NEAL R. GROSS & CO., INC.

RPTS PATERSON

HIF073030

DOE MODERNIZATION: LEGISLATION ADDRESSING CYBERSECURITY AND EMERGENCY RESPONSE

Wednesday, March 14, 2018

House of Representatives

Subcommittee on Energy

Committee on Energy and Commerce

Washington, D.C.

The subcommittee met, pursuant to call, at 10:00 a.m., in Room 2322 Rayburn House Office Building, Hon. Fred Upton [chairman of the subcommittee] presiding.

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

Staff present: Mike Bloomquist, Deputy Staff Director; Daniel Butler, Staff Assistant; Kelly Collins, Legislative Clerk,

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

Mr. Upton. Good morning. Good morning. So, this DOE modernization hearing is going to focus on the proposed legislation relating to core energy security missions of the Department.

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

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

For example, we directed the Department to modernize its strategic petroleum reserve and response capabilities. We clarified and enhanced DOE's role as the sector-specific agency for the energy sector, especially for critical electric infrastructure.

We moved through the House H.R. 3050 last summer to strengthen DOE's support for state energy emergency offices in their cybersecurity efforts and the common theme has been to update DOE's cybersecurity and emergency coordinating functions and provisions of technical assistance to other agencies, states, and asset owners.

So in keeping with these modernization efforts, the legislation today continues that work. H.R. 5174, the Energy Emergency Leadership Act, introduced by Mr. Walberg and Ranking

Member Rush, elevates the role in DOE and specifies certain emergency and preparedness functions to ensure full attention to the risks of cybersecurity and other threats to the energy sector.

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

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

Although several governmental authorities play a role, DOE has got to have the adequate visibility across the energy sector to ensure the federal, state, and asset owners are sufficiently prepared and coordinated and to efficiently deploy where needed its world class technological capabilities.

This bill certainly aims to assure that it can be done. Both H.R. 5239, the Cyber Sense Act of 2018, and H.R. 5240, the Enhancing Grid Security Through Public-Private Partnership Act, have been introduced by Mr. Latta and Mr. McNerney, two leaders on grid innovation.

The Cyber Sense bill, a version of which passed the House as part of H.R. 8 back in 2016, seeks to establish a voluntary

DOE program that would permit cybersecure products intended for use in the bulk power system.

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

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

I want to welcome back Undersecretary of Energy Mark Menezes, who returns from his appearance in January. I look forward to his comments and to talk about his own plans to elevate DOE's leadership in emergency response.

He's accompanied by Pat Hoffman, principal deputy assistant secretary in the Office of Electricity, who can provide technical perspective from her experience addressing cybersecurity and energy emergency functions.

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

We are going to hear from the state of Indiana's Emergency

Response Authority from Dominion Energy on pipeline security from EEI on electric cybersecurity and from the National Electrical Manufacturers Association to talk about cybersecurity of grid components.

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

[The prepared statement of Mr. Upton follows:]

**********INSERT**********

[The Bills H.R. 5174, H.R. 5175, H.R. 5239, and H.R. 5240 follow;}

**********INSERT**********

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

Mr. Chairman, I support the four bills before us and I want to specifically and respectfully acknowledge Mr. Walberg of Michigan who worked with my office on the Energy Emergency Leadership Act.

This bill will establish a new DOE assistant secretary position with jurisdiction over all energy emergency and security functions related to energy supply, infrastructure, and cybersecurity.

Mr. Chairman, while cybersecurity is an important issue, I would be remiss if I did not point out that today at this very same time students have declared this as National Walk-Out Day.

And as we speak, Mr. Chairman, students from across the country are leaving their classrooms to honor the lives of the 17 people killed at Stoneman Douglas High School last month and to press policy makers to pass common sense gun control laws.

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

Mr. Chairman, as policy makers, as parents, as grandparents,

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

Mr. Chairman, every single Democrat on the four Energy and Commerce committees sent a letter to Chairman Walden on March 7th urging him to hold hearings as soon as possible to address gun violence in America.

That followed a February 16th letter also signed by all 24 Democrats on the full committee to Chairman Walden and Health Subcommittee Chairman Burgess urging the Republican leadership to hold a hearing as soon as possible on federal investment in gun violence prevention research.

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

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

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

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

opportunities with our grid.

Our work, through the Grid Caucus, has led to the introduction of two bills we will discussing today. H.R. 5239, the Cyber Sense Act of 2018 would create a program to identify cybersecure products for the bulk power grid system through testing and verification.

The bulk power system is the backbone of American industry and provides all the benefits of reliable electric power to the American people. It's essential that we make this system as secure as possible as cyberattacks pose a serious threat to our electric grid.

Any vulnerable components of our grid is a threat to our security and this bill will go a long way to strengthen our system. Mr. Latta and I are also co-leads of H.R. 5240, the Enhancing Grid Security Through Public-Private Partnerships Act.

This bill will create a program to enhance the physical and cybersecurity of electric utilities through assessing security vulnerabilities, increase cybersecurity training, and data collection.

It will also require the interruption cost estimate calculator, which is used to calculate the return on investment on utility investments, to be updated at least every two years to ensure accurate calculations.

These two bipartisan bills, along with the other bills we have before us today, will help put us on the path to better

securing our electric utility system.

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

Thank you. I yield back.

Mr. Upton. Gentleman's time is expired.

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

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

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

Today's hearing examines legislation addressing cybersecurity and emergency response. It will help us respond to some of the most urgent challenges -- the reliability of our nation's energy infrastructure.

Because our energy infrastructure drives the entire nation's economy, I've made it a top priority for this committee to focus on emerging threats and proposed solutions to make our infrastructure more resilient.

We are looking ahead to make sure we are doing everything we can to protect our electric grid and our oil and natural gas infrastructure as well and improve our ability to respond when

the unexpected happens.

Because nearly all of our nation's energy infrastructure is privately owned and operated, the federal government needs to work closely with representatives of the energy sector and the companies in the supply chain that manufacture equipment and technologies.

In today's highly interconnected world, the threat of cyberattacks is ever present. So we have to be vigilant. We must also be prepared for physical threats whether they be sabotage or natural disasters like the hurricanes we experienced last year.

As the sector-specific agency for energy, the Department of Energy has a very important coordinating role to play and this function was on display earlier this year in response to Hurricanes Nate, Maria, Irma, and Harvey.

Many of us followed DOE's situation reports on the storms' impacts and the energy industry's recovery and restoration activities.

The Department of Energy's emergency responders in the field provided critical subject matter expertise and assisted with waivers and special permits to aid restoration.

To prevent a major fuel supply emergency, the Department of Energy's strategic petroleum reserve provided much-needed oil to refiners. The DOE also analyzed electricity supply to determine whether it needed to draw on its Federal Power Act authorities to secure the energy grid.

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

I join Chairman Upton in welcoming back Undersecretary of State -- Undersecretary of Energy, I guess, noted in tweets this morning -- Undersecretary of Energy Mark Menezes to our panel. I look forward to your comments on the Department of Energy's security priorities and its views on the legislation.

I also want to welcome the witnesses appearing on the second panel where we will hear a range of perspectives from state government, the energy industry, and supply chain manufacturers.

We are also joined by a witness from DOE's Idaho National Lab. I was there on Monday. Very much appreciated the briefings including the classified ones and so I am very impressed by the work that goes on at INL and our country should be very proud of the incredible men and women and the work they do there in every regard.

I also know that -- saw the unique capabilities to test system wide cybersecurity applications on a full scale electric grid loop.

INL is one of 17 DOE national labs tackling the critical scientific challenges of our time and the threats that come our way and I want to thank INL leadership and staff for sharing their research and expertise with the committee.

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

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

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

[The prepared statement of Chairman Walden follows:]

**********INSERT**********

Mr. Upton. Gentleman yields back.

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

Mr. Pallone. Thank you, Mr. Chairman.

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

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

Students and their families are justifiably frustrated with the inaction here in Washington. They are sick and tired of a president who says one thing in front of the cameras and then works behind the scenes to push the NRA agenda as soon as he thinks the cameras are focused somewhere else.

And they are also sick and tired of a Republican leadership in Congress that won't move forward on any common sense legislation, some of which has strong bipartisan support.

Americans have legitimate questions about the ever-increasing capacity of guns to kill in large numbers and the

ease with which people who are in danger to themselves and others can obtain them in the marketplace and those questions at least deserve to be explored through hearings in this committee.

Every Democrat on this committee has asked in two separate letters to the chairman for a series of five hearings on the gun violence epidemic.

We have not received a response and no hearings have yet to be scheduled. So I hope that the chairman and my Republican colleagues will finally see the need to schedule the five hearings we requested.

We don't expect them to necessarily agree with us or those participating in today's walkout on all the solutions to the gun violence epidemic.

However, we do hope that they will finally acknowledge the legitimate need to explore the questions we are asking and for this committee to take action.

And now, with regard to cybersecurity, I appreciate the majority taking these small but important bipartisan steps to enhance the Department of Energy's authorities with regard to our nation's energy infrastructure.

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

to prevent and respond to cyberattacks on these facilities.

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

H.R. 5175, the Pipeline and LNG Facilities Cybersecurity Preparedness Act, was introduced by Chairman Upton and Mr. Loebsack.

It would require the secretary of energy to carry out a program to establish policies and procedures that would improve the physical and cybersecurity of natural gas transmission and distribution pipelines, hazardous liquid pipelines and liquefied natural gas facilities.

Representative Latta and McNerney's bill, H.R. 5239, the Cyber Sense Act of 2018, is based on McNerney's language included in the last Congress energy bill.

It would require the secretary to establish a voluntary program to identify cybersecure products that can be used in bulk power systems.

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

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

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

And the bill would also establish a strategic transformer reserve program to reduce electric grid vulnerability to physical and cyberattacks, natural disasters, and climate change, and these are provisions that will better assure the security of our energy infrastructure and I hope this committee will consider them as we move forward.

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

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

I would just note for those of us that went on the bipartisan trip to look at the hurricane damage in Puerto Rico, on my local radio website this morning I see that the bridge that we saw that was washed out was rededicated yesterday with the governor and it's opened up.

It's been six months. It connects 60 families in a town of

about 33,000 folks. So I know we were there for an hour or so back in December. So I just thought I'd give that little update.

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

So welcome.

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

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

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

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

To demonstrate our commitment and focus on this mission, the secretary announced last month that he is establishing the Office of Cybersecurity, Energy Security, and Emergency Response, to be known as CESER.

This organizational challenge -- change will strengthen the department's role as the sector-specific agency or energy sector cybersecurity supporting our national security responsibilities.

The creation of CESER office will accomplish several goals -- one, build on the programs that we have today; two, elevate

the department's focus on energy infrastructure protection and response; three, enable a more coordinated preparedness and response to cyber and physical threats and natural disasters; and most importantly, four, create a structure and an office with an evolving mission to ensure sufficient authorities and resources are in place to address present and future threats.

The focus of the office will necessarily include electricity delivery, oil and natural gas infrastructure, and all forms of generation.

The secretary's desire to create dedicated and focused attention on these responsibilities will provide greater visibility, accountability, and flexibility to better protect our nation's energy infrastructure and support its asset owners.

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

The FAST Act designated DOE as the sector-specific agency for energy sector cybersecurity. Congress enacted several important new energy security measures in the FAST Act as it relates to cybersecurity.

The secretary of energy was provided new authority upon declaration of a grid security emergency by the president to issue emergency orders to protect, restore, or defend the reliability of critical electric infrastructure.

This authority allows DOE to respond as needed to threats of cyber and physical attacks on the grid, and although the administration does not have a formal position on any of the legislation under discussion today, we are pleased to continue to work with the committee to provide technical assistance.

And this morning, I would like to provide the subcommittee with some high-level priorities of the department in the context of the president's fiscal year 2019 budget request and which is the subject matter of today's bills.

Overall, investing in energy security and resilience from an all-hazards approach is vital, given the natural and manmade threats facing the nation's energy infrastructure, the energy industry, and the supply chain.

The fiscal year 2019 request would provide the department an opportunity to invest in early-stage research, network threat detection, cyber incident response teams, and the testing of supply chain components and systems.

Beyond providing guidance and technical support to the energy sector, our Office of Electricity supports R&D designed to develop advanced tools and techniques to provide enhanced cyberprotection for key energy systems.

OE cybersecurity for energy delivery systems' R&D program is designed to assist energy sector asset owners by developing cybersecurity solutions for our energy infrastructure.

OE co-funds projects with industry, our national labs, and university partners to make advances in cybersecurity capabilities. These research partnerships are helping to detect, prevent, and mitigate consequences of a cyber incident for our present and future energy systems.

It's important to emphasize that DOE plays a critical role in supporting the entire energy sector's efforts to enhance the security and resilience of the nation's critical energy infrastructure.

To address today's ever increasing and sophisticated challenges, it is critical for us to be leaders and cultivate a culture of resilience.

We must constantly develop, educate, and train a robust network of producers, distributors, vendors, public partners, regulators, policy makers, and stakeholders acting together to strengthen our ability to prepare, to respond, and recover.

As part of a comprehensive cyber -- energy cybersecurity resilient strategy, the department supports efforts to enhance visibility and situational awareness of operation networks, increase alignment of cyber preparedness and planning across local, state, and federal levels and leverage the expertise of DOE's national labs to drive cybersecurity innovation.

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

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

Thank you. [The prepared statement of Mr. Menezes follows:]

**********INSERT**********

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

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

I want to particularly thank, as Chairman Walden indicated in his opening statement, the willingness to work with the Idaho National Lab.

I know that he had a very productive day out there earlier this week and I will tell members of the -- our subcommittee that we are planning to have a classified briefing with them at some point in the near future so that we can -- we can know precisely what we have to be ready for and be able to ask questions in a -- in a classified setting. We are looking forward to setting that up in the next couple of weeks.

Let me just ask if you can help us identify other areas we might be able to clarify and strengthen your authorities to respond to energy supply emergencies, if we can have that commitment again today, and if you want to share any specifics today or certainly down the road where you can help us make sure that the worst doesn't happen and we will put out thousands, maybe

hundreds of thousands, maybe even millions of folks without the ability to hook into the needed energy resources for their daily lives.

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

Indeed, having a robust communications and coordination system with our industry asset owners is critical to do this. We currently serve on a variety of and coordinator subsector coordinating councils.

We work closely with industry. We have regular meetings. We coordinate. We make our labs available to those that need it.

We train, we practice, and we prepare. We do all that and, to be sure, we work with our sister agencies through the Energy Government Coordinating Council and work really on a daily basis with, as I mentioned, DHS and the other agencies.

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

It would be important -- it is important for the department with the bills that you have to be clear on the authorities, you know, that we have and if I could say, too, it would be important to ensure that we have the authority to get the resources that

we have when we are working with the other committees to ensure that we have the resources.

So we thank you for your leadership on that. But clear direction and the resources -- the authorization to have the resources would be very -- would be very helpful.

Mr. Upton. So DOE works with the Department of Homeland Security, TSA, and other agencies to ensure the protection of pipelines. But these agencies, as we know, certainly have other priorities.

It is my understanding that TSA, despite having some 50,000 employees, is only able to dedicate some -- a handful of folks, literally, three or four -- to pipeline security.

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

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

I will say that with pipelines both DHS and DOT co-chair, you know, that sector-specific pipeline industry. We are involved through the oil and natural gas subsector coordinating

council.

And so we have -- we have regular interaction with the agencies that you mentioned and other agencies but also with the industry.

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

Mr. Upton. Thank you.

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

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

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

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

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

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

Yes, a very important question. We are at probably a historical turning point from what has been going on in the past.

I had mentioned the ever increasing level of sophistication and the ever increasing number of threats. What has happened in the past simply is over and every day presents new challenges.

Some of the questions you asked, you know, would involve classified material that I can't get in today but it is public that we are facing threats today that we haven't seen in the past.

The Internet of Things, all software, all of these are providing opportunities for those that are very creative to try to attack our systems, and it's ongoing. It's daily. It's 24/7. It is around the clock.

Interestingly, as we know, that now it is machines that are doing all this and they're using artificial intelligence. So you have machines.

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

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

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

Pat, did you want to say something?

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

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

Mr. Menezes. We are doing what we can. I am not sure that we are doing everything that we can but we certainly are elevating education in the realm of preparedness in addition to, you know, response and ultimately recovery.

But it's going to be research and development and breakthrough technologies to be able to protect and defend our system and to be able to respond.

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

organizations.

And I can testify firsthand on the past success of the leadership of this committee and working with the ESCC and the industry partners in DOE's role.

I can assure you it was important for the electricity sector to have their CEOs participate, and when the CEOs participate they return to the company and they instill a culture of compliance and resilience and that they make many changes and they make sure that the workforce is very educated on these very technical and highly sophisticated programs.

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

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

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

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

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

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

Mr. Menezes. Well, let me go back to the days that I was

on that side of the dais in '05 when we decided to add the word cybersecurity into the mandatory reliability provisions that we put in EPAC of '05.

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

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

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

[Laughter.]

Mr. Menezes. I know that.

Mr. Barton. -- but roles do change.

Mr. Menezes. Yes. I don't think we have a formal definition. But --

Mr. Barton. Well, do we need one.

Mr. Menezes. -- I had mentioned that, you know, so cyber -- again, the Internet of Things and software typically are ways that they seek to gain entry into systems via those mechanisms.

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

Well, would you -- would you say that cybersecurity deals with the internet intercepting -- somehow making it difficult for

computer systems to operate, hacking into a controlled system or power plants or pipeline controls? Would that be a practical type of cybersecurity attack -- something like that?

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

You had mentioned the threat detection and the analysis, and it's not limited to just one sector of the energy industry, for example.

So it has to include -- you have points of potential entry into any systems and we are talking about supply chain today but, you know, we have generation.

We have all the distribution. We have transmission. We have the, you know, the producers, the vendors. It's all up and down the, you know, every point.

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

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

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

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

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

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

Mr. Menezes. Attacks?

Mr. Barton. Yes. Have there been attempts to --

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

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

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

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

try to figure out what is happening.

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

Mr. Menezes. Yes, sir.

Mr. Barton. Thank you.

Thank you, Mr. Chairman.

Mr. Upton. Gentleman's time has expired.

Mr. McNerney.

Mr. McNerney. Well, I thank the chairman and, again, I thank the witness.

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

Mr. Menezes. Yes, sir.

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

Mr. Menezes. We applaud the -- we applaud the committee for the leadership, you know, that you have shown and I think -- has one of them passed already, I believe? I mean, in past Congresses?

Mr. McNerney. Right. So --

Mr. Menezes. And I will say that on the supply chain -- you have already -- you have already seen action, right. You have seen action from NERC in proposing critical infrastructure protection standards. So you see it pending at FERC so certainly

your past efforts have generated that activity.

It's also generated activity here in this administration because in the fiscal year 2019 request we requested additional moneys to do -- to do what your bill is proposing to do.

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

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

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

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

So how can they reconcile those notions?

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

Ms. Hoffman. We see an increase in CESER budget line for

the 2019 request to -- yes, to $96 million.

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

Mr. Menezes. Well, can I point out a victory that we had -- that this office had with, you know, the administration?

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

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

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

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

Mr. Menezes. In this -- in this area. In this area.

Mr. McNerney. In this area?

Mr. Menezes. Yes, and they -- it's in our fiscal year 2019, you know, to set up CESER. It's all in the congressional

justification for it. So --

Mr. McNerney. So, I mean are you --

Mr. Menezes. -- so we have support in the administration on the topics that we are talking about today.

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

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

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

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

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

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

Mr. Olson.

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

My first question will be about Hurricane Harvey. I followed your reports on Hurricane Harvey -- the situation reports very closely as the storm hit and after the storm hit and the

impacts on our energy sector -- the Port of Houston and the petrochemical complex.

DOE was a good responder -- a good partner. Worked hand in hand with Governor Abbott, with the local county judges, my county judge, Bob Hebert, Fort Bend County -- county judge Matt Sebesta, Brazoria County -- county judge Ed Emmett, Harris County.

He helped to get waivers they needed and the assistant had to ensure the permits and waivers were issued without delay. That's very important.

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

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

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

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

Pat, do you have specific comments on that?

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

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

Some of the lessons learned is as we continue to move forward

the industry is on the front line so exchanging coordination of information is critical and absolute for having an effective recovery and restoration process and I think that's where you have seen the success as well as some of the lessons learned.

From a department perspective, being able to engage our power marketing administrations, to be continuing to use the strategic petroleum reserve are all important aspects of how the department can help in a restoration process.

The waivers and the coordination with industry were always very positive and helpful to support so being proactive in those areas as we continue.

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

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

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

You mentioned, Mr. Menezes, about AI -- artificial intelligence. I formed a caucus here in the House to look at those issues and I have a bill out to get us on board with AI because

that's our future to prevent some of these attacks.

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

AI is to empower people. It's not to have machines run our world but it's to empower people with information to make sound decisions when a disaster hits, like a hurricane.

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

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

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

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

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

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

Mr. Menezes. As a general rule, all the direction and --

that you can provide to us, particularly in the use of tools that we can use within industry, former Chairman Barton had asked about, you know, attacks on the system and we are here representing the department and to be sure, the department is, you know, subject to attacks.

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

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

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

I yield back. Thank you, Chairman.

Mr. Upton. Gentleman's time has expired.

Mr. Tonko.

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

I know DOE is taking its role as the sector-specific agency for cybersecurity seriously. But I have a few questions on the

reorganization of the Office of Electricity Delivery and Energy Reliability.

And, for the record, I am not necessarily opposed to the change but I would like to understand how it might affect DOE functions as we move into the future.

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

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

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

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

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

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

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

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

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

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

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

Mr. Menezes. What will happen with what?

Mr. Tonko. Other programs from the Office of Electricity.

Mr. Menezes. Well, they will continue and we will -- you

know, in a --

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

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

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

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

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

We are about busting these silos. Now, we are limited to the actual offices due to revenue streams. But as a practical matter, we collaborate. We share responsibilities and you know that we coordinate certainly all of our labs.

So what you're seeing over there is a coordinating effort and a collaborative effort so that we can make use of the resources that we currently have to do the things that were important.

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

Mr. Menezes. Well, we are in the process of identifying which employees will ultimately report to or be part of the new

office and, you know, there's a series of procedures and policies that we have to follow in order to do that. But we are going to be in full compliance with all of the regulations that we need to do.

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

Mr. Menezes. You have -- you have our commitment from that, sir.

Mr. Tonko. Okay. With that, I yield back, Mr. Chair.

Mr. Upton. Mr. Shimkus.

Mr. Shimkus. Thank you, Mr. Chairman.

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

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

Mr. Menezes. Yes, sir.

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

Mr. Menezes. That is fair, and it will be headed up by an assistance secretary.

Mr. Shimkus. And you want to, I think -- you used a good terminology -- you want to bust the silos that occur in major bureaucracies so we have people talking to each other.

Mr. Menezes. Yes, sir.

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

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

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

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

Mr. Menezes. They're on the front line. I mean, it is -- it is their -- they're, A, providing the service. They are doing

the things that we've come to expect from our energy infrastructure.

They own and operate the actual facilities, they develop the software, and they rely on the supply chain, all of which could be vulnerable. And so as the government, you know, agency responsible for that, we need to ensure that they do have the training, they have the know-how.

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

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

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

Mr. Menezes. Correct. In fact, you know, we -- the information sharing and analytical center, you know, has developed CRISP, which is the Cybersecurity Risk Information Sharing Program.

Mr. Shimkus. Thank you.

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

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

Mr. Shimkus. You know, let me go quickly. My time is almost expired. Talking about electromagnetic pulses either intentional or naturally occurring, the hardening of systems, the cost, and the communication with the private sector, I mean, the private sector when we talk about it they just say, oh, the cost is too much -- can't do that.

And there is some cost, but I think it is a concern that I hope that you all and maybe even this CESER subsection of DOE is talking about.

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

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

Mr. Menezes. Yes, it's -- yes. CESER is -- does have the energy security part of it so it would include the EMPs as well and the GMDs, if you want another acronym.

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

Mr. Upton. Mr. Loebsack.

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

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

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

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

Physical threats to pipelines and energy infrastructure do remain a significant threat, as everyone on this committee knows and you folks know. But today -- these days our pipeline system is increasingly technologically sophisticated as we get new

pipelines put in place and that does, I think, probably increase our vulnerability in some ways to cybersecurity attacks. And for the life of me, since I speak a little Spanish and even more Portuguese, I cannot figure out yet how to pronounce your name -- why it's only two syllables.

Mr. Menezes. It's Americanized Portuguese.

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

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

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

As we mentioned, DOE has to play a critical role in ensuring the safety and security of this infrastructure can you elaborate a little more about the level of vulnerability of our pipeline system to cyberattacks?

I mean, you have spoken about that some this morning already but can you elaborate even more, within the context of an open hearing, at any rate.

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

Perhaps the vulnerability on the pipelines exist because it's a transportation system, you know, at its sense and it -- probably the control mechanisms, the communication systems, and the operations systems, they may not be as fully integrated, say, as a fully operating electricity, you know, company in all sectors, for example, in the -- and so as a consequence it may

be the assumption that because they're more simplified, if you will, you might not have to develop technologies to make them as resilient as any other point of entry.

So as they are improving their efficiencies they are bringing in new softwares, you know, and new devices and, again, the result is you see the flow of product.

But as they become more sophisticated, we need to ensure that what they put in has the resiliency programmed in at the front end --

Mr. Loebsack. Right.

Mr. Menezes. -- so that it's resilient, and that's going to be the key. So --

Mr. Loebsack. Because I was kind of shocked actually at an earlier hearing when I found out that there isn't a lot of federal involvement, you know, when it comes to pipelines in the first place.

There's, you know, sort of oversight after they're already in place but it's -- there's precious little involvement as they're going in. I think that's one area where there can be more involvement to make sure that these things are put in properly and that they are secure.

Mr. Menezes. Yes. We are doing what we can in our role, you know, for the oil and natural gas subsector coordinating council and we do have regularly -- you know, meetings -- we have monthly meetings with the group and we have quarterly meetings

as well with the larger group, you know, that is co-led by DOT and DHS and we do bring in all those other agencies. So we are -- we have a structure within the existing authorities to try to address that.

Mr. Loebsack. Yes.

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

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

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

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

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

Mr. Loebsack. Thank you so much.

Mr. Menezes. Thank you.

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

Mr. Upton. Mr. Latta.

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

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

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

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

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

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

Our supply chains probably would be our most vulnerable areas and by supply chain it could be any component part, you know, that any of our energy partners, you know, would rely on.

That could make our entire system vulnerable. If point of entry could be on a -- what you think is a routine software program, perhaps to do accounting, you know, for a supplier of valves, for example.

Okay. So the importance has been noted in a couple of ways. NERC has already proposed CIPs -- the critical infrastructure protection standards -- which is pending at FERC to address this very supply chain issue with respect to, you know, the agencies that's responsible for developing our mandatory reliability provisions for the electricity grid and this administration in fiscal year 2019 has requested additional money so that we, with our labs and our experts, can similarly test these products for -- you know, for their vulnerabilities and we can mitigate those vulnerabilities. So we can make the whole system stronger by really addressing those most vulnerable, if you will.

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

Again, would you elaborate on the work that the DOE is doing to test the supply chain components and systems and also in a

follow-up of that, how does the quality control for supply chains help in ensuring that cybersecurity?

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

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

What we are looking at is actually partnering with industry to test and do a pilot program to test several components that are critical in the industry to do a deep dive testing of the components and subcomponents.

What the industry would like to understand is all the vulnerabilities so they can assess their risk and the risks that they are facing.

So part of what the NERC standards also emphasize is the disclosure of vulnerabilities and the continued testing.

One of the things that we want to emphasize is as we are looking at testing of components there may be a new vulnerability or a new threat vector that's discovered tomorrow. So what should be institutionalized is a process for continual improvement in cybersecurity.

As we've talked about the definition of cybersecurity being secure, information technology, secure firmware software, the information side of the industry, we really need to continually

test product, continually improve products, just like we would do from a manufacturing point of view.

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

Mr. Latta. When you're testing the products and getting that -- how do you get that information out to the industry? Because just like this past Friday I spoke at one of my electric co-ops in my district -- I have the largest number of co-ops in the state of Ohio -- and not too far in the past from that I also spoke at another one.

But how do you get that information out, especially with these products, to make sure that they know that they're, A, available and, B, that they're tested and they ought to be utilized once they're approved?

Ms. Hoffman. So the goal is to get the information out through the supply chain community and I am sure the next panel will talk about that and details of having that disclosure and that collaborative relationship with the industry with the mitigations and the solutions.

But the other area is through our national laboratories and through, say, the ISAC program to continue to really identify some of the vulnerabilities but get it out to industry and all the components and all the -- and all the sectors in the industry.

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

Mr. Upton. Okay. I would recognize Mr. Kinzinger. No, I am sorry -- Mr. McKinley.

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

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

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

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

Mr. Menezes. I did not see it.

Mr. McKinley. It just -- the fact that a lot of things have happened and I appreciate your remarks -- your answers back to Barton where you said that we are constantly under attack.

And maybe it's worked but I am saying there are groups saying the engineers can do this. They can still get past your system if they want to do that.

So the other thing, and just maybe it was coincidence in 2015

Ukraine was faced with a cyberattack. The Russians apparently are the ones that contributed to that.

What have we learned from that? Did we interact with the Ukraine and find out how that was shut down so we could prevent that from happening here?

Mr. Menezes. Since that occurred before I arrived, I will just --

Mr. McKinley. Just quickly, because I've got a series of more questions. Have we -- yes or no, have we worked -- interacted with them?

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

Mr. McKinley. Okay. But we've learned -- we've learned something from it.

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

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

Mr. McKinley. Okay, you are. Okay. What have we -- because they are -- it was -- they were able to display that just by entering 21 codes they could blow up a generator and thereby set in motion a blackout in the United States.

What have we done to prevent those 21 codes from being

introduced?

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

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

Mr. McKinley. Have we taken -- have they taken action, implemented things to prevent that from happening with that?

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

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

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

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

Mr. Menezes. Well, we need more infrastructure, to be sure,

both what you referenced. The New England ISO, together with NERC, has identified areas in the country where we rely heavily on natural gas for our power generation to ensure our resilient and the reliability of our grid.

It's in those constrained areas where it's important that we try to increase the infrastructure so that we can have adequate supply.

That has been the hallmark of this administration so that we have, you know, a sufficient diversity of fuels including natural gas.

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

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

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

Mr. McKinley. Right.

Mr. Menezes. It's not limited to that but it is a component

part of that. So it's also a function of working with the states because, you know, under federalism the states have a big role to play as to any interstate gas pipelines --

Mr. McKinley. I understand. I don't want a heavy hand --

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

Mr. McKinley. I don't want the heavy hand of the federal government stepping in. But there is a concern.

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

Mr. Menezes. Well, in the cybersecurity, clearly. I mean, this is -- your worldview changes as you get a security clearance and you get briefed in on what's happening.

I mean, I think you all have been read into a lot of this stuff. But yes, that causes me to stay awake and, frankly, as we have seen what are becoming, you know, common winter events when our system is stressed it seems as though, you know, we may be faced with an inadequate supply of what used to be baseload.

So the closure -- premature closing of what historically, you know, has been -- whether it's nuclear or clean coal, these facilities are going offline.

We are becoming more reliant on natural gas, which is not a bad thing. But it does have to get through pipelines and we've seen in the cyclone bomb, if you will, on the East Coast we see natural gas actually having price spikes, which forces the

operators to go to nuclear, coal, and, believe it or not, oil. So those are the things that keep me up at night.

Mr. McKinley. Okay. Thank you very much. I yield back.

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

I know we all recognize the very serious threat we face with cyberattacks. It can be especially difficult as the threats we face are constantly evolving and can vary significantly.

Individual bad actors are constantly attempting to obtain data -- bank routing numbers or medical records from everyday Americans -- while state actors, for example, North Korea's attack on Sony Pictures or China's break of the OPM files, represent a very different kind of threat. And for a lot of these nonstate actors, a very low barrier of entry.

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

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

You might have addressed this to some extent.

Ms. Hoffman. Sure. I appreciate the question. We've been

actively engaged with industry and we know that the core components of a strong cybersecurity program really looks at building capabilities.

And so our goal is to help industry build as much capabilities as possible so our R&D program is focussed on supporting that capability development.

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

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

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

So our R&D program, we also have two strong university programs, one with the University of Illinois and one with the University of Arkansas, to develop the next generation solutions

as well as partnerships with the national laboratories, looking at a moving target type activity to think about how could we make the system more dynamic.

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

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

Mr. Menezes. Right. I mean, as Pat Hoffman had testified earlier, the lessons that we learned with respect to the Ukraine.

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

So it's been ongoing. It had been a success story by all measures. We gain a lot from that. The industry gains a lot from that. I can -- I can vouch from industry that you take those lessons learned and you implement them.

And they could be as simple as revealing, for example, that you might need satellite phones, for example, because when you

lose your power you need to be able to communicate and you need to have enough satellite phones.

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

Mr. Kinzinger. Thank you.

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

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

Mr. Menezes. Right, and that -- to repeat what we had previously said, the short answer is yes. We currently have in place training programs throughout the process, whether it be at the front end on, you know, on preparedness.

We make sure that you have training, to anticipate, identify, you know, the new threat vectors, how to respond -- you know, how do you recover.

And, of course, the -- what's most important is to have the innovative R&D in place. So while driven primarily by our labs together with industry it's important that we train the workforce, and the workforce is not just in the departments, you know, or

the governments.

It's in the industries themselves and it's not limited to just the big player in the industries but it's all the participants which we have in place right now to cover, you know, the large utilities of all sizes whether you're a muni or a co-op.

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

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

I yield back.

Mr. Upton. Mr. Griffith.

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

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

I would hope that you would include me in whatever response you give him because I am interested in that.

And we have a new pipeline that's being built in my district and a lot of my constituents are concerned about all kinds of

issues.

And so I would also ask, and not expecting you to have an answer today, but also ask that you take a look at what can we do as far as making sure that the new pipelines have technology in them that lets us know if there's an earthquake in the area, a collapse somewhere.

The faster that people know about it the faster we can respond. Folks are very concerned about, you know, possible breaches.

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

Likewise on that same vein -- I am going to give you a second here but I just want to get it all out before I forget something -- it would also seem to me that DOE would want to know who had extra capacity and a new pipeline with the right kind of technology could tell you instantly whether or not they had the ability to

take on more natural gas at a particular moment should there be a failure in some other area so that we can get that natural gas to where it needs to go by rerouting it possibly.

And we've got two coming through Virginia, one through my district, one going through Bob Goodlatte's and other districts.

While we are laying this pipe is the time to put in any new innovations and new thoughts into that, and I am just hoping that DOE has some thoughts and plans.

And I will give you an opportunity to respond to that now but also ask that you get back to me on all those thoughts that are important to me intellectually but also important to the constituents in my district -- that they want to feel a little bit safer about this pipeline coming through their back yard.

Mr. Menezes. Well, thank you for the series of questions and the commentary. Of course, we -- you know, we agree with the issues that you have identified. If I can just take a quick crack at it, if you will, Pat, and then I will defer to you.

But, first of all, with respect to developing the technology on the -- on the resiliency side of it, first of all, you hit on a key point.

As you know, our system is becoming more and more open. We are actually excited about all the possibilities of getting more inputs on either side of the meter. Individuals will -- to be able to gain input.

We are -- we are increasing the flexibility of our grid for

a variety of good reasons -- make it more resilient, more reliable. However, every time we make it smarter it's a new entry -- it's a potentially new entry.

So in my conversations with the lab directors, for example, whom we meet with regularly on this, as they're developing ways to make things more efficient or greater access, more individuals who can get electrons -- you know, produce whatever they want when they want it, as an example, I make sure that my message to them is as you develop that new technology, please, at the front end, design it in such a way that it is resilient and it is secure. And so that message is out and they are -- they are doing that. So that's on that question.

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

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

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

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

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

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

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

Mr. Upton. Mr. Johnson.

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

I dare say that most people don't really think about the implications of cybersecurity when it comes to infrastructure and the importance of it.

So when looking at emerging cybersecurity risk and particularly threats of the highest consequence to energy infrastructure, it seems critical to me that DOE have full visibility on the greatest infrastructure risks and consequences.

Do you believe, Mr. Undersecretary, at this point that DOE

has sufficient visibility to day on what those risks and vulnerabilities are?

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

Mr. Johnson. Yes.

Mr. Menezes. So it is -- we are looking -- we are doing okay today, as several members have identified. It seems as though while we have the constant threats we've been able to, you know, avoid a major catastrophe.

But we want to make sure that going forward we have the visibility and the resources. I think Ms. Hoffman would like to say something.

Mr. Johnson. Sure.

Ms. Hoffman. I think it's important to continue to support the information sharing between industry and the Department of Energy in understanding the number of events that are going out.

The critical need, as the undersecretary has talked about, is moving forward -- that we want to get ahead, we want to see what the next generation threats are.

And so that close public-private partnership and information sharing and the flexibility and the freedom for the industry to

voluntarily share information with the department is absolutely important.

Mr. Johnson. Okay. I am encouraged by that answer because I've long held the belief and I still do that this is not -- this is not an issue that has an ending to it.

I mean, this is not a race that we are going to run and cross the finish line. As soon as we figure out how to keep the bad guys from getting into our networks, especially in the digital world where everything is connected, as soon as we figure that out, we've got another problem right on the tail end of that.

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

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

Mr. Menezes. I will take the -- you know, the larger view and I will defer then to Ms. Hoffman on the specifics.

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

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

increasing threat.

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

Mr. Johnson. Okay.

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

It's continuing to support the threat analysis programs such as the CRISP program where we are actively looking at indicators and looking at sharing of information, whether it's an indicator that's discovered by industry or by the federal government and allowing that to be shared with industry as quickly as possible.

And then it's really getting to the point that we can get to machine-to-machine sharing and we can get proactive whether it's with our official intelligence, whether it's with other capabilities.

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

Mr. Johnson. You know, one of the things that -- when I -- when I was on active duty in the Air Force even as far back as the -- as the mid-'90s as the world began to be interconnected and we started talking about things like network-centric warfare

and the digital age and what that meant to national security, risk management and risk assessment was -- began to be pushed down in the Department of Defense as part of our overall culture. So it's one thing to have our leaders talking about it.

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

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

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

Mr. Johnson. Okay. Well, thank you very much.

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

Mr. Upton. Mr. Long.

Mr. Long. Thank you, Mr. Chairman, and Mr. Menezes, when you opened this morning you mentioned I believe that the cyber threat from the bad actors, sometimes it boils down to their artificial intelligence attacking our systems and our defense is our artificial intelligence trying to prevent their artificial

-- can you speak to that for just 30 seconds and kind of -- I mean, that's a --

Mr. Menezes. I will let --

Mr. Long. -- can of very severe worms, I think.

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

Ms. Hoffman. So when -- so when we talk about cybersecurity, it's really looking at information, technology, and control system technology.

But a lot of it is layering computer protections against computer attacks and computer protections, and so you keep layering on, you know, different information technology solutions to thwart information-based attacks on the system.

So it becomes an information and a controlled system but a capability of an actor to use that information technology against the industry and so it becomes a very broad attack surface.

And so what we need to do is think about what is the right information technology placement in industry that provides the capability industry requires but doesn't provide that broader attack surface.

Mr. Long. Kind of reminds me of a friend of mine 40 years ago that had a restaurant and he said that he laid awake half the night trying to figure out how to keep his employees from stealing from him.

But the problem was that his employees laid awake the other half of the night trying to circumvent his new system.

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

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

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

So when we prioritize those things that we are addressing, it is -- obviously we have to address those threats that we know as those threats are evolving. I mean, that's the first thing.

We have to continue everything we've done in the past because they can always revert to prior technology, so we can't ignore that. We build on -- we build on what we know and then we try to anticipate where we think the next threats are coming from.

So we have to -- we have to make sure that we can respond to what we know and we have to be able to identify those threats.

As I mentioned earlier, we have a lot of hits on our systems. They could appear random. Because of our modelling techniques

it could be that we are -- we are witnessing ways -- new ways that they are trying to figure out ways to gain access to the system.

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

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

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

Mr. Menezes. I will defer to Pat.

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

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

We will look at the capabilities that industry has for dealing with this attack, trying to understand what is the cause -- the root cause of the attack but then also work with industry on providing mitigation measures and any support that's needed.

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

Mr. Long. Okay. Thank you.

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

Mr. Upton. Mr. Walberg.

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

Back when the Department of Energy was organized as a Cabinet agency back when I was in graduate school in 1977, the largest energy security concern was fuel supply disruptions, not electricity disruptions or cybersecurity, as we are talking about now.

As you would expect, the department's Organization Act reflected those concerns. Times have changed and we should be thinking differently now about energy security and emergency preparedness. So I am glad we are doing that here today.

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

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

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

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

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

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

Mr. Menezes. Right. Well, and the secretary announced the setting up of CESER. That's going to be -- that is a clear demonstration of his commitment and his organizational vision for the department, to highlight it, to increase the visibility, to coordinate efforts, and to be a source of additional guidance from Congress, the White House, and other agencies.

So he's committed to that and he's showing it in a very real and measurable way.

So that's what we are proposing and that's what we are doing.

And then we look forward to working with you, the appropriators, others, you know, to ensure that it has the adequate resources it needs to accomplish the goals that we hope it accomplishes.

Mr. Walberg. Ms. Hoffman.

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

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

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

Mr. Menezes. Yes, sir.

Mr. Walberg. Let me ask one more question, Mr. Menezes. Do you believe that elevating cybersecurity functions to a Senate-confirmed assistant secretary level will help

intergovernmental and interagency communication as well as multidirectional information sharing with DOE's ability to appropriately and quickly address cyber-related emergencies?

Mr. Menezes. I do. The key point -- the key part about being a Senate-confirmed appointee is the accountability that you have to maintain with the two branches of government.

You're in the executive branch and you're confirmed by the Senate, and so it forces you to work with Congress and to fully explain yourself to the executive branch.

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

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

I yield back.

Mr. Upton. Mr. Duncan.

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

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

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

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

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

It's a prime example of enhancing grid security through

public-private partnerships, which is the title of one of the bills we are reviewing today.

So I encourage DOE to continue looking for these opportunities, especially since the new Office of Cybersecurity, Energy Security, and Emergency Response. I guess you're going to pronounce that as CESER. Everything in government has an acronym, right?

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

Ms. Hoffman. So thank you for the question.

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

The national laboratories have important testing capabilities. You mentioned one of them. There are several capabilities that we are utilizing from an EMP perspective. We have partnership with the -- we have partnered with the industry in looking at an EMP strategy.

We have also worked with EPRI as they're looking at their mitigation and testing plan. We are looking at what the department can do to support EMP testing. As you know, it's a very expensive process to do EMP testing.

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

Ms. Hoffman. Yes, I am familiar with Clemson several other

activities in the labs.

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

Ms. Hoffman. I don't know if visited that facility but I've visited the --

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

Ms. Hoffman. Yes, sir.

Mr. Duncan. Both of you?

Mr. Menezes. Yes, sir.

Mr. Duncan. Okay.

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

When people think about infrastructure they think about roads, bridges, water, sewer, airports, port deepening, et cetera.

But grid hardening and our transmission of power supplies, so talking about -- I think Morgan Griffith talked about natural gas pipelines and other things. But are elements within DOE, discussing with the White House and members of Congress, specifically probably TNI Committee -- transportation and infrastructure -- plans to include grid hardening and cybersecurity as part of the infrastructure package or elements

within the DOE having those conversations?

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

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

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

Mr. Duncan. On this subject?

Mr. Menezes. Excuse me -- on the other body -- on the infrastructure -- on the president's infrastructure bill. And so --

Mr. Duncan. So let me just -- because my time is running out --

Mr. Menezes. So energy is a --

Mr. Duncan. -- is this a priority for the White House with regard to an infrastructure package -- grid hardening and cyber security as part of the infrastructure package and should it be?

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

Mr. Duncan. Let me encourage you to go back to Secretary Perry and go back to your bosses and others in the White House

you have conversations with and let's make this a priority in the upcoming infrastructure package.

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

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

Mr. Walberg. [Presiding.] I thank the gentleman. Seeing that there are no further members wishing to --

Mr. Rush. Mr. Chairman. Mr. Chairman.

Mr. Walberg. Mr. Rush.

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

Mr. Walberg. Without objection.

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

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

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

Mr. Rush. Thank you, Mr. Chairman.

Mr. Walberg. I thank the gentleman.

Again, seeing that there are no further members wishing to

ask questions, I would like to thank the panel for being with us today and providing us the answers and probably further questions that we'll have down the road.

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

Mr. Walberg. Thank you, sir.

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

[Pause.]

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

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

Our second witness panel for today's hearing includes Tristan Vance, director -- chief energy officer, Indiana Office of Energy Development -- welcome; Zachary Tudor, associate laboratory director for National and Homeland Security Idaho National Laboratory -- welcome; Mark Engel, senior enterprise security advisor, Dominion Energy -- welcome to you; Kyle Pitsor, vice president, government relations, National Electrical Manufacturers Association -- welcome you; and Scott Aaronson, vice president, security and preparedness, Edison Electric Institute. Welcome.

We appreciate you all being here today. We'll begin the

panel with Mr. Tristan Vance, and you are now recognized for five minutes to give an opening statement and I am sure you're well aware of the lighting format.

Welcome. We recognize you.

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

STATEMENT OF MR. VANCE

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

I am Tristan Vance, the director of the Indiana Office of Energy Development. I also serve as the chief energy officer for the state of Indiana and I am testifying on behalf of the National Association of State Energy Officials -- NASEO.

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

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

provisions.

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

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

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

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

NASEO's 2017 bipartisan recommendation to the Trump administration called for such action. In my capacity as a NASEO board member, I co-chaired the NASEO transition task force which developed this important recommendation.

We believe such action will save lives and protect the economy of communities in every region of the country.

The Energy Emergency Leadership Act will elevate this core DOE function and we strongly support the bill. I also want to stress the importance of CESER having a well-defined state energy security program and robust program management resources.

A strong DOE state energy emergency partnership such as the one that exists today in the DOE Office of Infrastructure Security and Energy Restoration is critical to respond to emergencies effectively.

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

While our nation has not faced a cybersecurity event with significant energy supply impacts, we should adopt the lessons learned from recent natural disasters for our cyber preparedness.

We share the subcommittee's concerns and the threat cybersecurity presents to the energy system -- electricity, natural gas, and petroleum.

A cyberattack to the energy system during a natural disaster is a horrific scenario. However, we must address such possibilities.

For example, the DOE-NASEO-NARUC Liberty Eclipse emergency exercise in 2016 focused on a combined cyber and natural disaster event.

These low-cost regional exercises are essential. We also strongly support H.R. 5239 and H.R. 5240 and believe states can leverage these activities. They build upon the work of utilities, DOE, and the states.

For example, in Indiana we created the Indiana Executive Council on Cybersecurity to lead a public-private partnership and have created a state-led exercise series focused on SCADA systems for electric and water utilities.

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

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

Thank you.

[The prepared statement of Mr. Vance follows:]

2219 **********INSERT**********

Mr. Walberg. Thank you.

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

STATEMENT OF MR. TUDOR

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

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

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

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

The potential consequences of a sophisticated cyberattack

create an imperative that federal agencies, labs, and industries collaborate to build capabilities and develop innovations that reduce the unacceptable risks associated with a cyberattack.

DOE, INL, and our other national laboratory partners are providing leadership and resources to assure that the nation has detective capabilities to reduce these risks.

These capabilities include a broad array of science and engineering programs, extensive teams of multidisciplinary national laboratory researches, unique user facilities and test beds for experimentation at scale, and a breadth of collaborative relationships with industry, universities, and federal agencies.

With regard to reducing cyber risks, INL's Cybercore Integration Center, known as Cybercore, performs research, development, testing, and evaluation of technologies and information products to prevent, detect, and respond to cyber vulnerabilities and intrusions.

When shared through public-private partnerships, these solutions create barriers to attack, mitigate the consequences of an attack, and enable rapid restoration of energy sector operations.

Specific examples of technology advancement that are reducing risks include, with DOE and other agencies, INL supported the recovery and information sharing in response to the cyberattack on Ukraine's electric grid. After our post-event analysis, INL developed and is conducting unique cyber strike

workshops for U.S. asset owners and operators to learn how to protect against similar attacks.

INL developed and completed a pilot study of our consequence-driven cyber-informed engineering methodology, or CCE, with Florida Power and Light.

CCE leverages an organization's knowledge and experiences to engineer out the potential and highest -- for the highest consequence cyber events. Briefings of the study's results were shared with the Section 9 electric utility partners, congressional staffers, and government leaders. A second pilot is currently underway.

INL also is advising the National Security Council on implementing the methodology with a larger set of participants.

INL is one of several national laboratories providing technical information and strategic planning guidance to assist CESER develop -- leadership to develop infrastructures, capabilities and processes for reducing cyber and physical risk.

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

Some examples of INL's current partnerships that are

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

DOE's pilot program, cybersecurity for the operational technology environment, is providing a forum for situational awareness for cyber risks among industry partners and stakeholders.

Examples I described demonstrate that DOE and INL are making significant progress in reducing the risks to our energy sector. However, with the increasing capabilities of our adversaries and the increasing complexity of our energy system technologies we will not completely eliminate all risks.

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

I look forward to your questions. Thank you.

[The prepared statement of Mr. Tudor follows:]

**********INSERT**********

Mr. Walberg. Thank you.

Mr. Engels, you're recognized.

STATEMENT OF MR. ENGELS

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

My name is Mark Engels and I am a senior enterprise security advisor at Dominion Energy. Dominion Energy is one of the largest producers and transporters of energy with a portfolio of approximately 26,200 megawatts of electricity generation, 6,600 miles of electric and transmission and distribution lines, 15,000 miles of natural gas pipeline, and the Cove Point liquefied natural gas facility in Maryland.

We operate one of the largest natural gas storage systems in the U.S. with one trillion cubic feet of capacity and serve more than 6 million utility and retail customers.

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

For Homeland Security Presidential Directive 7, both the Department of Energy, the Department of Homeland Security in coordination with the Department of Transportation function as the sector-specific agencies for natural gas pipelines and LNG.

The fact that pipelines have two SSAs comprised of three

different federal agencies cannot be understated, especially when it comes to interagency coordination in advance of, during, and post-incident operations.

The key to this coordination is maintaining a productive relationships between the energy government coordination councils' two co-chairs -- DOE and DHS -- and the oil and natural gas sector coordinating council.

The ONG SEC is comprised of owners and operators from 20-plus industry trade associations representing all aspects of the oil and natural gas sector.

I encourage DOE and TSA, who has regulatory authority for pipeline security, to develop a memo of understanding that outlines roles and responsibilities for dealing with cyber and physical security of natural gas pipelines and LNG.

TSA already has an MOU with the Department of Transportation's Pipeline and Hazardous Materials Safety Administration, or PHMSA, which has responsibility for pipeline safety.

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

The language in H.R. 5175 Section 22 could introduce complexity and confusion when it comes to DOE's involvements with states. Individual pipeline companies, Dominion Energy

included, already have longstanding relationships with state emergency response organizations, public utility commissions, and law enforcement for all hazard events.

H.R. 5175 directs DOE to focus on advanced cybersecurity applications, pilot demonstrations, develop workforce curricula, and provide mechanisms to help the energy sector evaluate, prioritize, and improve physical and cybersecurity capabilities.

Dominion Energy has worked with DOE and several national labs on a number of efforts that align with the proposed legislation.

They include being a peer reviewer for the Department of Energy's Cybersecurity for Energy Delivery Systems Program, participation into workforce and training efforts, Cyber Strike -- a hands-on workshop communicating lessons learned associated with the Ukraine grid attacks -- and Attack, an approached developed by INL to aggregate and evaluate cyber risk-related information.

Dominion Energy is a member of both the downstream natural gas and electricity information sharing and analysis centers, both who have benefited -- both of which have benefited from intelligence provided by DOE's Cybersecurity Risk Information Sharing Program, or CRISP.

Dominion's -- Dominion Energy and other national -- and other natural gas pipeline companies have worked very closely with TSA and DOE on cyber and physical security to build a partnership based on trust and respect.

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

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

[The prepared statement of Mr. Engels follows:]

**********INSERT**********

Mr. Walberg. Thank you.

Mr. Pitsor.

STATEMENT OF MR. PITSOR

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

My name is Kyle Pitsor, vice president of government relations for National Electrical Manufacturers Association, representing about 350 manufacturers of electrical equipment and medical imaging technologies.

NEMA and our member manufacturers have made cybersecurity a top priority. As the manufacturers of essential grid equipment, NEMA companies are a key line of defence against both physical and cyberattacks in the electricity transmission and distribution system.

We understand that a secure product supply chain is inherent to a secure grid and cybersecurity aspects should be built into, not bolted onto manufacturers' products whenever possible.

Manufacturers also understand that managing cybersecurity supply chain risk requires a collaborative effort and open lines of communication among electrical utility companies, federal and state and local governments, and suppliers of the full spectrum of grid systems and components, both hardware and software.

I would like to mention briefly some of the industry wide efforts NEMA and its members have pursued to establish best

practices for supply chain and manufacturer cybersecurity hygiene and then make a few comments on the Cyber Sense Act and the Enhancing Grid Security Through Public-Private Partnership Act.

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

NEMA published a white paper on cybersecurity, supply chain best practices for manufacturers that addresses supply chain integrity through four phases of a product's life cycle -- the manufacturing, delivery, operation, and end of life of a product.

This month in March, NEMA members have approved a new technical document detailing industry best practice cyber hygiene principles for electrical manufacturers to implement in their manufacturing and engineering processes.

The document raises a manufacturer's level of cybersecurity sophistication by following seven fundamental principles that are outlined in my statement.

With the above-mentioned two industry developed and cybersecurity best practices documents in mind, I will make a few comments about two of the bills under consideration today.

First of all, with respect to the Cyber Sense Act, NEMA member manufacturers support voluntary cyber evaluation of products used in the transmission, distribution, storage, and end use of electricity.

However, the specific requirements of any such program need to be carefully designed in close collaboration with manufacturers and other stakeholder groups and developed via an open and transparent process.

We recommend that any cybersecurity evaluation program abide by a set of principles that we've outlined in our written statement.

With respect to the Enhancing Grid Security Through Public-Private Partnership Act, NEMA supports the concepts included in the draft legislation.

With respect to Section 2, NEMA agrees that voluntary technical assistance efforts should be available to provide electric utilities with information and resources to effectively prepare for and combat both physical and cybersecurity threats.

We also agree that this technical assistance should be provided in close collaboration with state governments and public utility regulatory commissions as well as with equipment manufacturers.

Including manufacturers in the training and technical assistance efforts will ensure that products are installed and maintained as intended to limit the risk of cyberattack resulting from the proper -- possible misuse of a product.

NEMA also supports the recommendations included in Sections 3 and 4 of the legislation. One additional outage index that we recommend be included in Section 4(b) of the draft legislation

is the Momentary Average Interruption Frequency Index.

Momentary outages cost U.S. electricity consumers over $60 billion in 2014 and account for more than half of all power outages. Inclusion of this index, we believe, will improve the interrupter cost estimate information produced by the Department of Energy.

In conclusion, NEMA and member company manufacturers recognize that cybersecurity risks are constantly evolving and changing and requires a shared responsibility by all stakeholders.

NEMA looks forward to working with you as a resource to this committee as you continue your work to address cybersecurity concerns in the energy sector.

Thank you, and I look forward to any questions.

[The prepared statement of Mr. Pitsor follows:]

**********INSERT**********

Mr. Walberg. Thank you.

I now recognize Mr. Aaronson.

STATEMENT OF MR. AARONSON

Mr. Aaronson. Thank you, Mr. Chairman, Ranking Member Rush, and members of the subcommittee. I appreciate the opportunity to testify here today.

For EEI's member companies, which includes all of the nation's investor-owned electric companies, securing the energy grid is a top priority. I appreciate your invitation to discuss this important topic on their behalf.

The electric power industry, which includes investor-owned electric companies, public power utilities, and electric cooperatives, supports more than 7 million American jobs and contributes $880 billion annually to U.S. gross domestic product -- about 5 percent of the total.

That 5 percent is truly the first 5 percent, responsible for generating and delivering the energy that powers our economy and our way of life.

Our members own and operate some of the nation's most critical infrastructure and they take that responsibility seriously. EEI's member companies prepare for all hazards -- physical and cyber events, naturally occurring or manmade threats, and severe weather of every kind.

To address multiple threats, our companies take what's known as a defense in-depth approach with several layers of security. I would like to highlight three main areas of focus -- standards,

partnerships, and response and recovery.

First, standards -- through a process created by Congress the electric power sector is subject to mandatory enforceable critical infrastructure protection, or CIP, regulatory standards for cyber and physical security.

Through these standards, the bulk power system enjoys a baseline level of security. Standards are important, but with intelligent adversaries operating in a dynamic threat environment, regulations alone are insufficient and must be supplemented.

That brings me to the second area of focus, which is partnerships, which you have heard a lot about today. You heard it from DOE and you will hear it from this entire panel -- security is a shared responsibility.

None of us can do this alone. To be successful in this environment, industry and government must partner, and as you heard earlier, we are.

I am here this morning in my role as EEI's vice president for security and preparedness but I am also privileged to be a member of the secretariat for the Electricity Subsector Coordinating Council.

The ESCC is comprised of CEOs of 22 electric companies and nine major industry trade associations representing the full scope of electric generation, transmission, and distribution in the United States and Canada.

Through partnerships like the ESCC, government and industry leverage one another's strengths. This partnership manifests itself in many ways including deployment of government technologies, like CRISP, which you have heard about, multidirectional information sharing, drills and exercises, and facilitating cross-sector coordination.

What makes the ESCC effective is CEO leadership across all segments of the industry. This structure provides resources, sets priorities, drives accountability.

Furthermore, CEOs serve as a draw to other senior counterparts in industry sectors and in government. The unity of effort driven by industry working with government has produced significant tangible results.

Finally, the third area of focus is response and recovery. The electric power sector is proud of its record on reliability but outages do occur.

The past year has made one thing abundantly clear -- we can't protect everything from everything all of the time and investments help companies restore power and be prepared.

Our industry invests more than $120 billion each year to make the energy grid stronger, smarter, cleaner, more dynamic, and more secure.

In addition, the industry's culture of mutual assistance unleashes a world-class workforce amidst the toughest conditions to restore power safely and effectively.

Today, we have supplemented that traditional response in recovery with a 21st century edition -- cyber mutual assistance. So far, more than 140 entities are participating in the program, covering more than 80 percent of U.S. electricity customers.

That brings me to the bills before the subcommittee today. We appreciate both Congress and the Trump administration's support of the electric power sector.

Just as EEI's member companies evolve to meet new threats, our government partners continuously improve their posture through these new initiatives.

For example, we applaud DOE Secretary Perry and his team for establishing DOE's new Office of Cybersecurity, Energy Security, and Emergency Response, or CESER.

Legislation passed by this committee codified DOE's role as the sector-specific agency -- thank you -- and we believe the elevation of CESER will deepen the relationship between our industry and DOE on issues of cybersecurity and energy grid response initiatives.

In his testimony, Secretary Menezes mentioned DOE's establishment of the supply chain testing facility. We are interested in the details of that program. The subcommittee is also aware that through the NERC/FERC process as mandatory supply chain standard will be implemented soon.

The committee should consider those efforts when adopting legislation related to supply chains.

Finally, I would like to mention a report included in the Enhancing Grid Security Through Public-Private Partnerships Act looking at distribution, cyber, and physical security.

EEI supports this report because it could address several emerging questions that many in the industry also are asking.

What considerations should be made to protect a distribution system that is outside of mandatory NERC CIP standards?

How can we secure newer technology that is largely consumer grade but may increase the energy grid's attack surface?

A collaborative risk-based approach to security at the distribution level is essential. This report should drive that approach and consider the many different entities in the distribution grid, electric companies, and others.

Again, I appreciate you holding this hearing. I look forward to answering any of your questions.

[The prepared statement of Mr. Aaronson follows:]

**********INSERT**********

Mr. Walberg. Thank you. Thanks to the panel for your very efficient use of the five minutes time. Maybe it would be an example to myself and my colleagues.

Now privileged to represent the neighbor to the south who guards my border, Mr. Latta.

Mr. Latta. Well, thank you very much, Mr. Chairman, and I appreciate our panel for being here. And again, this is a really important hearing that we are having today because it affects us all.

Mr. Pitsor, if I could start with my questions with you, if I may, please. In your testimony you state that you support a voluntary cybersecurity evaluation of products used in bulk power systems such as the program described in H.R. 5239 Cyber Sense.

One point you raise is that once products are sold manufactures often don't know where or how these components are used, installed, or operated.

You suggest that asset owners should maintain a system of tracking products. Would you explain in detail why it is important to track these products?

Mr. Pitsor. As we look -- as we look at evaluation of cybersecurity threats of different components and how they're assembled in the manufacturers, once they have sold a product, they're assembled in the field. They're not necessarily aware of who purchased them and how they were assembled.

And so the tracking concept here is to have a database and

that could be shared so would be more familiar with where products have been placed, how they've been assembled, how they've been installed, how they've been commissioned.

So that if patching is necessary due to a cyber-related event or testing for that product, we would then be able to contact the asset user as to what patches should be installed and how they should be installed.

Mr. Latta. Let me follow up, when you're talking about the -- especially with the -- with the database because in Section 2(b)(2) of the Cyber Sense bill establishes a cybersecurity vulnerability reporting process and related database for products tested and identified as cybersecure under this program.

Would this help address the need for a system for tracking those products by having that, as you just mentioned?

Mr. Pitsor. I think a database would be very helpful in terms of addressing that need, yes.

Mr. Latta. Thank you.

Mr. Aaronson, if I could ask you, and I think you mentioned about -- in your testimony about when you were out with co-ops, and I know I just was at two of my co-ops. I represent the largest number of co-ops in the district -- in the state of Ohio.

But if I could ask this question -- as the new technologies are becoming increasingly interconnected within our electric grid, new vulnerabilities are emerging across the system including at the distribution level.

Currently, the physical or cybersecurity of the bulk power system or the interstate is addressed through the Critical Infrastructure Protection Standards issued by NERC.

But the distribution system intrastate is outside the jurisdiction of the mandatory NERC standards and the question is are there implications for this perceived gap in oversight and protection of the cybersecurity of the distribution portion of the nation's electrical grid.

Mr. Aaronson. So a couple of things to respond to there. As I mentioned in my testimony, we operate one big machine, right, with thousands of owners and operators from really large investor-owned electric companies that EEI represents to co-ops and municipal systems of varying sizes. And so as you know, the ESCC incorporates all of those and we work very closely.

I know both APPA and NRECA provided written testimony or written statement for the record. So I would refer to that.

With respect to gaps, and I call them perceived gaps, just because distribution level components are not subject to the federal CIP standards does not mean that there is not security happening at that level.

That said, we do think that anything we can do with respect to components that make up that part of the grid -- the intrastate -- the distribution level, is going to be an important approach to continue to advance security for all of us.

The other thing I would say about distribution security is

we need to prioritize. You know, in security we defend -- you protect diamonds like diamonds and pencils like pencils, and to be sure, there are diamonds at the distribution level that we need to be aware of. There are components that are crown jewels at the distribution level that we need to be securing.

And so approaches like Cyber Sense may allow us to do that and some of the things that Secretary Menezes and Assistant Secretary Hoffman were discussing with respect to really looking closely at those components and drilling down on the most critical, because if you have a hundred priorities you have no priorities -- but really finding those most critical components and beating the heck out of them so that we can understand if there are any vulnerabilities in them, again, will make us all more secure.

Mr. Latta. Well, thank you very much, Mr. Chairman. My time is about to expire and I yield back.

Mr. Walberg. I thank the gentleman.

Now I am privileged to recognize the ranking member, the gentleman from Illinois -- in fact, the district I was privileged to be born in -- I quickly add long before you represented the district, Mr. Rush.

[Laughter.]

Mr. Rush. Mr. Chairman, it's still the best district in the nation.

Mr. Vance, in your written testimony you noted that DOE held

a cybersecurity contest which brought together students competing to address the challenges of protecting infrastructure and firms that might employ the same students after they graduate.

Do you think that on both the public and private sector that we are doing enough to ensure that we have a skilled workforce capable of meeting the challenges we will inevitably face in regards to cybersecurity?

And I will invite any of the members of the panel to weigh in on some of these issues.

Mr. Vance. I think what we've been doing in Indiana is specifically trying to bring together the public and private sides together to analyse what some of the weaknesses are, what we are good at, what we are not good at, and as Mr. Aaronson from EEI spoke about just a second ago, I think we need to prioritize and figure out where those diamonds are and where those pencils are.

It's one thing for me and my colleagues in the private -- I am sorry, the public sector to sit in a room and try to figure out what we need to focus on. We are going to miss a lot of things.

What we need to do is sit down with the private sector and work through a collaborative process to identify where our weaknesses are and how to strengthen those.

So the bills being discussed today, I think, are four steps in the right direction to help strengthen those partnerships.

Mr. Rush. Anybody else want to chime in?

Mr. Tudor. Mr. Rush, thank you for the question.

I agree that public-private partnerships are key to moving these forward and these four pieces of legislation are definitely, you know, great steps towards that.

At the Idaho National Lab, you know, we know that the partnerships are the strongest part of our operation, whether it's with vendors, asset owners, you know, with other government agencies and that's the way that we will be able to develop the structures to keep our cyber resilience in our energy systems.

Mr. Rush. And does anyone have any suggestions on how the Congress could help you to ensure that we have enough skilled workforce other than what's information in these four bills?

Mr. Vance. I will add, real quick, just to give a little bit more perspective on what we are doing in Indiana. Our approach with our cybersecurity council has been to bring together all the potential industries involved in cybersecurity.

So right now, I've got about 250 or so members of that council spanning about 20 different industries with industry subgroups that then things can bubble up through those subgroups into the full committee that -- to address in a cross-sector manner.

So I will give you an example. One of the committees is focused on personal identifiable information because that's something that's not unique to any one specific industry and it really needs to be a topic in and of itself.

But it can't just be its own council or committee. It has to be part of a bigger picture because it ties back to energy,

water, finance -- all these other things.

So what we've been trying to do in Indiana is to build a large council that integrates all these different aspects so it can be addressed in a very -- in a cross-sector manner across different industries.

Mr. Aaronson. Mr. Rush, I would add, you know, I know you're very committed to workforce development in particular with respect to cyber and I think one of the things that you're hearing both from the previous panel and all of us is this is a shared responsibility.

It's a whole of community issue. I referenced in my verbal testimony the cyber mutual assistance program. To us, that is a force multiplier. That is when a company is in -- is being attacked their counterparts come from around the country and around the nation and around North America, frankly, to support them.

And so I think that's great for the electricity sector and we are very proud of that. But to be able to work with the National Guard, to be able to work with other sectors, to be able to prioritize restoration when cyber incidents maybe are impacting more than one sector.

We need to look at this again far more holistically. And then from a workforce perspective, you know, we are very proud of the development that we do within our sector through things like the CEWD. It's the Energy Workforce Development --

Committee for Energy and Workforce Development is a great example of how we can find those gaps that we have in our workforce and work through education, work through public-private partnerships to improve our staffing in our most critical needs.

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

Mr. Walberg. I thank the gentleman.

I now recognize the gentleman from Virginia, Mr. Griffith.

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

Mr. Tudor, I am going to come to you first but I am going to take what's more or less a point of personal privilege and just say that I saw you sitting throughout that first panel and all those questions on that second row there with a couple of young people who are very well behaved. Are they connected with you?

Mr. Tudor. Yes, sir. That's my son, Miles, and my niece, Sydney. They're getting a civics lesson today.

Mr. Griffith. Well, not the most riveting of hearings but one that's very important and they have done a great job and I thought they were -- you could tell they were doing some stuff back there and I thought they were like my kids, playing on an electronic device.

But, apparently, they have a numbers game that they're working on that's all done with their hands and they've been very quiet and very well behaved. So you're -- you and your family are to be commended for having such well-behaved children.

That being said, let's get down to business. You made

reference to the consequence-driven cyber-informed engineering -- CCE methodology.

You say this is more about getting ahead of the problems of vulnerabilities and threats rather than chasing them. Can you describe what role this approach may have in strengthening cybersecurity and critical infrastructure?

Mr. Tudor. Yes. Thank you for that question, sir.

So consequence-driven cyber-informed engineering, or CCE, kind of identifies the problem -- that we are constantly seeing new vulnerabilities, new threats every day. So an organization does a risk assessment on a Monday and by Wednesday when new vulnerabilities are discovered, many of the activities described in that risk assessment may be moot.

But if we go back and look at the key consequences of any organization and we take an electric utility at this, you know, if keeping the lights on is their mission but maybe there's several key components that if they were lost may prevent that mission from being carried out.

You know, looking at the engineering methods of those consequences, looking at the way an adversary might go about attacking those infrastructures, using a threat-based methodology and at INL we do a lot of work considering the threat first and we use that mind set when we look at our different mitigations, and then developing mitigations with the asset owner who is a key component of this.

So if we can engineer out those severe consequences, irregardless of the threat or the current risk or a current -- or a new vulnerability then we believe that that has a chance of maintaining that resiliency over a longer period rather than just addressing new vulnerabilities as they show up.

Mr. Griffith. I appreciate that, and there's a pilot program but it's had very limited deployment. Are you confident this methodology is an effective approach and, if so, what are you trying to examine before deciding whether this program should be expanded?

Mr. Tudor. Yes, thank you again.

We have conducted one pilot. We are on a second, and I think that as we've been briefing this across Congress, the National Security Council, and others, we've been very encouraged that people do believe that this type of methodology will be able to go forward.

So we are working with the DOE and others to develop some ways to do CCES scale. In our next few pilot engagements we'll be bringing more partners along to provide training for them and they can go out and provide training for others. So we hope to be able to scale out this methodology in the next several years.

Mr. Griffith. I appreciate that.

Mr. Engels, you have got a pipeline -- a new pipeline coming near my district, although not through my district, and I asked before about some, for lack of a better term, smart pipe

technology.

I know you're not expecting that question today and so if you could just get me an answer later as to what you all might be doing in regards to letting us know if there's some kind of a break in the line quicker using some smart technology.

Mr. Engels. I will be glad to follow up with you on that.

Mr. Griffith. And likewise, I have a friend who's got a farm where there's going to be a pump station and whatever you all could do to reassure folks that they're being placed in the safest location and likewise if there's any smart technology in there I would appreciate having that information.

Mr. Engels. I understand. We'll make sure we follow up.

Mr. Griffith. Thank you. All right.

Mr. Aaronson, you mentioned in your written testimony that approximately 75 percent of U.S. customers are served by a company that participates in cybersecurity risk information sharing program.

Do you have any insight what's going on with the other 25 percent?

Mr. Aaronson. So CRISP is a wonderful technology and the beauty of it is it was something that was actually developed by National Labs. It was piloted for a few years by a small subset of companies -- did some proof of concept, and that was then.

We'll call it commercialized, although maybe that's not a fair characterization because it is still a public-private

partnership with the Department of Energy, the North American Electrical Reliability Corporation through their information-sharing analysis center -- I am trying to not use acronyms -- and then the companies that deploy it.

What we are looking to do and what the ISAC is planning to do now is to expand the program. So started with five pilots. It has expanded to more than that, to the 75 percent of customers being represented by a company that has deployed CRISP.

The other thing you should note is that information, while it is gleaned from the companies that have deployed the sensors that make up CRISP, the information that is gleaned is actually socialized to the entire electric utility sector.

So while there are sensors on 75 percent of companies, we are going to get a much broader cross-section in the coming years.

Mr. Griffith. I appreciate that. Thank you for the answer.

I thank all of you for being here today, and I yield back.

Mr. Walberg. I thank the gentleman and I recognize the gentleman from California, Mr. McNerney.

Mr. McNerney. I want to thank the chairman and I thank the witnesses. Good testimony and informative.

Mr. Aaronson, in your testimony you pointed out that the EEI members do work to prepare for hazards and cyber or natural events.

What are your members doing to prepare for climate change events? Is that -- is that -- is there a standard or is there some sort of work that needs to be done that's being done?

Mr. Aaronson. So, again, I think we look at this as all hazards, and whether it is an act of war or an act of God, whether it is a natural disaster, whether it's an earthquake, whether it's the wildfires that I know that your district has been impacted by, we are looking at ways we can be more resilient, and a lot of what we do kind of crosses, again, acts of war and acts of God and is more about consequence management.

Why the lights were, you know, turned off -- why there was a power outage becomes a little less relevant and how quickly can we get them restored.

And so a lot of our focus is on that response and recovery and resilience component of preparation for all manner of hazards.

Mr. McNerney. Okay. Thank you.

Mr. Pitsor, I appreciate your comments on the enhancing grid security through public-private partnerships. You mentioned that you wanted to see a Momentary Average Interruption Frequency Index included in the ICE calculation. How would that improve the calculation? How would that improve the results?

Mr. Pitsor. Well, the MAIFI index represents some nearly 50 percent of all the momentary outages that occur in the U.S. and these are momentary outages that are usually five minutes or less.

We think that the overall interrupter calculation, if it's missing those 50 percent of the outages, it's not capturing fully the economic costs that are associated by these smaller momentary

outages.

For instance, electric motors trip off, computers don't have backup power trip off. There are costs associated with that that could be -- should be captured in the overall estimator.

Mr. McNerney. Okay. You mentioned the Cyber Sense Act. How would your members respond to nonvoluntary requirements for -- including cybersecurity in their products?

Mr. Pitsor. We are very supportive of the evaluation testing of electrical equipment. I think the key is going to be what type of equipment we are speaking of -- the scope of the testing, what protocols we are testing against, who's paying for that testing, and the follow-on work that will be done to address vulnerabilities that are found in terms of patching, recommissioning, the continuous process that goes on in addressing cyber --

Mr. McNerney. I mean, it seems that your members would want to have a set of standards they could -- they could link their products.

Mr. Pitsor. Exactly. Working on supply side standards that I mentioned, a new cyber security index standard and then looking at how we test different products and different configurations against different vulnerabilities. We segment those products because some products, as has been recognized, are behind layers of security. So the testing of those maybe are less than those that have outward-facing connection to the internet.

There's different levels of testing that would be required for those products.

Mr. McNerney. Do you have concerns about cuts that are being proposed in the fiscal 2019 budget's impact on cybersecurity or security in general? I guess Mr. Aaronson would be the right person to ask that question of.

Mr. Aaronson. So we appreciate what the Department of Energy has done with respect to CESER and elevating some of these issues. We've worked really closely in particular with the Office of Electricity and their Infrastructure Security Energy Restoration Office, which will ultimately matriculate over the CESER.

This last historic hurricane season and the nor'easters the last several weeks, and with that response from Puerto Rico -- so between that, our partnerships with the labs and our partnerships with the sector coordinating council we have really appreciated the ability to work closely with this administration and the previous administration. This has been a priority for Department of Energy for several years now.

Mr. McNerney. So you don't see any sort of a drawback with the cuts that are being proposed?

Mr. Aaronson. You know, at this point, I think the priorities that we care about most have not been impacted in our day-to-day interactions with the department.

Mr. McNerney. Thank you. I yield back.

Mr. Walberg. I thank the gentleman.

Now I recognize the good doctor and gentleman from Indiana, Mr. Bucshon.

Mr. Bucshon. Thank you, Mr. Chairman.

Mr. Vance, good to have you here from Indiana.

Mr. Vance. Thank you.

Mr. Bucshon. You're welcome. As you know -- this is a question for you -- as you know, electric cooperatives serve more than 1.3 million customers in the state of Indiana, primarily those in rural parts of the state, which is southwest Indiana, the Wabash Valley that I represent.

An additional 300,000 individuals are served by municipal electric utilities. Both cooperative and municipal utilities are generally much smaller than their investor-owned counterparts.

What are some of the specific challenges that you see these smaller utilities face in terms of defending their assets against cybersecurity threats?

Mr. Vance. I think the challenge is that a co-op or a municipal utility face are very similar to what an investor-owned utility face because they have the same issues in that every time that you move toward a networked piece of equipment you're exposing yourself to potential cybersecurity attacks.

So in Indiana we've been very aware of including our co-ops and our municipal utilities in our conversations on energy

security and cybersecurity. They sit on our cybersecurity council established by the governor.

I think one of the important things we are trying to do in Indiana as we continue exercises is to build those relationships so that we know we have those personal connections and when an energy emergency hits we cannot spend hours searching through a binder of 300 pages trying to figure out what to do.

I think to some extent the movie "Ghostbusters" summed it up well when it said, "Who are you going to call?" You have to know who you're going to call in those situations. We can't spend hours trying to figure it out.

So we've been including our munis and co-ops in our conversations.

Mr. Bucshon. Are there financial challenges to making sure that your networks and everything are secure that the state helps with or anything?

Mr. Vance. There's always finding constraints when it comes to infrastructure. But to the best of my knowledge, I have not -- I am not aware of any specific constraints with munis and co-ops. But we can get back to you on an answer to that.

Mr. Bucshon. Okay. One of the bills we are discussing, and somebody mentioned this a little while ago, Enhancing Grid Security Through Public-Private Partnership Act specifically requires the secretary of energy to take different sizes of and regions served by electric utilities into account when

administering cybersecurity programs.

Based on your experience in Indiana, what might this look like?

Mr. Vance. I think that would be something that we'd be very interested to work with DOE on. What that would look like I am not entirely sure, off the top of my head.

Mr. Bucshon. Anybody have any comments on any of this stuff? No?

Good. I yield back, Mr. Chairman.

Mr. Walberg. I thank the gentleman.

Seeing no one else on the panel, I recognize myself for five minutes. Thanks to the panel for being here.

Mr. Aaronson and Mr. Vance, I asked some questions to our DOE panel earlier and I would appreciate hearing your answers to them as well.

I appreciate the secretary's efforts to elevate the agency's leadership on emergency and cybersecurity functions and I believe they are commendable.

But I would like to see DOE leadership continue under future administrations, as I mentioned. Do you think it would be -- would help to codify DOE's assistant secretary functions in the DOE organization chart?

Either one -- Mr. Vance or Mr. Aaronson.

Mr. Vance. From our perspective, I would have to discuss with my other members of NASEO before I could make a statement

one way or the other.

But I would defer to DOE on that.

Mr. Walberg. Okay. Mr. Aaronson.

Mr. Aaronson. I would just simply say I see no problem with that. I think it could be useful, and to Mr. McNerney's question also, I think anything that provides accountability, that elevates something not just within the organization but then visibility as a Senate-confirmed position and across the various verticals within the department that acknowledges these intersector relationships between electric, gas, and other generating capabilities, and then I think anything that can get more resources.

I don't want to be dismissive of your question, Mr. McNerney. I think anything that -- you know, more resources so we can do some of these partnerships more, better, faster, and focus on all of the things that are happening in this -- in -- with respect to security in the sector is going to be valuable. So I think codifying it, elevating it, funding it, supporting it are all good outcomes.

Mr. Walberg. Okay. Let me ask, do you believe that elevating the cybersecurity functions to the Senate-confirmed assistant secretary level is a positive? Is it necessary?

Mr. Aaronson. You know, I will leave that to policy makers on that, sir. I think -- I think it's a positive development though, certainly.

Mr. Walberg. Okay.

Mr. Aaronson, one of the bills we are discussing today is the Enhancing Grid Security Through Public-Private Partnership Act, which directs DOE to provide cybersecurity training and technical assistance for electric utilities that have fewer available resources due to size or region.

The legislation builds upon the existing public-private partnership between DOE, the electrical cooperatives, and public utilities -- power utilities.

Could you explain for us the challenges facing certain electric utilities in improving the cybersecurity of their assets?

Mr. Aaronson. Sure. So, again, I would point everybody to the statement by the American Public Power Association and the National Rural Electric Cooperative Association with whom I serve as secretaries on the sector coordinating council with.

So one of the benefits of the sector coordinating council is that we do all come together with common cause, whether they are large investor-owns, smaller investor-owns, cooperatives, municipals, Canadians, independent power generators, the nuclear sector, gas, and on and on and on.

So we work really well together on these issues, again, of sort of mutual concern with respect to protection of our infrastructure.

With respect to challenges among the smaller entities, there

are workforce challenges. There are the ability to ingest intelligence.

There is the ability to implement some of the good information that is coming out of the government and some of the mitigation measures that are recommended. And so anything that we can do as a community -- again, whole of community so that it is a rising tide that lifts all boats -- ultimately helps all of the infrastructure that we own and operate together.

So we are very supportive of that particular provision for our co-op and municipal brothers and sisters but also for some of other smaller entities that are going to need help implementing the things you all recommend.

Mr. Walberg. So this Section 2 of H.R. 5240, the Enhancing Grid Security Through Public-Private Partnerships Act, does that strengthen and further these existing public-private partnerships?

Mr. Aaronson. I think it does.

Mr. Walberg. Okay.

Thank you. The gentleman from New York is here, my friend, and we recognize you for five minutes for questioning.

Mr. Tonko. Thank you, Mr. Chair, and thank you to our witnesses for being here this afternoon.

Mr. Aaronson, the utility industry has a long tradition and culture of mutual assistance. When a disaster strikes, everyone responds, and I know there are still crews from New York working

in Puerto Rico.

The industry has a good idea of how to deal with supply disruptions and restorations after a natural disaster. But cyber is still uncharted territory. When the industry comes together to think about the future of mutual assistance, does that include how you might respond to a cyber incident?

Mr. Aaronson. Very much so.

So the -- one of the things that we have done as a sector -- and actually I will give a little bit of a time line because in think it's instructive.

So you will recall the end of 2015 we had both GridEx III, which is a biannual exercise that NERC puts on, and then just a month later there was the attack in Ukraine that had impact on their distribution system.

The CEOs of the sector coordinating council got together for a meeting in January of 2016 and asked the question, do we have the surge capacity to deal with either the imagined threats in the GridEx scenario or the real ones that were perceived from the Ukraine scenario.

And the answer was sort of, which is never a good answer for chief executives. And so they told us as the sector coordinating council support staff to go put something together.

We put together something known as cyber mutual assistance, and so from that time just a little over two years ago we scoped what cyber mutual assistance would look like.

We developed a legal structure around it. We developed a play book. We exercised it. We've utilized it, and now 142 companies representing nearly 80 percent of all customers in North America have a company that is a member of the cyber mutual assistance program.

So we will be -- look, it's in its very nascent stages. Traditional mutual assistance has been around for more than 80 years. But it is a platform that we can begin to surge and support each other in the eventuality of a cyberattack.

Mr. Tonko. And in that collaboration, are there any differences that you would cite that they could distinctly -- make a distinction from, you know, the regular emergency planning and response efforts?

Mr. Aaronson. It is in some ways very similar in that the goal is to restore power and one of the things I tell people is the best way to not have cyber vulnerabilities is to not have cyber infrastructure.

So another thing that we are pursuing is to actually be able to operate in a degraded state manually, which is something Ukrainians were able to do and, again, which we have some capacity to do but, you know, are going to develop even more so.

With respect to the differences between traditional and cyber mutual assistance, the first one is the obvious one. You're not going to have bucket trucks of, you know, cyber linemen driving down the highway to the affected area.

But there is the capacity to support each other remotely. There are things that can be done to develop both information sharing in the event of these attacks and the sharing of equipment and the bringing in of noncompromised equipment to support the company that may have had equipment compromised.

Last is with storms you see them coming and they are regional. And so companies from all over North America will descend, and did certainly this last year, on the affected region.

Cyber doesn't know boundaries like that and so that is a consideration for how do you respond -- do I want to send my people into a company that's been impacted when I may be next, and that is something that the cyber mutual assistance program is contemplating and addressing.

Mr. Tonko. Okay. Thank you very much.

And Mr. Vance, a common theme we are hearing today is how partnerships -- those between utilities and between different levels of government -- are critical to ensuring that our electric system is reliable, resilient, and prepared for the worst.

Can you give us a sense of the level of cyber expertise at the state and local levels?

Mr. Vance. We have a number of folks at our Office of Technology who are the co-coordinators of our cybersecurity council who are spending their time on cybersecurity in coordination with our Department of Homeland Security, our Utility Regulatory Commission, and a number of folks across state

government.

So we do have some folks who are focused specifically on the cyber issues. This is a relatively recent thing. I think it started in 2016 but it's something we are trying to get up to speed on as soon as we possibly can.

Mr. Tonko. Thank you. And your testimony mentioned the importance of a robust state energy security program. What kind of services and resources can DOE provide to our given states?

Mr. Vance. I think that's something that can be defined as we explore this more. But the first things off the top of my head are more training and exercise.

A lot of this planning and exercise activities -- for example, the exercise we did in Rhode Island that mapped a cyberattack on top of a natural disaster -- is something that was a very useful exercise, bringing people together and go through these issues and also put a face to who some of these people were at utilities, at DOE, at the states.

So I think more exercise and opportunities to plan regionally are really helpful as well.

Mr. Tonko. Thank you very much.

And seeing that I have no time remaining, I yield back, Mr. Chair.

Mr. Walberg. I thank the gentleman.

Seeing there are no further members wishing to ask questions, I would like to thank all of our witnesses again for being here

today and for the insights you shared with us and considering our questions.

Before we conclude, I would like to ask for unanimous consent to submit the following documents for the record: number one, a statement from the American Public Power Association and the National Rural Electric Cooperative Association; a cybersecurity update letter from the American Public Power Association; a letter to Department of Energy Secretary Perry; a response letter from the Department of Energy Secretary Perry; a statement from Siemens Energy.

[The information follows:]

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

Mr. Walberg. And pursuant to committee rules, I remind members that they have 10 business days to submit additional questions for the record and I ask that witnesses submit their response within 10 business days upon receipt of the questions.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 1:04 p.m., the committee was adjourned.]