSON. OK. Do you believe further communication between different facets of the Federal Government are needed to ensure that our grid is secure, especially as utilities increasingly look at their own communication networks to add security and up to the second situation on awareness over their infrastructure?

Ms. EVANS. I appreciate that question. And as we continue to do this work and as we continue to improve the modeling that we are doing, I am sure we are going to show interdependencies. I believe that the framework that is in place right now allows us—especially with the President's release of the National Cyber Strategy—allows us the mechanism if we were to identify those as we do the work to bring those up accordingly through the administration and be able to identify those policy gaps.

Mr. JOHNSON. OK. In December 2016, the Department of Energy and the National Association of State Energy Officials cosponsored Liberty Eclipse—

Ms. EVANS. Yes.

Mr. JOHNSON [continuing]. A regional energy assurance exercise to promote State and local level preparedness and resilience for future energy emergencies stemming from a cyber incident. So, Ms. Evans, why are exercises such as Liberty Eclipse beneficial for coordination between Federal, State, and local governments?

Ms. EVANS. I find that the exercises are critical. As I mentioned earlier, we believe, when we put together a plan, that we have identified what all the contingencies are. But when you put together a plan, you don't know what you don't know until you actually exercise the plan. And the emergency when it is happening is not the time to exercise the plan.

And so these exercises, Liberty Eclipse, which we are getting ready to do another exercise on that, identify any gaps that are the issues that you are raising right now, either between the Federal Government going across or down with our State and local partners or across with industry.

Mr. JOHNSON. Were there any lessons learned from that exercise, and have any of them rendered any improvements?

Ms. EVANS. There were lessons learned, and it is my understanding that those lessons learned, the plans have been updated, and they are now going to be exercised again in this next exercise of Liberty Eclipse to see if they were adequately addressed and if any new gaps or any other new lessons need to be applied and updated as we go forward. So that is happening in this next exercise that we are doing of Liberty Eclipse at the end of October.

Mr. JOHNSON. Great. All right. Well, thank you.

Mr. Chairman, I yield back.

Mr. OLSON. Thank you.

The Chair now calls upon the gentleman from Oklahoma, Mr. Mullin, for 5 minutes.

Mr. MULLIN. The great State of Oklahoma. Great State.

Mr. OLSON. A good State, not the greatest.

Mr. MULLIN. Thank you, Mr. Chairman.

And, Ms. Evans, thank you so much for being here. It is always impressive when you see individuals come in here well informed and knowing the issues, so thank you for taking the time to get here.

Recently, there was a tragic explosion in my district at a drilling rig, and I am pretty sure you are aware of it. A question that I have is—which I really don't like the acronym CESER, but I guess that is how you pronounce it—what role does CESER have in assisting the U.S. Chemical and Hazard Investigation Board in their investigation and response?

Ms. EVANS. So it is my understanding that as a sector-specific agency and the way that we roll things down in an emergency response, that we would provide information to the appropriate agency and the appropriate board.

Mr. MULLIN. What kind of information are you providing for them?

Ms. EVANS. What comes up through the channel, if there are concerns that come directly from the industry, if there are types of information. I do not have the specifics on that one, but I do have the specifics, well, like, for example, when the Massachusetts one came up. And that is it comes up through us, but Department of Transportation is actually on the call. So they then share the information of what they are working with with their board, and they share it out with the other group, this is the initial findings, this is what we have at this point.

If there is anything that we need to do from an energy sector role, then what we have to do is raise it back, and we either share it with our sector or I have to raise it up to my management if a policy decision needs to be made.

Mr. MULLIN. Do you share that information with the public, if there is reason to be sharing, or is that someone else is sharing that information?

Ms. EVANS. As a sector-specific agency, we share information with our appropriate sector. Depending on how that investigation is done, so like in the case of the Massachusetts one, Transportation would then share that because they would be the appropriate agency to share the information with the public.

Mr. MULLIN. So you are assisting the Transportation—

Ms. EVANS. Yes. And so the other thing that I have learned through this is that the biggest thing that all of us have done in this sector is making sure that the information is shared so that there is unity of message so that we all have the same information—

Mr. MULLIN. Right.

Ms. EVANS [continuing]. So that that way we are not saying different things from a different vantage point but that the information is consistent.

Mr. MULLIN. So who is coordinating that response and that information, the flow of information? Who is gathering it and putting it in the right hands? Is Transportation leading that too?

Ms. EVANS. In the case of what happens here in the energy sector, they have associations, and as it relates to what happens and they send it out through industry, we share the information with them and then their industry associations then distribute it.

In the case of the Federal Government, if Transportation is the lead, we would feed into the Transportation type of information that would go up and then that secretary would be the accountable person.

Mr. MULLIN. Does that information flow freely or is that only when they specifically ask for the information?

Ms. EVANS. Based on my experience and based on the way that I am going to work this office, the information will flow freely.

Mr. MULLIN. Freely. So you will have a point of contact?

Ms. EVANS. Absolutely. I already have contacts now.

Mr. MULLIN. OK. Great.

As far as the briefings, because we do understand between cyber attacks and vulnerability of our electrical grid and just the oil and gas industry in itself, how often do you brief industry as far as security issues? Do you plan on briefing them, and if so, traditionally how often does that briefing take place?

Ms. EVANS. It is my understanding the way that the information flows specifically about what you are asking is that we as DOE provide information—and this is the question that was asked earlier about our relationship with NERC. And so NERC is directly tied into a lot of the tools in the modeling and the CRISP project that we were talking about. That information then informs the ISAC, and so they get that. They are tied directly into that platform, and so we are providing that information to them on a daily basis. Based on that information, they then distribute it down to the energy sector through the ISAC, and that is what the ISAC mechanism is set up for.

Mr. MULLIN. Are you doing specific classified briefings with industry when it comes to this?

Ms. EVANS. I would have to take that back for the record and find out what is the history associated with what types of briefings that we have done as a sector-specific agency with them.

Mr. MULLIN. Appreciate it. I am out of time. Thank you so much for being here. Appreciate it.

Mr. OLSON. Thank you.

The Chair now calls upon the gentleman from the great State of Michigan, Mr. Walberg, for 5 minutes.

Oh, I am sorry. Mr. Kennedy slipped in behind me. I'm sorry, Mr. Walberg.

The great State of Massachusetts, Mr. Kennedy, for 5 minutes. Mr. KENNEDY. Thank you very much, Mr. Olson.

Madam Secretary, thanks for being here. I am going to build a little bit off of my colleague Mr. Mullin's questions, probably not surprisingly, with regards to emergency response.

I am from Massachusetts. There has been an awful lot going on there in the past couple of weeks. I know you touched on it briefly or it was touched on a little bit earlier in the testimony, and I wanted to drill down on this a little bit.

So understanding that circumstances evolving and ongoing, but we had an overpressurized pipe result in rupture over 80 explosions, people that are still displaced from their homes, and gas that is apparently not going to get fully restored to the area until potentially mid-November, trying to figure out what happened. And it would be helpful for me to get a sense as to what oversight role you play in this, what the status of the investigation is, and what update you can give me to start.

Ms. EVANS. Thank you for that question. And what did happen with that and what is our role as a sector-specific agency, so we share this, this is through the energy sector, the energy government sector, so we are partners with the Department of Transportation as well as the Department of Homeland Security on this.

I can say, in that specific incident, because we have the emergency response piece, my staff called me within an hour of being notified of that. The Oil and Natural Gas Subsector Coordinating Council was also scheduled.

So within an hour of that, Department of Transportation and PHMSA in particular was also on the call because they are the industry part, the government part. We were all on the call. And they were sharing information as they were getting it with the electric sector right afterward, because we had a call with them also because they all wanted to know what was going on.

So as that investigation continues through this mechanism is how the information is then shared out with the community. But Department of Transportation is the lead in this particular case.

Mr. KENNEDY. And fair to say, ma'am, just so I understand it, that your role in that is then focused on the emergency response for the immediate triage?

Ms. EVANS. Yes.

Mr. KENNEDY. And so how is it, though, to the best that you can explain, understanding that is not the focus of the hearing but focus for me, how is it that this happens? How is it that firefighters are responding to all these explosions? There is a well-publicized case, one firefighter going out, putting out a fire while his own home explodes.

How is it that—why does it take so long? I understand that this had to be done manually from Columbia Gas, an alert that had to take place to then have somebody actually dispatch a human being down to try to alleviate the overpressurized pump. Is that typical? Is that how this should operate? Are there going to be regulations that come in? Would you suggest additional regulations to make

sure something like this—we can up the preventive measures on this? How should we be thinking about an appropriate response?

Ms. EVANS. So what happens in this particular case—and I appreciate the question because I—there are a lot of moving parts to the question that you just asked. So the industry, the company would have a response plan. That response plan is also—then there is a local response plan as well as then a State response plan. And I know this sounds like there are a lot of layers, but the communications does flow up pretty fast.

And so my office, as an emergency response piece, is directly tied into the State and local governments. And so we do get notified. There is a notification that happens when these things happen, and then people's response plans go into play. And so everybody's response plan is then executed.

So I think that that is the focus of what everybody was asking for, do we see gaps when they happen. And I think that is what is still being investigated, and that is what you are trying to understand right now is were those adequate plans, and if not, are there gaps, and then they have to feed back into the process that we have, because if you need a Federal response, it has to come up so that we can be able to respond.

Mr. KENNEDY. And I appreciate that. I am also wondering if the scope of the regulation is such where an accident like this can happen, right, and understanding the—we are still trying to investigate exactly what happened and how, but that there are going to be people that are without their homes in Greater—or without heat and hot water in their homes in Greater Boston through mid November if this is done on schedule, should we allow that? Is that a permissible response to say, it is OK for folks to be dislocated from their homes for 6 to 8 weeks?

And if not, why—if the company was actually in compliance with the regulatory environment that—the existing regulatory environment, why is that part acceptable? Because I have got two little kids under three. This doesn't affect me, but I would imagine that for a family trying to heat their home with space heaters, that some of these homes that is not even adequate, for 2 months becomes a real challenge.

And Columbia might be doing the best they can to replace hundreds of miles of pipeline, but something fell through the cracks here in a pretty big way without yet a conversation as to how do we make sure that such an incident like this, the consequences are going to be mitigated in the future. And so that is what I would love to get your insight to where we should look and how we should focus.

Ms. EVANS. So I would like to say that until the investigation is completed, it is hard to address that question. But you are asking some broader-based questions that are about risk management and what is acceptable from a nation.

So I am going to turn back to the administration's national strategy that they have dealing with critical infrastructure and in some of the things that have already been released by Department of Homeland Security, which is the risk management center.

So a lot of the things that you are talking about fall under risk management and is it acceptable. There are things until this inves-

tigation—the results are actually out is that it is possible that the level of risk associated with the infrastructure there is not acceptable because of the consequences that the American people are now experiencing because of what happened there.

That data and then our analysis is going to have to feed up through the policy process about what is the right risk management, is it going to take a regulatory change, is it a legislative change, is it an investment, and that is going to be a policy decision, and that is the intent. And that is what my office is focused on being able to do is provide that type of information after this happens so that the right policy can be made so we can answer that question for you.

Mr. KENNEDY. Chairman, appreciate your patience.

Look forward to working with you on this issue, Madam Secretary. Thank you.

Mr. OLSON. Thank you. I remind my friend too to please talk to FERC about pipelines as well because they are a big Federal agency. DOE has got a role, but FERC is a big one for pipelines.

Mr. KENNEDY. I am aware.

Mr. OLSON. Yes. I just want to make sure you talk to FERC.

The Chair now calls upon the gentleman from Michigan, the great State of Michigan, Mr. Walberg, for 5 minutes.

Mr. WALBERG. Well, I thank you, Mr. Chairman. And thanks to the assistant secretary for being here.

Workforce development has become a focus here, I think, in a very positive way in Congress, and having a well-trained, certified cybersecurity workforce is a key component to our overall cybersecurity strategy as a nation. However, recruitment and retention of cyber workers is a well-documented problem, challenge, frustration, especially in the public sector.

What programs are in place that allow cyber workers in the Department to have professional development opportunities as well as enhanced skill sets, and what plans do you have to add to that preparation?

Ms. EVANS. I appreciate the question on workforce. This is a passion of mine. So I am in the process now of looking at what kind of training and what type of programs are actually available for my own staff to be able to go forward.

I did mention the cyber force effort, that competition that is run by the national labs. That has a lot of promise to be expanded both internally as well as externally and continue to grow beyond the initial view of that, because a lot of what that is focused on is energy specific, and that is the baseline of skills that my team will have to have in order to be able to respond and be able to work with the industry.

So there are a lot of nuances when you go through this. And when you use the term “certified,” that means a lot of different things to a lot of different people. I would say right now that what we are looking at within the Department of Energy is the national initiative for cybersecurity education, which is run by NIST, and making sure that our positions and how we are using that framework really aligns.

And so I look at the structure of what we have. I am also looking with the chief information officer and what they have in place, be-

cause if they have training programs already in place, the idea is to leverage those as well.

Mr. WALBERG. Well, that is so important, and I appreciate that in talking with the private sector and their challenges in the energy industry with cyber. They have been appreciative of the relationship that has developed because of what we have done here of having public-private sharing back and forth together. But to keep the good people that have been trained and to stay in the public sector is so important as well, so I would encourage you, and thanks for your commitment to that.

Ms. EVANS, I would like to follow up on Mr. McNerney's question earlier on. You said you were not confident that the U.S. electric sector can prevent a state actor attack. Would you please elaborate on this a little bit further?

Ms. EVANS. For me to have a certain confidence level of that, I want to make sure that I am providing all the information that they need to have so that they can make sure that they have the proper defenses in place. I know based on my experience and the previous work that I have done and the workforce issues that you have brought up, there are a lot of opportunities for the utilities to improve.

And I think a lot of things that are going forward, there are basic things that all of us have to do across multiple sectors as it relates to hygiene. So the more we integrate technology into what we are doing, the higher the risk it becomes. And I think it really does become a risk management type of approach, and the executives of those utilities as well as the workers need to understand what are the risks that they are bringing into their enterprise as they go forward.

I think right now that that is the dialogue that is happening. I think DHS is showing the leadership with the risk management center so that that information can then perpetuate throughout the industry, and then what you are going to see is those interdependencies. Right now, that whole holistic approach is really not understood across the industry.

Mr. WALBERG. Thank you.

When the Department of Energy was organized as a Cabinet agency in 1977, the largest energy security concerns were fuel supply disruptions, not electricity disruptions or cybersecurity. As you would expect, the Department's Organization Act reflected those concerns. Times have changed, and we should be thinking differently about energy security and emergency preparedness.

In my bill with Ranking Member Rush, H.R. 5174, we specify functions to include emergency planning coordination and response. Could you talk about your work to elevate these functions in your new office?

Ms. EVANS. I appreciate the opportunity. I am happy to talk about that. I am currently, right now, looking at what we have in place, and we have, as I talked about earlier, the emergency response piece that we have, specifically associated with hurricanes, natural disasters is really robust.

What I really want to look at is the exercises and then how do you continuously improve that to bring in other threat factors that we have been talking about, manmade disasters, cyber disasters, so

that same robustness and the same responsibilities that we have as the sector-specific agency and in the National Response Framework as ESF-12 are broadened based on what you envision that this office and what the Department is responsible to do.

So I am leaning forward into that. I am trying to redirect some of the activities that we have right now. I am looking at several of the investments that we have already made to make sure that they capture these other pieces so that we can make sure that we are operationalizing those for the Department.

Mr. WALBERG. We wish you well on that and would appreciate any involvement that we could have with you in identifying gaps and assisting in finding solutions to meet those needs.

Ms. EVANS. I would be happy to talk to your staff about what we are doing as we continue.

Mr. WALBERG. Thank you. I yield back.

Mr. OLSON. Thank you.

The Chair now calls upon the gentleman from the Commonwealth of Virginia, Mr. Griffith, for 5 minutes.

Mr. GRIFFITH. Thank you very much, Mr. Chairman. Thank you for being here today.

As we change our mix in our grid, we are becoming more and more reliant on natural gas, which means we have more and more natural gas pipelines running across the country which are subject to potential harm or attack. I do think that your agency is the right one to do it. The chairman mentioned a few minutes ago that people need to talk to FERC also, and we may need legislation to make sure that we have coordination going there.

I personally think we have given too much power to FERC as a Congress, and we need to take some of that back anyway. But along those lines, I find it interesting, because I think it would be helpful in this if we looked at some of the new technologies.

As a disclosure, I have a Corning facility in my district, and they were showing me a number of their products. They did not make this product in my district, but they have apparently got a fiber that they can put on top of a pipeline that can detect temperature change and vibrations that then shows you on a computer if somebody is driving a truck up near the pipeline, getting out of the truck, walking, starting to shovel. You can tell all of that from the vibrations. And if there is any kind of a leak, so you have got both the bad actor and then just the bad pipe issue, they can also—because the temperature changes and it can detect the temperature change, it can pick up a pinprick leak.

And I am just wondering why we aren't asking at least on the new pipelines that we are putting in for natural gas that we don't have some kind of a technology like that so that we can observe if somebody's trying to do something untoward or observe if there is just an accident about to happen. I think it would behoove us to do some of that.

Have you all looked at any of that or is that something you would be open to?

Ms. EVANS. I would be open to doing that. Based on my previous experience, I was a partner in a venture capital firm so I understand a lot of what you are talking about with the new technologies. I would say that trying to be a little disruptive that a lot

of the models that are currently being looked at right now are from the center going out, kind of the command and control piece. And what you are really describing is from the outside in.

Mr. GRIFFITH. Yes.

Ms. EVANS. And so that is going to change the architecture. And I view that that is what my role is is to be able to say, hey, if we agree on this, here is an architecture that we are recommending so that we can then talk to industry about it.

Based on that, and we are looking at it from a national security standpoint, it is my understanding the way this is supposed to work—so you guys can correct me here—is is that then that would feed into the FERC process, which then could then do and address some of the things that you are talking about, because we would show this is the modeling, this is how it works, here is a voluntary way that you can do it and can then be built into the standards process, which would then be overseen by FERC.

Mr. GRIFFITH. Well, and that may be, but I am not sure that they are completely on board with all of this, and so I would be more than happy to work with you all to see if we needed legislation to just say this is where we are going to go. You have to figure out first how you want to change that architecture, but it does seem to me that that is probably a better way to go instead of from the central office out, have the information coming in and—

Ms. EVANS. And I will be happy to brief you as we continue to do this work.

Mr. GRIFFITH. Yes, ma'am. And I appreciate that. I also should probably note that while I have seen this one product by one manufacturer, I am sure there are competing interests and I don't care which one gets picked. I just want to make sure—because I have a lot of constituents right now with two pipelines coming through the area, one through my district, and one through the neighboring districts.

There are a lot of people who were concerned about problems like we heard about from the Senator from Massachusetts and pumping stations, and they are worried about the safety of their communities and their homes, and it just seems like we probably could put their minds to ease.

I know when I have talked about this technology with those folks, they said, if only they were doing that, I would feel a lot better about it. They would still probably have some reservations, but they would feel a lot better that 20 years from now they weren't going to have a major problem. I thank you.

And I yield back.

Mr. OLSON. I thank the gentleman.

And seeing there are no further members wishing to ask questions, I would like to thank Secretary Evans for joining us today. And I just want to remind you, if you go out to Texas Tech this Saturday or sometime in the future to watch a football game between the Red Raiders and the Mountaineers, enjoy Lubbock, Texas.

Two things you should do out there: first of all, The Shack BBQ, The Shack BBQ, 2309 Frankford Avenue, Lubbock, Texas, the best barbecue in the Panhandle of Texas, much better than—sorry—

West Virginia barbecue, Virginia barbecue, North Carolina, Kansas City. We got the best.

Also, if you want to see a real tornado, Texas Tech has this thing called the National Wind Institute. They have this machine that generates small tornados just to study a tornado. So it is kind of cool. Go see that tornado. Enjoy Lubbock, Texas. You have to go out there.

Before we conclude, I would like to ask unanimous consent to submit for the record the following documents: a report from DOE's Office of Energy Delivery and Energy Reliability; number two, a letter from the committee to send to Secretary Perry; number three, response letter from DOE to the committee; number four, a letter to Speaker Ryan from EEI/NRECA, and American Public Power Association.

Without objection?

Mr. RUSH. No objection.

Mr. OLSON. No objection. So ordered.

[The information appears at the conclusion of the hearing.¹]

Mr. RUSH. Mr. Chairman—

Mr. OLSON. Yes, sir.

Mr. RUSH. I just want to say this to Secretary Evans. It has really been refreshing to hear your testimony this morning. You certainly have an understanding and broad knowledge of all the areas, and you have taken the time to really answer in a very effective way the questions that the Members have. And I just wanted to ask you to don't get tainted by the politics. I thought you were a very refreshing witness, and we look forward to working with you.

Ms. EVANS. Thank you, sir. I look forward to working with you as well.

Mr. RUSH. Thank you.

Mr. OLSON. Thank you. Amen.

In pursuit to committee rules, I remind Members that they have 10 business days to submit additional questions for the record. I would ask the witness to submit her response within 10 business days upon receipt of those questions.

Without objection, this subcommittee is adjourned.

[Whereupon, at 11:59 a.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

¹The report has been retained in committee files and also is available at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108725.pdf>.

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.

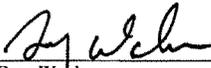
¹ P.L. 114-94, Section 61003

The Honorable Rick Perry
Page 2

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.

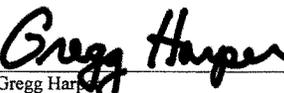
Sincerely,



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 Rick Perry
Page 3

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 Greg Walden
Chairman
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 Dannenfels, Deputy Assistant Secretary for House Affairs, Office of Congressional and Intergovernmental Affairs, at (202) 586-5450.

Sincerely,

Rick Perry

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 energy¹, 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.

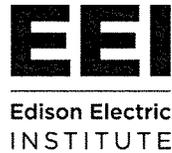
Role-Based Access Control (RBAC) - Honeywell developed the RBAC technology for the Experion® Process Knowledge System product suite, an energy delivery control system used extensively within the oil and gas industry. RBAC limits user access to the least needed to perform a given task, which helps reduce 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.



September 26, 2018

The Honorable Paul D. Ryan
 Speaker of the House
 H-232 The Capitol
 Washington, DC 20515

Dear Speaker Ryan:

We are writing to urge you to bring to the House floor key energy grid security bills passed earlier this year by the House Energy and Commerce Committee. We write on behalf of our membership, the U.S. electric power industry, which includes investor-owned electric companies, public power utilities, and electric cooperatives. The sector supports more than 7 million American jobs and contributes \$880 billion annually to U.S. gross domestic product, about 5 percent of the total.

The threat to the grid from cyber and physical attacks is real and growing. Protecting and maintaining electric sector security and reliability is a top priority for our associations and our members. To keep up with evolving threats, the industry welcomes close coordination with government partners. In the FAST Act, Congress recognized the role the Department of Energy (DOE) plays in grid security by designating DOE as the Sector Specific Agency (SSA) for physical and cybersecurity for the energy sector and provided DOE with the authority to address imminent grid security incidents. Additionally, the Cybersecurity Information Sharing Act (CISA) has been helpful in facilitating sharing between industry and government. Congress has been a constructive partner to enhance grid security.

The Energy and Commerce Committee passed several bills this year aimed at strengthening our shared responsibility to protect some of the nation's most critical infrastructure. We are particularly supportive of H.R. 5174, the Energy Emergency Leadership Act, and H.R. 5240, the Enhancing Grid Security through Public-Private Partnerships Act. H.R. 5174 would amend the DOE Organization Act to include energy emergency and energy security among the functions that the Secretary shall assign to an Assistant Secretary, with the intent to clarify and codify the functions of DOE's new Office of Cybersecurity, Energy Security, and Emergency Response (CESER). H.R. 5240 directs DOE to establish a program to facilitate and encourage public-private partnerships to promote and advance the physical and cybersecurity of the electric power sector.

September 26, 2018
Page 2

Each would be a welcome addition to electric sector security practices. Our industry has a defense-in-depth approach to grid security that starts with mandatory and enforceable cyber and physical security standards. To that, our companies add information sharing, planning, preparation, response, and recovery activities, as well as drills and exercises to regularly test our postures and capabilities. And as it is a shared responsibility, we partner with government at all levels and with other critical infrastructure sectors across many of these efforts.

In addition to passing these Energy and Commerce Committee bills, there is more that Congress can do, including modernizing the SAFETY Act to meet the new threat of cyber-attacks; allowing electric companies access to federal databases to counter insider threats; and increasing security clearances to key electric company staff, while at the same time rapidly declassifying and making available actionable information about grid security.

Thank you for considering this important topic. We appreciate your leadership and efforts to help improve the security posture of our nation, including the energy sector, and we look forward to working with you and your colleagues to keep the energy grid reliable, resilient, and secure.

Sincerely,

American Public Power Association
Edison Electric Institute
National Rural Electric Cooperative Association

CC: Democratic Leader Nancy Pelosi
CC: The Honorable Greg Walden, Chairman, House Energy & Commerce Committee
CC: The Honorable Frank Pallone, Ranking Member, House Energy & Commerce Committee
CC: The Honorable Fred Upton, Chairman, Energy Subcommittee
CC: The Honorable Bobby Rush, Ranking Member, Energy Subcommittee

The American Public Power Association is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide.

The Edison Electric Institute (EEI) is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for about 220 million Americans, and operate in all 50 states and the District of Columbia.

The National Rural Electric Cooperative Association is the national trade association representing more than 900 local electric cooperatives. From growing suburbs to remote farming communities, electric co-ops serve as engines of economic development for 42 million Americans across 56 percent of the nation's landscape. As local businesses built by the consumers they serve, electric cooperatives have meaningful ties to rural America and invest \$12 billion annually in their communities.

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

October 25, 2018

The Honorable Karen Evans
Assistant Secretary
Cybersecurity, Energy Security, and Emergency Response
U.S. Department of Energy
1000 Independence Avenue, S.W.
Washington, DC 20585

Dear Assistant Secretary Evans:

Thank you for appearing before the Subcommittee on Energy on September 27, 2018, to testify at the hearing entitled "DOE Modernization: The Office of Cybersecurity, Energy Security, 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 Members 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, November 8, 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 Subcommittee.

Sincerely,



Fred Upton
Chairman
Subcommittee on Energy

cc: The Honorable Bobby L. Rush, Ranking Member, Subcommittee on Energy

Attachments

[Ms. Evans did not answer submitted questions by the closing of the record.]

Attachment I—Additional Questions for the Record**The Honorable Fred Upton**

1. Through this Committee's efforts, DOE was established, in statute, as the lead sector specific agency for cybersecurity for the energy sector. This new mandate was included in the FAST Act of 2015.
 - a. While the "lead sector-specific agency" mandate is new, DOE has been engaged in this work for many years. What makes DOE equipped to serve as the lead agency?
 - b. What sets DOE apart from the other agencies, do they have the same level of technical expertise and established energy sector coordinating experience?
2. DOE's role in energy supply emergencies involves working with state emergency offices. Last year, the House passed legislation I authored, HR 3050, to enhance DOE's support of state energy assurance planning, including cybersecurity support.
 - a. Will the new CESER office include state energy assurance planning?
 - b. What are your priorities for continuing to assist state level emergency planning?
3. Ms. Evans, as part of CESER, the Cybersecurity for Energy Delivery Systems (CEDs) Program supports projects that advance cybersecurity capabilities for energy sector asset owners.
 - a. Ms. Evans, for electric utilities that are small or medium sized, why are programs such as CEDs particularly necessary?
 - b. How have industry partners used these resources?
4. Ms. Evans, in your previous role at OMB, you had the opportunity to work with the Department of Homeland Security, DOE, and other agencies – in your experience, what is necessary for successful coordination among federal agencies during times of emergency?
5. DOE hosted the Clear Path IV regional exercise in April 2016 in Oregon. This two-day event simulated a magnitude 9.0 earthquake and tsunami that caused catastrophic damage along the 700-mile long Cascadia Subduction Zone.
 - a. Why are exercises such as Clear Path IV beneficial for coordination between government and private entities?
 - b. What were the lessons learned? What improvements can be made?
 - c. What are DOE's plans for future exercises such as this?

6. DOE's National Labs serve as a critical strategic and technology partner when it comes to research, development, and demonstration of advanced technologies, analysis of cybersecurity risks and threats, modeling and simulation of cyber impacts, and information sharing on evolving threats. The Idaho National Lab is home to the INL Cyber Security Test Bed and is the only facility of its kind located within a national laboratory.
 - a. How is a full-scale test bed beneficial when it comes to cybersecurity of infrastructure control systems?
 - b. Does this program include coordination with the Department of Homeland Security?
7. Earlier this year, the Committee requested Secretary Perry explain coordination among DOE, the Department of Homeland Security, TSA and other agencies to ensure physical and cyber protection of pipelines. The Secretary responded to that letter, by stating: "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."
 - a. Can you talk about what DOE is doing in this leadership role to ensure there is a coordinated effort to protect the reliable flow of energy?
 - b. What is your relationship with the Department of Homeland Security, and how do you see DOE's work on pipelines fitting into the broader critical infrastructure protection mission of DHS?
8. This past August, the Department of Homeland Security held an event in New York City, hosting the "first ever" national cybersecurity summit. Secretary Perry participated in this summit.
 - a. At the summit, the DHS secretary spoke about prioritizing working with industry to improve information sharing systems. Can you explain what role DOE plays when it comes to the energy industry and how that fits in with DHS's work?
 - b. DHS also announced formation of a "National Risk Management Center"; This sounds like a reasonable effort, but can you explain DOE's role in identify and communicating critical infrastructure risks in areas of DOE expertise—such as the bulk power system?
9. DOE has released crude oil from the Strategic Petroleum Reserve in the wake of hurricanes in the Gulf of Mexico, when offshore oil production was temporarily offline. However, DOE is opposed to gasoline reserves because they are too costly and proven ineffective. In fact, the Administration has proposed eliminating the \$25 million per year Northeast Gasoline Supply Reserve in its last two budget proposals.
 - a. What are the disadvantages of gasoline reserves vs crude oil reserves?

- b. If you were able to reprogram that \$25 million dollars, and put it toward hurricane response, what would you spend it on?

The Honorable Kathy Castor

1. Whether this Administration wants to admit it or not, we are moving towards a renewable energy future. Even as the federal government retreats from energy innovation, cities and states are scaling up and market forces that are shouldering fossil fuels and driving renewables persist. Coal plants are closing at a rapid rate; the cost of renewable energy keeps going down; energy storage technology continues to improve and get cheaper; and digital technology is making electric markets cleaner and more efficient. Even Exxon Mobil has invested over \$1 billion annually in hundreds of research and development projects looking into alternative forms of energy. While this shift away from polluting fossil fuels to clean sources of energy is good for air quality, climate change, and consumers, renewable energy presents unique challenges to cybersecurity. Are you incorporating this move away from fossil fuels and towards renewable energy sources into your preparedness initiatives with respect to cybersecurity?
2. Another function of your office is to protect the nation's energy infrastructure not just from cyber threats but also from natural disasters. We know that renewable energy, energy storage technology, and microgrids can all increase resiliency in the electricity grid after extreme weather events. Are you considering the advantages renewable energy presents with respect to grid resiliency and emergency response in the face of a natural disaster?

Attachment 2—Member Requests for the Record

During the hearing, Members asked you to provide additional information for the record, and you indicated that you would provide that information. For your convenience, descriptions of the requested information are provided below.

The Honorable Markwayne Mullin

1. Are you doing specific classified briefings with industry when it comes to cyber attacks and vulnerability of our electrical grid in the oil and gas industry?

The Honorable Paul Tonko

1. Please share information on any DOE plan, technical assistance program, or funding available to assist small utilities, such as small public power authorities and rural cooperatives, improve their cybersecurity.

