RPTR ZAMORA

EDTR ROSEN

KEEPING THE LIGHTS ON: ADDRESSING CYBER THREATS TO THE GRID

FRIDAY, JULY 12, 2019

House of Representatives,

Subcommittee on Energy,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 9:33 a.m., in Room 2123, Rayburn House Office Building, Hon. Bobby L. Rush [chairman of the subcommittee] presiding.

Present: Representatives Rush, Peters, McNerney, Loebsack, Butterfield, Schrader, Kennedy, Veasey, Kuster, Kelly, Barragan, McEachin, O'Halleran, Blunt Rochester, Pallone (ex officio), Upton, Latta, Rodgers, Olson, McKinley, Griffith, Johnson, Bucshon, Flores, Hudson, Walberg, Duncan, and Walden (ex officio).

Staff Present: Jeff Carroll, Staff Director; Jacqueline Cohen, Chief Environment Counsel; Jean Fruci, Energy and Environment Policy Advisor; Waverly Gordon, Deputy Chief Counsel; Tiffany Guarascio, Deputy Staff Director; Omar Guzman-Toro, Policy

Analyst; Rick Kessler, Senior Advisor and Staff Director, Energy and Environment; John Marshall, Policy Coordinator; Elysa Montfort, Press Secretary; Meghan Mullon, Staff Assistant; Lisa Olson, FERC Detailee; Alivia Roberts, Press Assistant; Tim Robinson, Chief Counsel; Andrew Souvall, Director of Communications, Outreach and Member Services; Tuley Wright, Energy and Environment Policy Advisor; Adam Buckalew, Minority Director of Coalitions and Deputy Chief Counsel, Health; Robin Colwell, Minority Chief Counsel, Communications & Technology; Jordan Davis, Minority Senior Advisor; Melissa Froelich, Minority Chief Counsel, CPAC; Peter Kielty, Minority General Counsel; Mary Martin, Minority Chief Counsel, Energy & Environment & Climate Change; Brandon Mooney, Minority Deputy Chief Counsel, Energy; and Brannon Rains, Minority Legislative Clerk.

Mr. Rush. The subcommittee will now come to order. I want to thank all the members and the witnesses for appearing before the subcommittee this morning.

The chair will now yield 5 minutes to my great friend, Mr. McNerney from California, for 5 minutes.

Mr. McNerney. Good morning, Mr. Chairman. I thank you for yielding me the 5 minutes.

And I thank the witnesses for coming this morning. It is an incredibly important issue that we needed to care a lot about and make good policy on.

We are meeting today to discuss the state of cybersecurity in the grid and the continuing threats facing America's energy infrastructure. We continue to see increasing threats to the grid, originating both at home and abroad. I am glad to see the DOE and FERC and others taking steps to address the growing dangers posed by nefarious actors.

Our energy grid serves as the backbone of our economy, touching every aspect of our lives, and a reliable grid is also crucial to our national security and for a clean energy future. For lawmakers to encourage and enable innovative advancements that we can improve the security and reliability of our Nation's electric grid, we must work on a bipartisan basis, and actively engage with industry leaders as we are doing today here.

Fortunately, the modernization and innovation of our energy infrastructure is already underway. What was once a one-way delivery system has evolved into a dynamic network where information and energy flows both ways. Technological advancements are both -- are also borne from the need to secure the energy grids against potential physical and cyber threats.

For example, technology allowing for the rerouting of power and quick response

in the event of attack is being deployed across the grid. The cooperation among Federal, State, and local governments is essential to protecting Americans and our Nation's infrastructure.

Given today's cyber environment it is more important than ever that Congress pursue policies that continue to foster these exciting developments and support our grid infrastructure.

This is an issue that I am very passionate about, and vulnerable components -- any vulnerable component is a threat to our physical and national security, making it imperative that we invest in grid modernization and security.

That is why I am proud to cochair the bipartisan Grid Innovation Caucus with my good friend from across the aisle, Representative Bob Latta from Ohio. Together, we are focused on providing a forum for discussing solutions to the many challenges facing the grid, and to educate Members of Congress and staff about the importance of the electric grid with relation to the economy, energy security, advanced technologies being utilized to enhance grid capabilities.

This work has informed our introduction of two bills on the topic, both of which have already been marked up and advanced by this subcommittee. Their aim is to bolster America's electric infrastructure by encouraging coordination between the Department of Energy and the electric utilities.

My bill, which I introduced along with Mr. Latta, H.R. 359, the Enhancing Grid Security Through Public-Private Partnership Act, would create a program to enhance the physical and cybersecurity of the electric utilities through assessing security vulnerabilities and increasing cybersecurity training and collect data.

It would also require the interrupt cost estimate calculator, which is used to

calculate the return on investment on utility investments to be updated at least every 2 years to ensure accurate calculations.

Mr. Latta's bill, which he introduced along with me, H.R. 360, the critical Cyber Sense Act, makes important headway in protecting our critical grid infrastructure. The Cyber Sense Act would create a program to identify cyber secure products for the bulk power grid through testing and verification program.

The Bulk-Power System supports American industry and provides all the benefits of a reliable electric power to the American people. It is essential that we make this system as secure as possible as cyber attacks do pose a serious threat to the electric grid. Any vulnerable component in our grid is a threat to our security, and this bill will go a long way to strengthening that system. I thank Mr. Latta for his partnership and looking forward to working with him.

I also want to take a moment to mention my support for H.R. 362, the Energy Emergency Leadership Act sponsored by Chairman Rush and Mr. Walberg. This bill would establish new DOE Assistant Secretary position with jurisdiction over all energy, emergency, and security functions related to energy supply, infrastructure, and cybersecurity.

Finally, I want to mention my support for one more bill on this topic, H.R. 370, the Pipeline and LNG Facilities Cybersecurity Preparedness Act, sponsored by Ranking Member Upton and Mr. Loebsack. This bill would require the Secretary of Energy to establish a program relating to the physical security, and cybersecurity for pipelines and liquefied natural gas facilities.

As the bills I have mentioned show, our committee is uniquely positioned to examine the issues before us today as we work to put America on a path to better

securing our electric and utilities system.

Now I yield back to the chairman.

Mr. Rush. I want to thank the gentleman. And on a point of personal privilege, the chair was originally scheduled to be at home in Chicago this morning for a funeral. One of my dear friends, Ms. Dana Russell, trusted friend and colleague and supporter, and due to inclement weather last night, my flight was canceled so I couldn't be in Chicago.

And Mr. McNerney graciously agreed to sit in the chair for me last night, because I wasn't going to be here this morning. But I am here now, and so I am -- want to thank him, Mr. McNerney, personally for agreeing to sit in the chair for me in my absence. But as you can see, I am here, and so thank you.

Mr. McNerney. Well, I appreciate the sentiment, and I also appreciate the confidence that you have shown in me, Mr. Chairman.

Mr. Rush. Thank you very much.

The chair now recognizes Mr. Upton, the ranking member of the subcommittee, for 5 minutes for the purposes of an opening statement.

Mr. Upton. Well, thank you, Mr. Chairman. I am sorry to hear about your friend, and I am grateful that you didn't get on that plane because I drove home through that storm last night, and I don't think that plane would have had lot of --

Mr. Rush. Thank you.

Mr. Upton. Yeah. Yeah. Smart.

Today's hearing continues the subcommittee's ongoing oversight of cybersecurity threats to the electric grid, a priority that all of us have had. And while this is the first hearing specifically on the topic this year, the subcommittee has been raising questions

about persistent and emerging threats to the electrical grid in closed briefings, and in hearings with Federal officials and others over the course of this session, building on the work that we have done over the last couple of Congresses.

It is unquestionable that ensuring the reliable supply of electricity is vital to our Nation's security, economy, our health, and welfare. Electricity enables telecommunications, financial transactions, the transport and delivery of energy and agriculture; it powers the infrastructure that delivers our drinking water; it enables business and industry to make and provide the goods and services of our modern society; it powers our hospitals, our households, and everything else.

But let's face it. The U.S. has the world's most complex electric grid, and while we have a well-developed system of grid operators to ensure that the lights stay on, we are confronting new challenges every day, and adapting to a changing generation mix, new technologies, and consumer preferences.

We are also responding to new threats and working to strengthen the cybersecurity of the Nation's grid. The integration into the system of new digital technologies that are essential for keeping up with our Nation's energy needs constantly add vulnerabilities.

Other vulnerabilities are being added with increasing dependence on pipeline infrastructure by electric generating units. Combine that with a rapid expansion of cyber capabilities by more of America's adversaries in safeguarding transmission infrastructure remains particularly urgent.

Many of the Federal oversight and regulatory structures in place today that ensure that the system can mitigate and respond to cyber can be traced to this committee's legislative work.

In 2005, we authorized FERC to commission the North American Electric Reliability Corporation, NERC, with the authority to establish and enforce reliability standards and to coordinate activities among industry and the Feds to confront cyber threats.

In 2015, this committee wrote provisions, including the FAST Act, to strengthen DOE's energy sector specific authorities and to facilitate sharing of the threat information between private sector asset owners and the Federal Government.

As a Federal agency with a leading expertise on our Nation's electricity grid and the cybersecurity threats against it, it is imperative that we arm DOE with the tools and authorities to protect our electricity system from the transmission lines to the very generating stations and their pipelines.

Most recently, we developed legislation to elevate DOE's functions overseeing cybersecurity and to improve information sharing, emergency planning, and other technical activities in this jurisdiction. That legislative work is continuing, but unfortunately -- or but fortunately, the Department has used its own authorities to implement enhanced leadership over cybersecurity and to improve interagency coordination.

Against that backdrop, today's hearing provides a great opportunity to update the subcommittee on what these agencies are doing to advance cybersecurity practices, protections and response planning.

I am looking forward to hearing from Assistant Secretary Karen Evans, who heads the DOE Office of Cybersecurity, Energy Security, and Emergency Response, or CESER. When she testified in September last year, she had been on the job for just a couple of weeks, though she brought long Federal experience to the table as soon as she sat down.

So I look forward to discussing DOE's current work, how well it is exercising its

coordinating role over the cybersecurity threat, and to learn what challenges she sees going forward and how she plans to address those challenges.

It will also be helpful to hear today from the regulators of the electric grid, Andy Dodge, who heads FERC's Office of Electric Reliability, and of course, from Jim Robb, who heads NERC. Both of these entities serve as the front lines of regulatory oversight of electric grid infrastructure protection. I am particularly interested in learning what measures you are working on to address threats to ensure best practices and to coordinate response to cyber incidents.

The risk of massive blackouts can be hard to think about, but the cybersecurity realities of today require that we face these risks head on, that we be sure that our agencies and appropriate groups have the tools in the toolbox and the information that they need to address the risk and what they are prepared for the consequences of successful attacks.

Thank you, Mr. Chairman, for this hearing. I yield back.

Mr. Rush. The gentleman yields back.

The chair now recognizes the chairman of the full committee, Mr. Pallone, for 5 minutes for the purposes of an opening statement.

The Chairman. Thank you, Chairman Rush.

Today we are here to get a update from Federal agencies about how they are addressing cyber threats to our electricity grid. We know our adversaries are developing new techniques to compromise and attack our grid, so it is vitally important that the Federal Government and the electricity -- or the electric industry remain vigilant in ensuring the grid is secure.

Our committee has been conducting robust oversight on this important topic in a

bipartisan fashion for years. Today's hearing is a public forum to discuss how the Federal Government is addressing cybersecurity challenges, but the committee also continues to receive closed-door briefings on the issue to understand more classified matters.

Our witnesses and their respective agencies all take cybersecurity to the grid very seriously, and I believe Secretary Perry made the right decision in creating the position of Assistant Secretary for Cybersecurity, Energy Security, and Emergency Response to focus specifically on these pressing issues.

Last month, the subcommittee favorably reported out legislation introduced by Chairman Rush and Mr. Walberg that would enshrine in statute this important new division at DOE, and I look forward to bringing this bill and three other bipartisan cybersecurity bills up for a markup at the full committee soon.

We must be both active and vigilant when it comes to cybersecurity, because time is of the essence. In March, we had the first reported malicious cyber event that disrupted grid operations of a western utility. Thankfully, there seemed to be very little effect on the transmission grid and no customers lost power, but we must stay ahead of anyone who is a cyber threat.

And I appreciate the work of FERC and N-E-R-C, or NERC, to continue enhancing critical infrastructure protection standards, like the final rule last October to bolster supply chain risk management. This rule implements new reliability standards that respond to supply chain risks, like malicious software, by requiring responsible entities to develop and implement security controls for industrial control systems, hardware, software, and services.

And these are the types of important forward-looking actions we need to proactively protect our grid against attacks. And while this hearing today is not

specifically about pipeline cybersecurity, I would be remiss not to mention how important that is to our grid system. We have a reliable pipeline system, but we never want to find ourselves in a different situation, so I remain concerned about the lack of resources and expertise at the Transportation Security Administration's pipeline security program.

I look forward to hearing from DOE about possible ways they could help address these safety gaps. As I have said before, if TSA continues to devote scant resources or attention to these matters, we must start looking at other options to keep our pipes secure. So, again, I thank our witnesses for being here today as we discuss this critical security issue.

And with that, Mr. Chairman, unless someone else wants the time, I yield back.

Mr. Rush. The gentleman yields back.

The chair now recognizes the ranking member of the full committee, Mr. Walden, for the purposes of an opening statement.

Mr. Walberg. Well, good morning, Mr. Chairman.

Mr. Rush. Good morning.

Mr. Walberg. I am delighted to have the witnesses here and to have this hearing.

By any measure, the reliable supply of electricity is an essential part of everything that we do. We know that. And as we have learned in previous briefings and hearings in today's highly interconnected and digital world, the threat of cyber attacks, the reliability of electricity is ever present and it is growing.

And one of our responsibilities on the Energy and Commerce Committee is to review and, where necessary, revise laws and policies that concern the reliable delivery of energy. This is part of the committee's black letter jurisdiction, and it is something that we all take very seriously, no matter which party is in the majority.

This morning's oversight hearing continues this important work, and it focuses on the status of efforts to address cybersecurity threats to the electricity grid. We will hear testimony from our witnesses today -- you are key players in keeping the lights on -- Department of Energy, Federal Energy Regulatory Commission, and the North American Electric Reliability Corporation, or NERC.

Each of your organizations has a role in supporting effective information sharing, technical assistance, standard settings, oversight of standards implementation, sound engineering practices, all of that as it relates to the Bulk-Power System. And I look forward to hearing updates from the witnesses, especially on coordination and on sharing among the Federal entities and industries. We know that has always been an issue and it continues to be.

Our past oversights examine some of the work DOE is doing to carry out its broad energy emergency and cybersecurity responsibilities over the energy sector. This includes providing, supporting, and facilitating the technical assistance to the energy sector to help identify vulnerabilities and to mitigate risk.

I have seen some of this work firsthand at our national labs, especially in the northwest, the Pacific Northwest National Laboratory in Washington State, and I went out to Idaho Falls to the Idaho National Laboratory. Terrific people working in those labs, doing amazing work on behalf of the country. They provide the analytical tools, they provide the test beds, and other capabilities that are proving very helpful for all kinds of industries and systems we rely upon.

We learned last year how deployment of new surveillance and information sharing tools, particularly in what is called the cybersecurity risk information sharing program, or CRISP, have proven especially helpful in identifying systemic and systematic

cyber attacks across the energy sector.

So I would be interested to hear today from NERC and DOE how this approach is being expanded more broadly, especially as it relates to supply chain risk and operational technology systems, the switches and supervisory control and data acquisition, or SCADA system, embedded in the grid. We know that as more connected devices and smart grid technologies are added to the grid, the vulnerabilities will continue to grow.

Information sharing is central to strong cyber defenses. This is especially important as our energy systems become more interconnected. Republican leader Fred Upton has noted repeatedly, how, because the Nation's pipeline systems -- and you have heard this from others today -- are such an integral part of the electricity fuel supply system harm to pipelines means potential harm to the supply of electricity.

So we have to think about pipelines as part of our larger energy system rather than just a piece of hardware or a simple mode of transportation. While pipelines fall under separate regulatory regimes, Department of Energy must maintain visibility over pipelines to ensure the delivery of electricity to consumers. They are all interconnected.

That is why this committee has been pushing to codify DOE's emergency response role and strengthen the Department's capabilities to monitor for cyber threats and to provide technical assistance to the industries.

It is also important to enhance coordination of response should attacks succeed at a large scale. Members on this panel have had the benefit of briefings over the past few years to understand emergency response exercises in the electric sector. An update on these exercises will also be useful today, so we look forward to that.

And this testimony this morning will underscore the risk to our critical electrical infrastructure from nation states and other bad actors is increasing. This means the

technical assistance, the information sharing, and deployment of innovative technologies and best practices to get ahead of the threats is ever more urgent.

We must be sure our critical infrastructure protection standards are up to date, and sufficiently flexible to meet the risk, and we must be sure we are providing our Federal agencies the tools needed to serve the industry and the Nation more effectively. We have real responsibility here, and hearings like this will help us do our job better.

So, Mr. Chairman, thank you for having this oversight hearing. And, again, to our witnesses, thank you for your testimony, guidance, and counsel. You will improve our work. And with that, I will I yield back the balance of my time.

Mr. Rush. The gentleman yields back.

The chair would now like to welcome all of our expert witnesses for today's hearing. From my left, the Honorable Karen S. Evans. She is the Assistant Secretary of the Office of Cybersecurity, Energy Security, and Emergency Response, CESER, at the U.S. Department of Energy.

Next to hear is seated Mr. J. Andrew Dodge, Sr. He is the director of the Office of Electric Reliability for the Federal Energy Regulatory Commission, FERC.

And sitting next to Mr. Dodge is Mr. Jim Robb, the president and chief executive officer of the North American Electric Reliability Corporation.

And I want to, again, thank all of the witnesses for being here with us today, and we look forward to your testimony. But before we begin, I have to give you a little tutorial. I would like to explain the lighting system.

In front of you is a series of lights. The light will initially be green at the start of your opening statement. The light will turn yellow when you have 1 minute remaining. Please begin to wrap up your testimony at the yellow light. The light will turn a bright,

bright, bright red when your testimony expires.

And with that said, Assistant Secretary Evans, you are now recognized for 5 minutes.

STATEMENTS OF HON. KAREN S. EVANS, ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE (CESER), U.S. DEPARTMENT OF ENERGY; J. ANDREW (ANDY) DODGE, SR., DIRECTOR, OFFICE OF ELECTRIC RELIABILITY, FEDERAL ENERGY REGULATORY COMMISSION; AND JIM ROBB, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

STATEMENT OF KAREN S. EVANS

Ms. Evans. Thank you, sir. Good morning, Chairman Rush, Ranking Member Upton, and members of the committee. Thank you for the opportunity to discuss the continuing threats facing our national energy infrastructure.

Focusing on cybersecurity, energy security, and resilience of the nation's energy systems is one of the energy secretary's top priorities. By the administration proposing and Congress affirming the Office of Cybersecurity, Energy Security, and Emergency Response, CESER, the Secretary has clearly demonstrated his commitment to achieving the administration's goal of energy security and more broadly, national security.

Our Nation's energy infrastructure has become a primary target for hostile cyber actors, both state-sponsored and the nonstate sponsored. The frequency, scale, and sophistication of cyber threats continue to increase. Cyber incidents have the potential to

disrupt energy services, damage highly specialized equipment, and even threaten human health and safety.

The release of the President's National Cyber Strategy, the NCS, in September 2018 reflects the administration's commitment to protecting America from cyber threats. The Department of Energy plays an active role in supporting the security of our Nation's critical energy infrastructure in implementing the NCS.

The efforts reflect a concerted response to the emergence of energy cybersecurity and resilience as one of the Nation's most important security challenges. Fostering partnerships with public and private sector stakeholders is of the utmost importance to me as the assistant secretary for CESER.

The NCS prioritizes risk reduction activities across seven key areas, which include national security and energy and power. DOE cybersecurity activities for the energy sector align to the secure critical infrastructure section of pillar one, which is protecting the American people, the homeland, and the American way of life under the category to prioritize actions according to identified national risks.

In the energy sector the core of the critical infrastructure partners is represented by the Electricity Subsector Coordinating Council, or the ESCC, the Oil and Natural Gas Sub Sector Coordinating Council, the ONGSCC, and the Energy Government Coordinating Council, the EGCC.

The ESCC and the ONGSCC represent the interest of their respective industries. The EGCC, which is led by DOE and DHS, is where the interagency partners, States, and international partners come together to discuss the important security and resilience issues for the energy sector. This forum ensures that we are working together in a whole-of-government response.

It is critical for us to be proactive and cultivate a secure energy network of producers, distributors, regulators, vendors, and public partners acting together to strengthen our ability to identify, detect, protect, respond, and recover. The Department is focusing cyber support efforts to strength the energy sector cybersecurity preparedness, coordinate cyber incident response and recovery, and accelerate game-changing research development and deployment of resilient energy delivery systems.

DOE also maintains a close relationship with FERC and NERC to ensure that they have the relevant information to execute their missions. DOE also holds regular discussions with the three energy sector information sharing and analysis centers, which include the Downstream Natural Gas ISAC, the Oil and Natural Gas ISAC, and the Electricity ISAC, to share emerging and potential threats, and to disseminate information.

Establishing CESER is the result of the administration's commitment to prioritize the energy security and national security. CESER is working on many fronts collaborating with industry, State and local governments, to protect our Nation's critical energy infrastructure from all hazards, including this growing cyber threat.

Our long-term approach will strengthen our Nation's national security and positively impact our economy. I appreciate the opportunity to appear before this committee to discuss cybersecurity in the energy sector, and I applaud your leadership. I look forward to working with you and your respective staffs to continue to address cyber and physical security challenges.

[The prepared statement of Ms. Evans follows:]

******** INSERT 1-1 ********

Mr. Rush. I want to thank you, Madam Secretary.

And now I want to recognize Mr. Robb for -- Mr. Dodge, I am sorry, for 5 minutes for the purposes of an opening statement.

STATEMENT OF J. ANDREW DODGE

Mr. Dodge. Thank you very much. Good morning, Chairman Rush, Ranking Member Upton, and members of the subcommittee. Thank you for the opportunity to testify today. My name is Andy Dodge, and I am the director of Electric Reliability at FERC, or the Federal Regulatory Energy Commission. During my testimony I will often refer to that as the Commission.

I am here today as Commission staff witness, and my remarks do not necessarily represent the views of the Commission or any individual commissioner. Today, I will provide a brief overview of the Commission's authorities and activities to help protect and improve the cybersecurity of the Nation's Bulk-Power System.

Our work includes mandatory reliability standards, audits of those standards, identification and sharing of best practices. We work very closely with the North American Electric Reliability Council, or NERC, its regional entities, other Federal and State agencies, and responsible entities to carry out this very important work.

As a result of the Energy Policy Act 2005 and Section 215 of the Federal Power Act, NERC is responsible for developing, and proposing, new or modified reliability standards to the Commission. The Commission oversees NERC's development and enforcement of critical infrastructure protection9 standards, or CIP standards.

The original set of eight mandatory CIP standards were the so-called version one standards. They were actually developed in 2006 and became totally enforceable in 2010. The CIP standards are continuously reviewed and updated to address new cybersecurity threats and challenges, as well as technological changes. We are currently in version five of the overall standards. There are currently eleven active cybersecurity standards and one active physical security standard. In all, there are over 200 distinct requirements.

The CIP standards are a portfolio of requirements that constitute a defense in-depth approach to cybersecurity based on an assessment of risk. Importantly, the CIP reliability standards are objective-based and responsible entities are free to choose compliance approaches best tailored to their individual systems.

The foundational standard is CIP-002. This standard requires each utility to perform a risk assessment of its assets and then to categorize those assets in the low, medium, and high impact to the electric grid. The other CIP standards then build upon the CIP-002 standard, and they require utility companies to develop and implement cybersecurity plans, train personnel adequately, establish physical and electronic access parameters, and then, also, test and apply patches in a timely manner, identify and report cybersecurity incidents, and also, develop and implement recovery plans amongst other things.

Recently, the Commission further enhanced the CIP reliability standards to address supply chain risk, and also incident reporting. Although NERC and its regional entities are primary enforcement authorities for the CIP standards, since 2016, the Commission has been auditing sample utilities each year with respect to their compliance to the version five of the CIP standards.

As a result of these audits, the Commission has issued two reports that described the lessons learned from the audits as well as best practices. By publishing these lessons learned reports, we hope to help other utility companies improve their compliance with the CIP reliability standards as well as their overall cybersecurity.

In addition to the mandatory reliability standards, the Commission has adopted voluntary initiatives overseen by our Office of Energy Infrastructure Security, or OEIS. OEIS engages in partners with industry, States, and other Federal agencies to develop and promote best practices for critical infrastructure security.

These initiatives include voluntary architecture assessments of interested entities, classified briefings for State and industry officials, and joint security programs, other Federal Government agencies and industry.

In conclusion, protecting the electric system from cyber and physical threats is critically important to securing our Nation's critical infrastructure. The Commission is taking both a standards or mandatory approach as well as a collaborative voluntary approach to ensuring a reliable and secure operation of the grid.

I thank you for the opportunity to testify today and participate in this hearing, and I very much look forward to answering your questions. Thank you.

[The prepared statement of Mr. Dodge follows:]

******** INSERT 1-2 ********

Mr. Rush. I want to thank the gentleman.

The chair now recognizes Mr. Robb for 5 minutes.

STATEMENT OF JAMES B. ROBB

Mr. Robb. Thank you, Chairman Rush, Ranking Member Upton, and members of the subcommittee. I appreciate the opportunity to be with you today. This is my first appearance in front of the committee as NERC CEO since taking the job last year.

You have all noted in your opening comments how foundational electricity is to modern society. And all of us here on the panel, NERC, FERC, the Department of Energy, we all take our job of strengthening the reliability and security of the fabric of the industry very seriously.

We know the citizens of the United States and our neighbors in Canada and Mexico depend on a reliable supply of electricity for all of their daily life needs. To date, there has been no successful cyber attack that has resulted in a loss of load in the United States. While we are very proud of that statistic, I can assure you that we will never rest in our laurels, as the threats are real and the potential consequences as noted are significant.

As a result the electricity sector has taken the cybersecurity threat extremely seriously, and has put in place a robust system to protect our critical infrastructure. We find that boards and executive leadership play strong support, focus, and set cybersecurity as one of their top corporate priorities.

Unlike our day in and day out job to reduce risks to reliability, cyber risks originate

from determined adversaries who use multiple persistent techniques to attack our grid.

The electricity sector employs a multi-pronged approach to support security of the Bulk Power System. The approach includes mandatory and enforceable reliability standards and security standards, information sharing and partnerships with our sector-specific agency, the Department of Energy, as well as other government entities, such as DHS and DOD, to confront rapidly developing threats, and drilling education and engagement with industry. Together, we believe they form a solid foundation of best practices and strategies to effectively confront this ever-evolving threat.

With respect to standards, our critical infrastructure protection standards provide a common foundation for security. Our standards are developed using subject matter expertise from industry then reviewed and approved by NERC's independent board of trustees, and, ultimately, by the FERC.

The CIP standards, as Andy noted, require companies to establish plans, protocols, and controls to protect their critical systems against cyber attack, ensure personnel are adequately trained on cyber hygiene, report security instances in a timely manner, and effectively recover from events.

Our standards evolve with increased understanding of threats. Recent updates to the CIP standards address supply chain risks and improve cyber incident reporting. And we expect later this year to address cloud computing and EMP.

Compliance with standards is routinely audited, and noncompliance is subject to financial penalties, at times quite significant, and require in many cases CEO execution and board-level reporting.

But standards are just one important element of a comprehensive strategy. Because the security threat evolves rapidly, in addition to the defense provided by the

standards, industry and government must maintain constant situational awareness, real-time communication, and prompt emergency response capabilities. And that is where robust information sharing comes in, and that is a service that we provide through the electricity sector, information sharing and analysis center, or the E-ISAC.

Operated by NERC and working in close collaboration with the Department of Energy and the Electricity Subsector Coordinating Council, the E-ISAC is the central hub for sharing of security information within the electricity sector. The E-ISAC communicates with over 1,000 electricity industry organizations via secure portal with critical security information that is provided by both industry and government.

Through the E-ISAC, we manage a terrific information sharing program called CRISP, the Cybersecurity Risk Information Sharing Program. CRISP uses innovative technology developed by the Department of Energy and the national labs to monitor cyber activity on company systems, and we have developed over the last several years the capability to rapidly declassify insights from CRISP within 24 hours to communicate insights out to industry.

CRISP companies currently cover about 75 percent of U.S. customers, and we are working to further expand the program. Information by CRISP is shared beyond CRISP members so that all 1,000 E-ISAC members can benefit.

We also conduct a biannual continent-wide security drill we call GridEx. GridEx is the largest geographically distributed security exercise for the electricity sector. Conducted every other year in partnership with the ESCC and our government partners, it simulates a widespread coordinated cyber and physical attack designed to overwhelm even the most prepared organizations and exercise their ability to respond and to recover.

And, finally, we invest significantly in education and outreach. We conduct periodic webinars, critical broadcast calls, and recently established an all-points bulletin to rapidly communicate key insights and threats to industry. For the most serious threats we can also use a NERC alert, which provides concise, actionable security information and mitigation strategies to industry, and, in many cases, require industry to report back to us on successful threat mitigation.

In addition, we sponsor the premiere annual grid security conference in partnership with our regional entities called GridSecCon, and it has proven to be a terrific training and outreach engagement forum for NERC, the E-ISAC, our government partners, key industry security -- industry security officials, and key vendors to engage and learn from each other.

Again, I thank the committee for inviting me here today. I look forward to your questions.

[The prepared statement of Mr. Robb follows:]

******** INSERT 1-3 ********

Mr. Rush. The chair thanks the witness. And with that, we are now concluding the opening statements from the witnesses, and we will now proceed to members' questioning. Each member will have 5 minutes to ask questions of our witnesses, and I will start by recognizing myself for 5 minutes.

Assistant Secretary Evans, it is certainly great to see you this morning before our committee once again. And as you know, I have sponsored, along with Mr. Walberg, H.R. 362, which will essentially codify your position within DOE as a new Assistant Secretary position with jurisdiction over all energy emergency and security functions relating to energy supply infrastructure and cybersecurity.

So we look forward to passing -- marking that bill up and passing it out of the House, and we hope the President will sign it subsequent to it passing in the Senate. So we want to be invited to your celebration when you are sworn in as the codified Assistant Secretary, all right.

But I have a question for you now. Currently there appears to be some overlap, or even some tension among some of the Federal agencies as it regards to who is responsible for cybersecurity when it comes to protecting the energy sector. What makes DOE uniquely positioned to take on a leading role when it comes to technical expertise, knowledge, experience, and resources in protecting the energy-specific sectors? Why is DOE uniquely positioned to address all those issues?

Ms. Evans. Well, first, thank you, sir. And when it is signed, we will invite you down for the celebration, everyone on the committee, because we applaud your leadership and your forward leaning into this important issue.

Where DOE is uniquely positioned for this is the partnership that DOE has as the

sector-specific agency out through the entire sector as well as State and local government. But what is even more unique about the Department of Energy is the national lab structure and leveraging the capabilities that the national lab has.

So when you hear maybe that there is some tension, I don't know that there is actually the tension. It is the specific expertise of the energy sector, and that is why the administration has us as the sector-specific agency under the PDDs, and as well as with the National Cyber Strategy as it goes forward.

There is clarity that we continue to work through as to the incident response and how that should work, but I think there is no disagreement in the executive branch that this is an important sector, and that the public/private partnership is critical and that leveraging the national labs' capabilities and our understanding in the energy sector does make us that lead, and why we are the sector-specific agency for the energy sector.

Mr. Rush. Thank you very much. I want to move on. Today, we have not experienced any large-scale cyber attacks on our energy grid. That said, we know that Russia and China, and even Iran are wrapping up their capabilities to potentially attack our energy grid and cause disruptions to our economy.

And I know that DOE takes these potential threats very, very seriously. But are there any areas where Congress should provide more assistance either in the form of additional authority, resources, or anything else that you might think of?

And I would also like to hear from Director Dodge and Mr. Robb on this issue, on whether there is anything more that this Congress can do to help you all protect the grid from foreign attacks? Beginning with you, Secretary Evans.

Ms. Evans. I appreciate the opportunity to answer that question. As I outlined in my testimony, it is clear from the worldwide threat assessment what the DNI has said

about our adversaries' capabilities and what they can do in the energy sector. When we are looking at it from a national security perspective and what the Department is doing, we are really -- I think, the key area really is the partnership and then the information sharing.

And so, as we are implementing the national strategy, we are really looking to clarify roles and responsibilities to specifically answer the question that you have posed: Do we need more legislative authority? Do we need -- as a government, what is that administrative package that needs to come up here so that we can have that information sharing in a way that will facilitate and ease some of the issues that industry may feel that they have going forward?

One area that we are also working out that we are looking at is under the FAST Act, you have given the Secretary the authority, once the President designates a grid emergency, what exactly is involved in that, and how we would then move private industry resources to deal with the national emergency. At that point, industry has also expressed and is working with us how some additional liability protections may be needed.

Mr. Rush. My time is expiring, so I won't be able to get answers on that question. Will you please respond in writing to that question?

The chair now recognizes the ranking member, Mr. Upton, for 5 minutes.

Mr. Upton. Well, thank you again for your testimony. I have a couple of questions, and I am going to try to get through them all. I know that we have had exercises on grid security that have been, I think, very helpful. Can you tell us what are some of the things you have learned from that, number one, and also, whether we have had exercises actually on pipelines in terms of cyber attacks on pipelines in terms of an

exercise?

Ms. Evans. As it specifically relates to pipelines, we have done a joint exercise with FERC in a classified setting to really exercise out that interdependency and to see what weaknesses we need to shore up. I would -- there are lessons learned. There are things that we are applying and taking forward in the whole-of-government approach. And I would yield over to FERC if they would like to speak more about that exercise that has happened.

Mr. Dodge. Thank you. The only thing I would like to add about the exercise, it was actually a DOE-led classified security briefing and then it was actually a joint tabletop drill between DOE and FERC, and involved electric industry officials, natural gas industry officials. It also included all the RTOs and ISOs, and it was a rather extensive event. There were lessons learned, as Ms. Evans indicated. It was a classified briefing, and the items from those we are actively following up on.

Mr. Upton. And do you plan on doing any of that this year yet, calendar 2020, 2019 or 2020? Is there another one that is -- a date that is set or not?

Mr. Robb. So let me hop in here. We will be conducting our fifth GridEx exercise this November, and it will be a multisector exercise, highly focused on the electric system, but will also involve communications and fuel suppliers such as natural gas.

You asked about kind of the -- and that exercise, again, is a continent-wide overwhelming attack, and it is really designed to break everybody's system, really to kind of push them to the limit so they understand where their vulnerabilities are in terms of response and recovery.

One of the things we are doing this year in our executive tabletop is to take a very strong focus on a narrow region of the country and really start to focus in on the

operational coordination that would be required between gas pipelines, the communications sector, the utilities sector, and probably even the finance sector in what would be involved in actually restoring the system after such a catastrophic event.

Mr. Upton. And a follow-up question, was TSA involved at all with the exercises?

Mr. Robb. They have been invited to participate this year, and I believe they will be.

Mr. Upton. Have they testified -- or have they participated in the past or not?

Ms. Evans. TSA participates in all the activities that we do from a government perspective. And so, we did last October --

Mr. Upton. They actually had a person there or they actually --

Ms. Evans. Yes, sir. Yes, sir. They had -- they have a representative there. Two weeks ago, also, we just had the Oil and Natural Gas Subsector Coordinating Council meeting out in Oklahoma City. TSA actively participates. We work directly with the industry to actually go through the initiative and the update that we have jointly announced with the oil and natural gas that happened last October.

So TSA, Transportation, DOE, Department of Homeland Security, we are all there leveraging our resources to look at the pipeline security and how to make it more robust.

Mr. Upton. I am looking at a statement -- and I am sorry I didn't print this out. I just saw it just a few minutes ago. It was reported, I think, in Politico this morning that TSA Administrator David Pekoske is talking about they want to be more involved but they realize that they are, in essence, short-staffed, and the likelihood of operating under a continuing resolution, which means that they won't be able to expand anything beyond what they had in fiscal year 2019.

And as we learned a few weeks ago, they only have, I think, four people out of the

50,000 that work on pipelines. So I just question the substantive role that they might have knowing that we have entrusted you all to work together with the enactment of the FAST Act, and really appreciate the work that you do, and I look forward to supporting the legislation to make you someday a portrait-hanging deal as an Assistant Secretary.

So with that, Mr. Chairman, I yield back.

Mr. Rush. The gentleman yields back.

The chair now recognizes Mr. Peters for 5 minutes.

Mr. Peters. Thank you, Mr. Chairman.

Thanks to the witnesses for being here.

Ms. Evans -- well, first of all, I appreciate we are in a nonclassified situation, so you will obviously tell me if you can't answer my questions. But do you know how many cyber attacks the electric grid sustains on a regular day, average day?

Ms. Evans. So DOE continuously monitors across multiple things, so it depends on how we talk about a cyber attack. And so, we are in constant communications with the ISACs, and we constantly monitor what is happening in the state of the sector as a whole. So beyond that, I am happy to come back in a more appropriate setting to give you more details, if you would like.

Mr. Peters. Well, you didn't tell me a number. Do you know the number yourself?

Ms. Evans. That is why I said it depends on how you --

Mr. Peters. How you define the attack?

Ms. Evans. Yes, and how you want to quantify that.

Mr. Peters. Are you able to determine how much of that activity is coming from state actors?

Ms. Evans. So, again, I would be happy to talk about that more, but, yeah, the way that we are designing the system --

Mr. Peters. I am not asking you to tell me if it is coming from -- are you able -- do you know whether it is coming from state actors, or is that something you don't want to answer here?

Ms. Evans. I would like to answer that in a more appropriate setting.

Mr. Peters. Let me move on then to something else, maybe to Mr. Robb, to follow up with a question that the chairman asked of Ms. Evans about what needs to be done now from Congress.

It is my observation that we rely heavily on the utilities, private companies to deal with this. And when they came to speak to us last Congress, they suggested that the thing that they needed most to modernize the grid, not just related to security, but to modernize it was research support from Congress that they wanted to be sort of left to their own to be able to innovate, which I think is generally appropriate.

How comfortable do you feel that individual utilities are able to handle these attacks, and is there anything that you think -- to follow on with Mr. Rush's question -- that Congress should be doing to back that up in terms of security?

Mr. Robb. I am not sure I caught the entire question with the door closing, but --

Mr. Peters. Okay.

Mr. Robb. The point I would make in response to Chairman Rush's question is that the biggest issue for us is that for NERC, we are sort of -- threat actors or so forth is of less interest to us than what is of interest are the attack vectors and so forth.

The most important thing from our perspective would be for government to be able to, more rapidly, declassify information to get it into actionable insights that we can

get out to industry. Industry doesn't need to know the origin. We don't need to know the sources.

Mr. Peters. Right.

Mr. Robb. We just need to know the whats. And I think unfortunately right now, the whats and the whos are intricately tied up and so that kind of clogs the machinery up.

That would be the most important thing that I would see government being able to do that would facilitate better information sharing and better awareness at an industry, would be rapid declassification and/or broader availability of security clearances for folks to participate in those conversations.

Mr. Peters. So real-time ability to share information on attack kind of thing?

Mr. Robb. Absolutely. Absolutely.

Mr. Peters. Right. What should be the responsibility, the legal liability for utilities fending off these attacks? Suppose something gets through because of the weakness of a particular utility. What incentives do we have to make sure that they are carrying their weight?

Mr. Robb. Well, I am probably not the best expert to talk about legal liability. What I would say though in response to the question, is that every CEO I know of, and this goes from the largest IOUs to the smallest public powers, take this threat enormously seriously. So they -- right now I think they all do everything that makes sense for them in their situation to protect against these attacks.

Mr. Peters. It is just my observation that unless -- I appreciate that. I think that is probably something that every CEO wants to avoid. But unless there is a bottom-line impact, sometimes it doesn't filter through the culture of the entire company.

And I think -- I like the way that we rely on private innovators to deal with these

problems. I think often they are better situated than the government, but on the other hand, we have to provide those incentives through the private industry to make sure that they do emphasize this as a business matter. And I guess my time is expired. We will have to continue that conversation later. But thank you again for being here.

Mr. Rush. The chair thanks the gentleman.

The chair now recognizes the ranking member of the full committee, Mr. Walden, for 5 minutes.

Mr. Walberg. Thank you, Mr. Chairman. As you can see, Mr. Chairman, it is dangerous protecting the grid. I am just saying. We all have to do our part.

Mr. Robb, in addition to reports of Russian and Chinese cyber activities, you referenced news reports have indicated in recent weeks that Iran may threaten retaliation. And that could include cyber attacks on critical infrastructure. From your perspective, can you briefly walk through how the owners of the bulk power -system prepare for when they see something like this in the news. Are they ready for it?

Mr. Robb. First of all, I believe that the utilities are on kind of constant alert, because they know that they are a great attack target for foreign adversaries, and so, I think the security establishment within the utilities sector is topnotch, and I think always on alert.

In the case of, you know, the situation surrounding Iran, as soon as we were made aware of the situation, we had an all-points bulletin that we put together in concert with DOE with an appropriate level of declassification of insight that we had out within 3 hours.

Mr. Walberg. Right. Now, in recent months the U.S. and its allies have been addressing security concerns about Chinese telecommunications technologies, such as

Huawei. This raises questions about the use of similar equipment in the Bulk Power System.

How are you all -- Mr. Robb and Ms. Evans, if you could both could address this, how are you all addressing supply chain risks from this technology in the Bulk Power Supply system? Ms. Evans?

Ms. Evans. As you know, the administration has released several guidance and executive orders associated with supply chain risk management. The Department of Energy, the CESER program in particular, already had a program underway which was dealing with it, which is our CTRICS program, which is cyber testing for resilience of industrial control systems, but it is really looking at the technology associated with what is in the energy grid. That really is looking at that, what is the supply chain risk? How are you doing that?

We also have purchased a tool which we intend to deploy out to the sector as a whole so that they can then start looking at their own suppliers. And then on top of that, the last piece is, is that the Department has announced an advanced manufacturing initiative, which is looking at things in the long range, for all the innovative technologies, all the different things that are happening so that we can make sure that we are looking at that upfront as we are then manufacturing these technologies.

Mr. Walberg. So will that give purchasers of the technology in the systems, will that give them -- can you give them an assurance that what they are buying is certified safe --

Ms. Evans. It is --

Mr. Walberg. -- as well as saying that equipment over there may not be?

Ms. Evans. The idea of our programs to be able to go forward, which actually

merit the same type of approach that you have taken in the legislation, is a voluntary participation. So leveraging the capabilities of the labs and looking at the test beds --

Mr. Peters. Right.

Ms. Evans. -- it is publishing and then us working in jointly with like the National Institute of Standards to do the widest distribution of that information so that you could then become an informed consumer. So what you will then see is industry partners who are actively participating. For example, NIST has a very active cyber center of excellence that the energy sector and the industry partners are actively participating in.

Mr. Walberg. Yeah. So what I want to know is, as a simple consumer here, I realize that is not who is buying this equipment in the power grid, but will there be like a stamp of approval URL, you know, approval that this equipment meets the standards, you can rest assured it is -- it has no backdoors, no chips that are programmed?

Ms. Evans. That is what we hope to be able to identify jointly through the Advanced Manufacturing Institute.

Mr. Walberg. All right. All right.

Ms. Evans. So do we have an outcome in mind? Not necessarily, but it will evolve through the Advanced Manufacturing Institute.

Mr. Walberg. Because I know we have some of this equipment in different telecommunication systems today.

Ms. Evans. Absolutely.

Mr. Walberg. And it gets very expensive to take it out. And you don't want, you know, buy the next piece of equipment that -- to replace it and then somebody says, Oh, by the way, that is not good either, and so we want to avoid that. Mr. Robb, I have only got 30 seconds, but please, take it.

Mr. Robb. Sure. So on this last point, we think a supplier certification program is a very smart thing to do. The work that DOE is doing in this area is terrific. There is also some voluntary industry groups coming together to try to create a similar program.

To your initial question around Huawei, ZTE, and the list of suspect companies, we are actually going to be issuing -- well, first of all, we issued an all-points bulletin back in March in response to the Defense Authorization Act prohibitions around those suppliers, alerted industry to that fact. We gave them some time to get their head around where some of those technologies might be deployed in their systems.

Next week, we will be issuing what we call a level-two NERC alert, which will require industry to inventory all the instances that they still have of those devices, communicate back to us their mitigation strategies around them, and we will have that information by the end of the summer.

Mr. Walberg. Thank you, Mr. Chairman. Thank you.

RPTR ALLDRIDGE

EDTR ZAMORA

[10:33 a.m.]

Mr. Rush. The gentleman yields back.

The chair now recognizes Mr. McNerney for 5 minutes.

Mr. McNerney. Mr. McNerney from California.

Mr. Rush. Mr. McNerney from the great State of -- great nation of California.

Mr. McNerney. Thank you, Mr. Chairman. Again, I thank the witnesses.

Mr. Robb, you testified that, as of yet, there have been no successful cyber attacks on our utility system. And that is a great achievement of your office, so I appreciate that.

Ms. Evans, are you aware of any foreign governments that are embedding cyber weapons into our utility grid today to be used in possible future attacks? If you are free to answer that question.

Ms. Evans. I would reference back to the unclassified version of the worldwide threat assessment. I think that the DNI has been very specific about what our adversaries' capabilities are. I specifically quoted in my testimony, and I also have it memorized, it is at the bottom of page 5 and the top of page 6. And so he was very clear about what the capabilities and what our adversaries can do.

Mr. McNerney. Thank you.

Mr. Robb, concerning information sharing, is the security clearance of utility officials an obstacle to effective data sharing of cybersecurity information?

Mr. Robb. I would say yes. Just the sheer number of individuals who are waiting for a clearance that don't yet have them is problematic.

Mr. McNerney. How can we remedy that problem?

Mr. Robb. I don't have the answer to that question, but it is a problem that needs to be resolved.

Mr. McNerney. Okay. Let's collaborate on that a little bit then.

Assistant Secretary Evans, you note in your testimony that one area of truly foundational problem is the cybersecurity workforce development. What is CESER and the DOE doing to train workers against these kinds of threats?

Ms. Evans. So I appreciate the opportunity to highlight the work that we are doing there. We have the cyber strike training. And the executive order that the administration has released recognizes the fact that we have to deal with cybersecurity workforce issues in general, but very specific about the energy sector.

So we are looking and leading the effort in conjunction with Department of Homeland Security to see what those gaps are and how to train and make that more robust. And then the other area that we are really trying to innovate and lean forward on is the use of competitions to be able to use that applied learning. The labs are strategically placed in this area with all the different types of test beds that they have so that we can use those competitions for a learning experience and then feed that result back into the training that we need to do for the sector as a whole.

Mr. McNerney. I have met some of those folks at the national labs. It is impressive what they are doing. And the young people are impressive that are doing the work as well.

Ms. Evans. Yes, sir.

Mr. McNerney. Again, Assistant Secretary Evans, can you describe some of the unique threats facing small utilities today with regard to cyber attacks?

Ms. Evans. I would say that one of the biggest things that we need to do, which you hit on a little bit, is making sure that dissemination of information and the sharing of that information hits at all levels, and that we are working with State and local governments and the associations to make sure that they have the tools that they need and that they have the awareness and the education that all of them need to have so that you can properly prepare and make sure that you are assessing the risk that is happening in your area.

We are working with those State and local governments with the energy coordinators in the governors' offices and in the States to also then drive down this information. And then also working across with other parts of the government that interact with State and local governments as well to make sure that these tools, as well as with the ISACs, have the widest proliferation.

Mr. McNerney. Good answer.

Mr. Dodge, can you describe some of the work that the OEIS is doing to assist small utilities in addressing their vulnerabilities?

Mr. Dodge. Sure. Through FERC, through the OEIS office, they actually work with DOE to actually constantly stay aware of all the threats that are taking place. They also coordinate with the ISAC to find out the threats are taking place as well.

Through DOE, they actually then conduct classified briefings with the smaller utilities, and they are actively going out and identifying and sharing best practices with the smaller utilities. In addition to that, they are actually volunteering -- on a voluntary basis conducting architecture assessments with any of the entities that are interested in that service.

Mr. McNerney. So it sounds like the availability of classification -- security

classifications is an issue then?

Mr. Dodge. I am sorry?

Mr. McNerney. The availability of security classifications for these small utilities could be a problem?

Mr. Dodge. We work to try to overcome that as much as we possibly can. And part of what we would do is we work with DOE is actually get one day read-ins for some of the personnel from the utility companies to alert them of threats.

Mr. McNerney. All right. Mr. Chairman, I yield back.

Mr. Rush. The gentleman from the great State of California yields back.

And the chair now recognizes the gentleman from the only State in the Union that eclipses California as a great State, Mr. Latta from Ohio, for 5 minutes.

Mr. Latta. Well, thank you, Mr. Chairman. And thanks for conducting today's hearing. Very informative. And I want to thank our witnesses for being with us today. It is a very, very important topic that we all worry about constantly on this committee.

I just want to follow up a little bit from my friend and colleague and co-chair of the Grid Innovation Caucus, Mr. McNerney, talked about a little bit earlier that we had introduced legislation earlier this year on H.R. 359, which, one, being the Enhancing Grid Security, and H.R. 360, the Cyber Sense Act. And on the Cyber Sense, just, again, to go through that, because I know that my friend from Oregon was talking a little bit about it. We had been looking at what has been happening, a lot of different things that are happening from around the world with -- we have to be very careful about what is being put into our systems and what kind of devices.

But the 360 is the Cyber Sense Act. And, again, that program would identify and promote cyber secure products for use in the bulk power system and also would establish

that testing. I know he brought about, you know, that seal of approval. But we want to make sure that there is that testing of these products that would be going on and a reporting of the cybersecurity vulnerability. And also, the Secretary at DOE would be required to keep related database for those products to assist electric utilities in that evaluation of these products.

And, you know, both these bills have now been reported favorably out of our subcommittee. Hopefully, we will see those be signed into law soon.

But if I could ask Assistant Secretary Evans, do you think that our legislation we have been working on, not only the Grid Security, but also the Cyber Sense, is going to be helpful in making sure that you can do your job?

Ms. Evans. I appreciate the leadership that you -- that the committee is showing in this area. I do believe that the intent of what you have going forward about having vulnerability disclosures and the idea of constantly -- or having the ability to verify and validate products as they go out and ensuring that the supply chain risk is minimized is important regardless of whether the legislation gets passed or not. And so our office is working and leveraging that capability and using the national labs, and we are moving forward.

When the legislation -- I am assuming you will be successful. When the legislation is passed, it will enhance that and allow for us to move in a more robust manner.

Mr. Latta. Well, thank you very much.

You know, in the aftermath of the 2015 Ukraine cyber attack, the investigation found that the perpetrators didn't rely on any exploits or software vulnerabilities to disrupt the grid. Rather, they gained access to the system over time learning how to maneuver it and use it against itself. In short, patching vulnerabilities wouldn't have

prevented the attack, but patching continues to represent the majority of our cybersecurity efforts.

And to the panel, what steps can be taken to improve the monitoring of the system networks to prevent potential attackers from learning how to use a system against itself? And, Assistant Secretary, if you'd like to start, we would just ask everyone to answer that question.

Ms. Evans. So I would like to change the dynamic, and that is what we are attempting to do through our research and development in the CEDS program that we have, because a lot of what we are looking at is after the fact, so patching and maintaining systems.

A lot of the things that we are looking at in investing through our portfolio is being able to detect and protect, which is changing the dynamic in a way of using technology so that you cannot necessarily do it after the fact but prevent it up front. So looking at more active dynamic types of things, such as software-defined networks, looking at quantum key distribution. How can you use those types of technologies that are evolving right now to ensure the validity of the data or look at the interactions of the transactions that are happening between the operational technology as well as the information technology systems.

We are investing pretty heavily in that, leveraging what is happening in the labs, and we currently have a lab call right now that is out that is looking for some ways of how we can accelerate that deployment.

Mr. Latta. Thank you.

Mr. Dodge and Mr. Robb, we have got about 35 seconds.

Mr. Dodge. Sure. So FERC just recently changed the cybersecurity reporting

standard requirements. And previously, entities were only required if they had an event related to a cybersecurity that impacted reliability of bulk power system. Now they will have to report events where -- or possible intrusions or attempts to actually compromise the cyber assets that impact the cyber assets as well as a bulk power system. And that information sharing associated with that will be a huge benefit.

I defer to Jim.

Mr. Latta. Mr. Robb.

Mr. Robb. I will be very quick. I think I would underscore Secretary Evans' discussion. I think from our perspective, one of the most valuable capabilities to advance would be the ability to monitor what is going on with operational technology systems in the same way we can enterprise systems right now.

Mr. Latta. Thank you very much.

Mr. Chairman, my time has expired, and I yield back.

Mr. Rush. The gentleman yields back.

The chair now recognizes the gentleman from Virginia, Mr. McEachin, for 5 minutes.

Mr. McEachin. Mr. Chairman, sadly, my questions have been asked, so I will yield back.

Mr. Rush. The chair thanks the gentleman for yielding back.

Now the chair recognizes Ms. Blunt Rochester for 5 minutes.

Ms. Blunt Rochester. Thank you, Mr. Chairman. And thank you so much to the panel for discussing the security of our Nation's critical energy infrastructure. As was stated by everyone, this is of utmost importance, and we thank you for your work.

I just want to pick up on some of the questioning that was asked before from a

workforce perspective. I served in our State of Delaware as head of State personnel for a while and secretary of Labor. And one of the big challenges is always recruitment, retention, compensation, training. Sometimes the first budget that gets cut is training.

I am curious if you could just talk to us about some of the both challenges that you see in terms of recruitment and retention of individuals in this cybersecurity space and particularly from a nonprofit and a public sector perspective when you are competing with the private sector. And then the other question that I had was around innovation. Are there innovative things that are being done to recruit folks to work in your organizations?

I will start with that, and if we could start with Ms. Evans.

Ms. Evans. So I appreciate the question, and especially coming from Delaware, because the State of Delaware, based on my previous experience, is very innovative in the approach that they are taking. In my work as the U.S. cyber challenge director, we really looked at this. And the blending of nonprofit public sector, the education system, and how you do that and how to identify that and then make it and that commitment of bringing them in is clearly demonstrated in the way that the State of Delaware has tackled this issue.

There are incentives. There are things that we need to do, but what really gets people excited -- and you have to look outside the more traditional places. Some of the people that are best in this field do not come out of STEM. And that is clearly demonstrated when you put together teams in the competitions to see all the skill sets that are needed.

Ms. Blunt Rochester. Thank you. Thank you.

Mr. Dodge.

Mr. Dodge. Thank you for the question. So from a FERC perspective, we are actively monitoring our staffing levels and our needs. And we have actually undertook several programs in the last couple of years. I am not going to get the precise names of the programs. But, basically, there is an internship program where we actually reach out to colleges and bring people in as they are freshman, sophomore in college, and they come in, and they spend a summer or a part of the year working for us.

We are actively working to improve our on-campus relationships with different universities. And then we actively go out and do on-campus recruiting as a followup. And then in addition to that, the Federal Government actually has a tuition reimbursement program that, after the students graduate, they come work for FERC for a period of time. There is actually some tuition reimbursement where they actually can forgive some of their previous student debt.

Ms. Blunt Rochester. Thank you.

And, Mr. Robb.

Mr. Robb. Yeah. I don't have any great insights into kind of the workforce development challenge that we have in the sector other than to underscore that it is real, as we all know.

I would say from a NERC perspective, what we have found is we have been able to attract and retain some very top-flight cyber skilled individuals. But we do that not because we pay them top dollar; we do that because they are committed to our mission. And a number of people in the sector are very committed to the security and the value associated with electricity and so on and so forth. So we appeal to that part of individuals. And we have had some pretty good success with that, but it is a challenge.

Ms. Blunt Rochester. Yeah. Thank you.

And, Ms. Evans, thank you for bringing up also the nontraditional. I think one of the challenges we have as well is an aging workforce. And so even when you look at workforce planning and who will be retiring, making sure that we are staffed up.

My other question was more related, not so much to the cyber, but to our -- to kind of natural disasters and things like that and whether or not, with the severe weather incidents that we are seeing, how are you preparing, whether you call it climate change, whether you call it severe weather, whatever you want to call it? These things are real as well. Could you talk about preparation for those?

Ms. Evans. We also have the emergency response capability in our group. We are looking at our staffing of how to do that. The staffing and the way that our plans are set up mirror the way the FEMA regions are set up. But we also then use a lot of the modeling that is available within the national labs so that we can do predictive types of things.

But what is key to the success in this emergency response is our partnership with private industry. And so we continuously have to have that dialogue with them because it is their resources that we need and that we work with in order to be able to share that information and be able to respond.

Ms. Blunt Rochester. Thank you so much.

And I yield back.

Mr. Rush. The chair thanks the gentlelady for yielding back, and now recognizes Mr. Olson for 5 minutes.

Mr. Olson. I thank the chair. And welcome to our three witnesses.

As my colleagues all know, I love to brag about Texas. And along that line, Mr. Chairman, you are correct, one former part of Mexico became a country before it

became a State, but it wasn't California. It was the Republic of Texas, in existence from 1836 to 1845. God bless Texas.

Mr. Rush. We haven't recovered yet.

Mr. Olson. And this is not a brag, but our grid is the biggest target in America for cyber attacks. We have a free market power system that covers 95 percent of our State run by a group called ERCOT. They manage 46,000 miles of electric power lines, 650 separate generation units. Last summer, their daily load was 72 megawatts hourly. That is a huge, huge amount of power. And as you know, if that goes down, that could be very, very bad.

Along the Houston Ship Channel, 52 miles long, lies America's largest petrochemical complex valued at over $15 billion and growing quickly. And with the shale revolution, we have more and more oil coming into our region for refining. Those are being exported now. Nearly 7 million people live within 30 miles of the port of Houston, Houston Ship Channel. The bad actors know if they can take down our grid, have us lose control of some of these industrial processes, people will be harmed, and some people may even die.

My question is for all three of you. We right now are working hard with the private sector, government there in Houston to address these cyber issues. But we all know we have resources that are limited. We can't go crazy. We can't jack up the prices. These things have to work.

So my question for all of you is how do we balance the proper way to achieve how we can best prevent cyber attacks while making sure we don't jack up prices and make us noncompetitive in a global market? How could we balance this out? What is the key?

Ms. Evans, you are up first.

Ms. Evans. All right. The way to -- the way that we are approaching this and that we are working with our partners at DHS is really doing risk modeling. And so it is really identifying what are those most critical assets that an industry has. And then in my particular case, what I am trying to do is develop a set of tools so that the government as well as our industry partners can actually look at what is the best way, what is the highest risk, how do I protect that, what is the cost associated with reducing the risk in that particular asset.

And so as we move forward with that, a lot of this is, then, how you give them that information so that they can then use that in the marketplace going forward.

Mr. Olson. That is the same model Governor Perry had there in Texas. That made our grid pretty secure when he was our governor. Thank you.

Mr. Dodge, your thoughts, sir.

Mr. Dodge. Thank you. Thank you for the question. So from FERC's perspective, we have the Office of Energy Infrastructure Security that actively is doing things on a voluntary basis, conducting classified briefings, performing architecture assessments, identifying best practices, sharing those best practices. In addition to that, FERC undertook a security investments tech conference back in the spring, a couple months ago, where we actually brought in members of the electric industry as well as the natural gas industry as well as Federal and State public utility commissions and also officials.

The goal of that tech conference was to actually identify best practices, share those best practices amongst protecting infrastructure that is not only FERC's jurisdiction but other infrastructure, look at cost recovery mechanisms to determine whether they are adequate, and whether FERC or the State should take additional action. And also, I was remiss to mention that actually that was a joint DOE, FERC-led tech conference. So

we are actively working with FERC on that.

We received comments back from the public on that tech conference, and we are process reviewing these comments in determining next steps.

Mr. Olson. Thank you. And the man from Neal Armstrong's university, Mr. Robb.

Mr. Robb. Go Purdue.

Mr. Olson. 50 years ago, that man walked on the Moon.

Mr. Robb. I would echo what has been said here. I think one of the key things that we are doing as NERC is taking a risk-based focus to all the work that we do, both in terms of which standards are applicable to which entities and then which standards do we audit and so on and so forth.

So I think there is a clear recognition that one size fits all doesn't work in this area. So in terms of striking that balance between economics and risk reduction, you really just got to make sure you are focusing on the most important risks and not leaving yourself exposed on the other side.

Mr. Olson. Thank you, Mr. Chairman. I remind everybody the stars at night are big and bright.

Mr. Rush. The chair wants to bring the gentleman from Texas down to size. Your time is up.

And now we recognize the gentlelady from New Hampshire, Ms. Kuster, for 5 minutes.

Ms. Kuster. Thank you, Mr. Chairman. I appreciate it. And thank you to all the folks that we have here today.

This is a very important issue, and I know people in New Hampshire are concerned about their critical importance to our families and to communities all across the country.

And it doesn't typically get the attention it deserves, so I appreciate this hearing.

Ensuring that our electric grid can operate without disruptions is imperative to ensuring that hospitals can treat patients, first responders can do their jobs, and schools can educate our children. But all of this can be jeopardized if a foreign entity or bad actor is successful with a cyber attack on our electric grid.

We know our utilities are on the front line of ensuring that our grid is protected, but not all utilities are adequately maintaining safeguards that could combat a cyber attack. And while I am pleased to see FERC taking recent steps to strengthen cybersecurity standards for our Nation's electric system, I still have questions about how we can act in a more transparent way.

So, Mr. Dodge, my first question is directed to you. Could you please explain what happens at FERC when it becomes aware of a utility's noncompliance with cybersecurity regulations?

Mr. Dodge. Sure. Thank you very much for the question. I appreciate the question. So there is a process, and actually the process that takes place is in terms of compliance. FERC oversees the development and enforcement of the mandatory reliability standards, including the CIP standards. NERC, and actually its regional entities, actually conduct periodic audits of the red strategies to make sure --

Ms. Kuster. I am asking when FERC becomes aware that a utility is noncompliant with security regulations.

Mr. Dodge. So that the process would actually take place is either through an audit conducted by NERC or its regional entity or through a self-report from the registered entity to NERC. NERC actually coordinates that. They investigate the noncompliance. The registered entity actually files a mitigation plan, and they mitigate

the concern. And then NERC submits the actual violation, along with a recommendation for penalty, to FERC for review. FERC staff reviews that and makes a decision whether to assess the penalty or not.

Ms. Kuster. And that FERC assessment, does FERC disclose to the public the specific utility that is in violation?

Mr. Dodge. So through the FAST Act that was passed a couple years ago, this actually gives us authority underneath FOIA to identify CEII, which is critical energy infrastructure information.

So critical energy infrastructure information could be engineering, design, prints, vulnerability information about specific electric system assets. FERC, as a policy, looks at that information and any of that information that could potentially be useful to someone who wants to impose harm on the electric system. We do not divulge that information.

So over the past 6 to 12 months, we received a number request, FOIA requests, for CEII-related information, including the entities who have violated some of the CIP standards. We reviewed them in excruciatingly detail, and we have determined which ones to release, which ones not to release. We are still working through that. And we have released the names of some entities where we did not believe it would actually be a threat to security of that entity.

Ms. Kuster. So how would you suggest that we keep our constituents informed of the level of risk to them from a cyber attack?

If you are not willing to be transparent with the public -- and I have heard your explanation why, this is a balance for us. If our constituents are at risk, we need to be able to inform them of the level of risk.

Mr. Dodge. So whenever a -- the utility companies, registering entities, are

actively monitoring the compliance to the CIP standards. As soon as they find a problem or through a self-report or through an investigation, routine audits conducted by NERC or one of its registered entities, they actually work to mitigate that concern and address that concern. We do go through -- you know, through the FOIA process and CEII process and review the individual FOIA requests, and we do make the information available as appropriate.

Ms. Kuster. So if there is a bad actor, you would tell my constituents or anyone else in this country, in this Congress, tell the public we have had repeated concerns about compliance with this bad actor?

Mr. Dodge. So we actually review the information that is publicly available or the information that is filed with FERC. And we look at the information. We look at what level of detail, technical details in the information, whether releasing that information would identify any vulnerabilities or make available any information that was particularly useful to someone who wants to impose malintent or ill harm on the electric system. We do not release the names of the entities in that situation.

Ms. Kuster. So I am just trying to raise the balance of protecting our constituents. But my time is up. I appreciate your response.

Mr. Dodge. Thank you.

Mr. Rush. I thank the gentlelady.

The chair recognizes my friend, the gentleman from West Virginia, who has the best mustache in the whole Congress, Mr. McKinley, for 5 minutes.

Mr. McKinley. Thank you, my friend.

Mr. Chairman, I would like to ask unanimous consent that this article with comments from Mr. Robb about the grid be submitted for the record.

Mr. Rush. Without objection, so ordered.

[The information follows:]

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

Mr. McKinley. Thank you.

Mr. Chairman, I would also like to expand on the theme of this keeping the lights on to include grid reliability. Last Congress, as you well know, our committee held a number of hearings on this -- on the grid and reliability and resiliency. But it is not just the Energy and Commerce Committee that is concerned about the grid and its reliability. We had a report that was produced by the National Energy Technology Laboratory that said that without the use of coal, the Eastern United States would have suffered widespread blackouts during the 2018 bomb cyclone. Think about that.

ISO New England said that -- in their report said that the most significant challenge that they face is fuel security and that coal and nuclear power plants are needed to maintain reliability. And lastly, Secretary Perry said in 2017 that the resiliency of the electric grid is threatened by the premature retirements of these fuel secure traditional base load sources.

So, Mr. Robb, if I could turn to you. Last week, you made these remarks, these profound comments, I believe, regarding the grids in both Texas and New England specifically.

Regarding Texas, you said -- pardon my French here on this. You said there is no way in hell they can keep the lights on, and yet they do. Regarding New England, you said the grid operators constantly are finding ways to pull another rabbit out of the hat to keep the lights on, when any of us would look at that situation as engineers and say it has got to break.

So, Mr. Robb, should Congress be more concerned with this situation?

Mr. Robb. So I am not sure I used exactly all the colorful language that was

reported in the --

Mr. McKinley. It is in the press. Whatever is in the press, you know we believe it.

Mr. Robb. I have to watch my vocabulary sometimes.

I think the point around this -- and I threw a third market in there, California. I think all three of these markets are demonstrating the challenges associated with the transformation that is going on within the electric grid. The agencies in California revolve around the deployment of solar and the role of natural gas to balance those resources. Texas has kind of a contemporary problem of just reserve margin, which is one of the planning statistics that we look at to assess whether or not there is enough resource to meet load. That is below levels that traditionally people would say are reliable. New England has a fuel security problem, as noted there.

I don't know that these are congressional issues as much as they are market issues and State policies around resource development and deployment. And the point that I don't think got reported quite as clearly as I would have hoped is that what we are seeing in these area are market operators innovating and finding ways to make the system work in ways that aren't consistent with traditional rules of thumb. And I think the key here is for us to modernize our thinking.

Mr. McKinley. Let me try to get a couple more questions in. If I could go to my fellow colleague from -- fellow Mountaineer from West Virginia, Ms. Evans, and also Mr. Dodge.

In your experiences, are fuel security -- are fuel secure coal and nuclear plant base load power plants critical to maintaining grid reliability? Both of you, please.

Mr. Dodge. So there has been a lot of work done in this area. And, you know, what you really have to look on overall --

Mr. McKinley. It is a yes or no, isn't it?

Mr. Dodge. So what you really --

Mr. McKinley. Let me ask the question again.

Are fuel-secure coal and nuclear base load power plants critical to maintaining grid reliability?

Mr. Dodge. I would like to get back to you in writing with the answer to that question.

Mr. McKinley. Be what?

Mr. Dodge. I would like to get back to you with an answer to that question.

Mr. McKinley. Okay.

Ms. Evans.

Ms. Evans. I believe that the Secretary has, and the administration has, expressed its commitment to multiple sources as it relates to the reliability and our commitment as it goes forward. And our budget request also reflects our commitment to new sources such as nuclear.

So if you need a more detailed answer, I am happy to take that question for the record and get back to you as well.

Mr. McKinley. Thank you.

I yield back my time.

Mr. Rush. The gentleman yields back.

The chair now recognizes Mr. O'Halleran from the great State of Arizona.

Mr. O'Halleran. Thank you, Mr. Chairman, especially for letting us know that Arizona is a great State since I came from Illinois originally. It is also a great State. Thank you.

Thank you, Mr. Chairman and Ranking Member Upton, for holding today's important hearing on ways to -- as the government can ensure our electrical grid assets remain protected and our agencies and stakeholders are fully empowered to defend against cyber threats.

My State of Arizona is one of the most diverse States in the country when it comes to electric generation and sources. While more electric grids integrate renewable energy into their grids, it is essential that reliability of the grid is never interrupted.

As cyber attacks continue to increase across multiple sectors, it has become clear that threats from information sharing, collaboration, and partnerships between government agencies and industry are necessary to achieve a full defensive cyber posture.

Assistant Secretary Evans, in your testimony, you highlighted the cyber analytics tools and techniques programs as one of the several DOE initiatives to promote cybersecurity defense at the energy sector who owns the critical infrastructure assets. What is DOE doing to support threatened information sharing, analysis, and timely, and I repeat timely, return of actionable intelligence back to energy sector entities? And is the energy information flow reciprocal?

Ms. Evans. I appreciate the opportunity to talk about that specific initiative. We refer to it as CATT. And the key to that is the timeliness of getting the information back. So I would like to share one particular piece that is happening on that project.

One of the things that is important is getting the contributions of the information from private sector. I think what you have heard today is that there is a lot of information sharing that happens. What we have to do, then, is be able to anonymize it to put it into a big pool, which our national labs have worked with us on that, but then keep enough

information with it so that as they identify something across a big trend, that we can then take it back out of that pool and give actionable information either through the ISAC or directly to that entity.

That is what that platform is doing through the multiple pilots that we have into research and development. We talked about CRISP. That is one of the contributions to that. And the whole key to that is to keep our portion of it declassified so that it will end up being machine to machine in the long run by using the advances of technology.

Mr. O'Halleran. I have some other questions that I prepared. But, in general, as I have been listening today, I have heard the word whole of government mentioned. I have heard best management and practices mentioned. The shortage of, obviously, potentially the workforce that is going to be needed. And then I took a look at your budget in the Department of Energy and found that -- I don't know how you are going to get that all accomplished with that budget. I don't know -- I am not going to leave you here today secure to be able to tell my constituents that we are in a position to fully defend the electrical grid at this moment in time. I would like to make sure that I can eventually be able to see a timeline on these projects that you have mentioned today, a cost estimate on how much it is going to cost us within that timeline and with a more aggressive timeline, because this is something that we continually -- is continually changing, as you know, but also continuing to be a threat to our country.

I am concerned about some of the more volunteering reporting structure that I heard about today, especially as we get down and down into having less personnel available and that are a level of competency to be able to address those needs on an ongoing basis. And we have newer and newer energy sources coming online with much smaller budgets and getting into the grid than some of the other major competitors that

are out there.

So, in general, I think this has been a good and enlightening process today. But as far as enlightening me, it has been one that has left me with more questions than answers, especially in the integration of how that whole process is working in that timely fashion.

So I want to thank you all for being here today, and I yield.

Mr. Rush. The chair thanks the gentleman.

Now the chair recognizes Mr. Griffith from Virginia, the great State of Virginia, for 5 minutes.

Mr. Griffith. Thank you very much, Mr. Chairman. I greatly appreciate it.

Assistant Secretary Evans, you and I spoke last year discussing pipelines and some of the concerns that my constituents have. And I was going to ask you some questions on updating me on what you all were doing related to pipeline cybersecurity and coordination. You answered those questions earlier when Ranking Member Upton was asking questions, and so I appreciated those answers. I am going to skip those questions that I would have asked, because I don't believe in asking the same question over again just so it gets on my video clip.

But if anybody back home is watching this, I encourage them to flip back a little bit and look at your answers, both yours and Mr. Dodge's answers, to Ranking Member Upton in regard to the coordination that you all are doing. And it sounds like -- although it was classified, it sounds like you all are headed in the right direction.

Do you have anything to add? Are you doing the same kind of coordination on physical threats to the pipelines as well?

Ms. Evans. The short answer is yes, sir, and that that then is also then

demonstrated through the exercises. And that information is also shared through the ESEC meetings that we have when the government partners are there and talking about the physical threats that happen to the pipelines with the voluntary reports. And FBI is there, and that has been highlighted from our industry partners to the FBI.

Mr. Griffith. All right. Mr. Dodge, did you want to add anything regard to the physical threats? Because we have already talked about the cyber.

Mr. Dodge. The only thing I would add is that in terms of the pipeline activity, OEIS is also involved with that activity. They work with DOE to conduct a security briefing threats. In addition to the ESCC, they are actually actively involved with the ONG SEC as well.

Mr. Griffith. And because there are continuing concerns, I think that the questions that Mr. O'Halleran just asked are also important. And some of the questions, we will continue to look at at this committee. And if you need our help passing legislation or something, we want to make sure that we have as much safety as we can. And I appreciate that.

Assistant Secretary Evans, when it comes to pipelines, TSA is taking the lead in developing some voluntary guidelines for industry to follow. According to reports from the GAO and the CRS, they have only a handful of people working on cybersecurity for pipelines.

Do the TSA staffing and resource constraints concern you? And this is a lob in hopes that maybe I think maybe DOE ought to take the lead.

Ms. Evans. So as you know, through the oil and natural gas, SEC as well as the government, the Government Coordinating Council, we work jointly with Department of Homeland Security and TSA. And so our resources we use to leverage the TSA resources

because we recognize as a government that we need to address this vulnerability.

Mr. Griffith. And I appreciate that. But am I correct -- and I may not be. But am I correct that DOE is actually putting more capacity and has more folks working on this than TSA?

Ms. Evans. I would not presume to answer a TSA staffing issue, sir, at this time, because I know that that is an internal discussion to DHS, and it is more appropriate for that question to go to DHS at this time.

Mr. Griffith. Maybe you can encourage them to talk to us about this as well. I appreciate it.

Would you describe the Energy Government Coordinating Council and DOE's role in that council?

Ms. Evans. We are the co-chair of the Government Coordinating Council with Department of Homeland Security. We help craft the agenda. Going forward, we work with DHS hand in hand and our government partners. A good example of that work, we just recently did a top secret SCI briefing for the Interstate Natural Gas Association of America, so -- keeping with the pipeline theme, so that we could really share with them and coordinate through the intelligence community what risks that they are facing. And that was to the executive board of that association.

Mr. Griffith. And I don't even remember now who it was. They didn't reveal any secrets, but they felt like that was a useful -- somebody reported to me they felt like that was a useful -- it was a good use of their time and it was a useful meeting.

In this space, should DOE have the lead role to ensure the safe and reliable flow of energy across the U.S.?

Ms. Evans. I believe, sir, right now that we do have that role as it relates to the

sector-specific responsibilities that we have that are outlined both in the FAST Act and the Presidential directives.

Mr. Griffith. Well, and as I have revealed my prejudices in this regard, I do think the DOE is probably where -- I think DOE should probably be in the leadership role in coordinating preparedness and cybersecurity efforts on all aspects of our pipelines. And you have already indicated you can't talk about the staffing, but would you disagree with me on that?

Ms. Evans. I believe that we have unique expertise. And as the sector-specific agency, we use that expertise across the energy sector and with our partners in private industry.

Mr. Griffith. I appreciate it very much.

Thank you, Mr. Chairman. I yield back.

Mr. Rush. The gentleman yields back.

The chair now recognizes the gentlelady from Washington, Mrs. McMorris Rodgers, for 5 minutes.

Mrs. Rodgers. Thank you, Mr. Chairman. And I appreciate the witnesses being here today to share your perspective on this important topic.

Assistant Secretary Evans, I understand that one of the most exciting projects is looking at how software-defined networking, SDN, technology developed by Schweitzer Engineering Laboratories in Pullman, Washington, in partnership with the Pacific Northwest National Laboratory, next door in the Tri-Cities, can be used to help secure the energy infrastructure at critical national security facilities.

Can you share more about this project with the committee and tell us how it is going?

Ms. Evans. So that is a promising project that we are funding. This particular project, it is called CEDS. Everything has an acronym. So it is the strategic engagement between the Department of Defense and Department of Energy. But it also includes the Veterans Administration as well as the Coast Guard.

And what it is really looking at is a different way to manage the network and network trafficking. And so that is the idea behind software-defined networks. And so it is divorcing it from, really, very static types of architecture to make it more dynamic so that you can then address, on an ongoing basis, the threats, and doing analytics, and then adjusting your configurations as it goes forward.

So we -- right now, there is a successful implementation that is happening in Virginia at Fort Belvoir. And PNNL is continuing to work to roll this out with our partners in multiple places, and I believe the next place is going to be Nevada.

So as that information comes in, we are using that to then invest in other efforts across the national labs so that we can then add that into the overall solution that was brought up earlier.

Mrs. Rodgers. It is crucial that information about vulnerabilities such as cyber attacks is shared between government entities and electric grid asset owners. I believe the creation of CESER was an important step, and I applaud the Department's commitment to engaging the public-private critical infrastructure community. But there is more work to be done, especially regarding engagement with critical infrastructure equipment manufacturers.

Again to Assistant Secretary Evans, what steps has your office taken to include, not just asset owners, but also vendors such as the designers and manufacturers of critical infrastructure equipment like SEL in my district?

Ms. Evans. Well, the initial piece -- several of this is done through our research and development programs that we have that we fund where we are requesting that manufacturers and folks that produce hardware that are in the grid participate. So there were 11 projects that were recently funded that are actually looking at firmware down to the level of how these things are done, and then being able to say, okay, that is a more secure product. We have demonstrated that, and now we are going to go ahead and implement that and show that information out. So those are some of the short-term things that we are doing.

The longer term things are like our CyTRICS program which is looking at bigger types of manufacturing activities and being able to share that information out. And the longer term play that we have is the advanced manufacturing institute that is really going to look at how can we improve this in the long run on an ongoing basis to address that manufacturing up front and be able to share that information and then be able to take advantage of the innovation that we have.

Mrs. Rodgers. Thank you.

There is a growing concern about the presence of certain foreign manufactured components in various aspects of our 21st century infrastructure, whether in communications, telecommunications, or our electric grid.

For the panel, what potential risk does the growing dependence on foreign manufactured components in our energy supply chain create? And how do we mitigate such potential risk while recognizing that it would be impossible to completely phase out all foreign-made equipment?

Mr. Dodge. So from a FERC perspective, approximately 2 years ago, we actually directed NERC to develop a standard to address supply chain risk. NERC filed the

standard with us and we approved it. It actually helps address some aspects of supply chain risk. We also directed NERC to go back and do additional work in this area and to look at the supply chain risk associated with electronic access control systems, as well physical access control systems, as well as look at the potential supply chain risk for low risk -- or low impact cybersecurity assets.

They have conducted a report on that, and they are in the process of following up on that. And I defer to Jim to add additional information on that.

Mr. Robb. So Andy is right where this is an ongoing exploration of a very complicated topic. Our next step on this is that we will be issuing, later in August, what we call a 1600 data request which will go out to all the utilities that are in the NERC registry and collect a lot more information on what suppliers, what equipment is actually out there. So we will have a better sense of the extended condition, which will then inform what the appropriate next steps might be in order to mitigate whatever threats might be out there.

Mrs. Rodgers. Okay. I look forward to seeing more of that. Thank you.

And I will yield back my time.

Mr. Rush. The gentlelady yields back.

The chair now recognizes the brilliant cosponsor of H.R. 2062, Mr. Walberg of Michigan, for 5 minutes. Great State of Michigan. Upper Michigan, not lower Michigan.

Mr. Walberg. Lower Michigan. Thank you, Mr. Chairman. And having been born and raised part of my life in your district as well, I appreciate serving with you and also drawing attention to the fact that we were successful in getting $3 million amendment for CESER passed the House. And that is the first step.

Secretary Evans and the rest of the panel, thank you for being here. As I am sure

you know, Chairman Rush and I, as he has just mentioned, have H.R. 362, the Energy Emergency Leadership Act, which would codify the functions assigned to your office as permanent Assistant Secretary.

Can you briefly address for us today how you think such an authorization could improve CESER's ability to carry out its important mission in the long term?

Ms. Evans. I think it -- first, I appreciate the leadership that you are showing with that and the commitment to the office and the commitment to the administration.

What it will do is ensure the ongoing establishment of the office. It will ensure continuity as it goes forward. That has already been done with the line item in the budget. That helps. And so this would be the conclusion to solidify what this Assistant Secretary position is intended to do to realize what you had envisioned with the FAST Act of 2015 as well.

Mr. Walberg. I appreciate that.

Secretary Evans, due to the fast evolving nature of cybersecurity risks, security cannot be achieved through standards alone. Reliability and security depend on constant awareness and information sharing between utilities and the government and coordination among the government's efforts.

As you know, the FAST Act that you mentioned codified DOE as the sector-specific agency for cybersecurity for the energy sector. This provision requires DOE to coordinate with the Department of Homeland Security and other relevant Federal agencies.

Can you provide an evaluation of how your office and DOE have coordinated with other agencies?

Ms. Evans. We take our responsibility very seriously as the sector-specific agency, and we lead those efforts in conjunction with the Department of Homeland Security. The

Department of Homeland Security overall has responsibilities for all the sectors. We are just one of those sectors. We view we are critical to that effort, and we work in multiple ways jointly with the whole of government. I know everybody is talking about the whole-of-government approach, but that truly is the way that we need to do this.

We are just one piece of the puzzle, and it has to be looked at across the board both within the intelligence community as well as the Department of Defense, Department of Transportation. All of this is interconnected. And we do lead that as the energy-specific agency, and it does work well.

And so there is -- there are examples upon examples of where we can show that it is working well. And it is being mobilized right now as we are watching the hurricanes approach. And so I do believe that us as the lead, as the sector-specific agency, we are committed to doing that, and our partnership with our fellow agencies, it does work well.

Mr. Walberg. Thank you.

The FAST Act also amended the Federal Power Act by introducing a new tool of grid scale emergency declarations that could be provided by the President. If the executive branch were to ask or order a utility to take or not take certain actions with regard to the intrusion or vulnerability, there are concerns that utilities may face legal exposure by acting contrary to their first course of action.

Has CESER or the Department considered the possibility and in such circumstances that are not grid scale emergencies? Are you aware of these concerns over this type of incentive structure creating ambiguity or strain?

Ms. Evans. So that is one thing that we are working in partnership with our industry partners as well as State and local governments. Should the President declare a grid emergency, looking at the way that Department of Homeland Security is -- through

the National Risk Management Center is identifying risk, we -- and then also the work that is going on through our Office of Electricity with the North American resiliency model, you can then start seeing what kind of risk there would be based on the way the infrastructure is set out.

We are working in conjunction with them to be able to highlight these issues through a policy process in the administration to make the determination should additional legislation or liability protections are needed, if and when that happens.

Mr. Walberg. Mr. Dodge, if I could, has FERC looked at this issue as well?

Mr. Dodge. [Off mic.]

Mr. Walberg. Okay. Thank you.

I yield back.

Mr. Rush. The gentleman yields back.

The chair now recognizes Mr. Johnson for 5 minutes.

Mr. Johnson. Thank you, Mr. Chairman. And thanks to our panel for being with us today.

Ms. Evans, because DOE is the sector-specific agency for cybersecurity for the energy sector, the work your office does is so very important. And that importance will continue to increase as our dependency on technology grows.

Last time you testified, we discussed DOE's role in the tri-sector working group, which, as I understand it, was organized to help us better identify and ideally safeguard some of the interdependencies of the critical functions of each sector of that group; that is, our electric utilities, our financial sector, and telecom industries.

So last time we talked, this work was just beginning and discussions were under way on how to best direct that work. Can you please provide an update on how these

conversations have been going and if this work is helping to better safeguard these critical industries?

Ms. Evans. So I am happy to provide the update. The work is continuing. There is -- obviously, there is an industry side of this. The industry group has identified and has fed into the process that DHS, when they release the national critical functions, that work of the tri-sector group, both the government as well as the industry side, fed into what are those national risk indicators.

Based on that, now, the groups are going down, both on the government side as well as the industry side, looking at those interdependencies. And then, in essence, it is a risk register. And then looking at those interdependencies between those three sectors and then what can we do to mitigate the risk as we go forward.

So the work is continuing. It is getting to a more granular level. But that is to be expected so that we can then inform how are we going to, then, deal with it as we go forward.

Mr. Johnson. Okay. All right. Well, I am an IT guy by -- in my profession before I came to serve here in Congress. How can Congress be helpful with this work moving forward?

Ms. Evans. What I believe is going to happen, and this is what we are going to have to look at going forward is, as you start seeing these interdependencies, especially as it relates to technology, we have covered some of the issues going forward is there probably will be help. There will be things that we will need to discuss with you that could say that maybe the legal framework in order to be able to share the information needs to be more robust. That is a path that we are exploring. We are looking at it from the government side. I know the industry side is looking at that as well.

Mr. Johnson. Okay. Shifting gears just a little bit. To the entire panel, looking at strengthening our workforce, I spent 26-1/2 years in the Air Force doing large scale IT projects. Many of them very secure programs. Lots of experience and skills among our military veterans that are getting out. So what are you doing -- and I will give each panelist an opportunity to comment on this. What are you doing to incorporate cleared individuals such as military veterans in your cyber assignments or cyber workforce hiring initiatives?

Ms. Evans, you want to go first?

RPTR ZAMORA

EDTR ZAMORA

[11:32 a.m.]

Ms. Evans. Oh, okay. Sure. As you said, sir, they have a series of skills that are readily transferable. We are doing targeted recruiting as we are going forward. We do partner with DOD. There are a series of programs that are out there that some of them have already been mentioned today that allow for that transference to go back and forth.

And so there are programs that the nonprofit sectors are also looking at so that military personnel know how their skills translate into civilian sector as well. I think a lot of times what I have seen in my experience is they don't necessarily know that it translates into this particular job --

Mr. Johnson. Yeah. It has been that way since 1999 when I retired. The information -- the amount of information going to our veterans and letting them know where their services might be useful has not gotten a lot better in almost 30 years. I hear you.

Mr. Dodge.

Mr. Dodge. Sure. Thank you for the question. So we received a similar question a little bit earlier today and we responded to that. I am not an expert in the Federal Government, the human resource policies, but I can tell you that we have recently hired several recent veterans into our organization.

Mr. Johnson. Okay.

Mr. Robb, quickly.

Mr. Robb. Yeah. I kind of have a similar answer as Andy. And I would say this

transcends cyber. We found military veterans to be a great fit for our mission in a number of areas, and I would guess a material -- I won't give you a number but a material part of our workforce are ex-military.

Mr. Johnson. Okay. All right. Thank you.

Mr. Chairman, I yield back.

Mr. Rush. The gentleman yields back.

The chair now recognizes the gentleman from Texas, Mr. Veasey, for 5 minutes.

Mr. Veasey. Thank you, Chairman Rush. Really appreciate you holding this hearing and the witnesses that have taken the time to come before the subcommittee to discuss ways we can improve the cybersecurity of our Nation's grid.

It is clear that electrification of our world has brought many benefits, but we also face the risk of foreign actors that would like to disrupt that. They understand that it is a benefit and know how disruptive that it would be if they could cause any sort of havoc in that. Advancements in cybersecurity best practices will be helpful in reducing those risks, and we should continue to partner with industry in ensuring our defenses are strong.

And my question today, and anybody on the panel can answer it, I think that it was referenced in testimony from Ms. Evans in particular that the assessment released earlier this year by the Office of the Director of National Intelligence details the capabilities of Russia and China to cause massive disruptions to our energy systems.

And I was wondering if you could expand a little more on what a disruption to an electrical distribution network or a natural pipeline, gas pipeline would mean for those citizens and companies impacted. Can anybody touch on that?

Mr. Dodge. Could you just repeat the very last portion of your question?

Mr. Veasey. Yes. Just expanding on -- a little more on what a disruption to an

electrical distribution network or a natural gas pipeline would mean for citizens and those companies that would be impacted by that disruption.

Mr. Dodge. Okay. Sure. Thanks for the question. So we have not had a disruption up to this point. I want to point that out and make that very clear. We have actually improved the cybersecurity reporting standards that actually reports attempts as well as actual events.

So from an actual customer perspective, it likely could be an interruption, whether it is on an electric distribution system or a natural gas system, and it could be a disruption for some period of time. The period of time could vary quite a bit, and I don't really have additional insight to the answer to your question other than that.

Mr. Veasey. Anyone else have any thoughts?

Mr. Robb. So I would just make the observation that one of the key tenets of the NERC and FERC reliability regime is that if an incident occurs, it quickly gets contained, right, so it doesn't cascade beyond kind of a local boundary to allow kind of, you know -- the various parties that would be required to do restoration are working on a smaller problem rather than a large one.

So the one thing I would say is that the highest likelihood in that area is that an electrical disruption would be contained to a fairly specific area and not cascade.

The other point I would make and, again, this will probably be a better comment for -- coming from the gas industry is a disruption on the natural gas system is really very, very complicated from a safety perspective because of the -- just the nature of the fuel.

Mr. Veasey. Right. Right. Exactly.

Secretary Evans, you talked in your testimony about DOE's role on the National Security Council, and you mentioned the regular unclassified threat briefings that DOE

provides to interagency and industry partners that go with the classified threat briefings to cleared members of the sector.

Can you talk a little bit about the importance of working with industry to head off threats and specifically DOE's interactions with the three energy-focused information sharing and analysis centers?

Ms. Evans. Yes, I am happy to discuss that. We do try to get the information declassified to the greatest extent possible so that it can be distributed through the information sharing and analysis centers that you mentioned. We hold regular meetings with those folks who manage that, the technical teams who manage the ISACs. And they come -- those are handled at classified levels so that they can understand the context around the threat.

But we also then work across with the energy sector and the associations and through the sector specific -- the sector coordinating councils to do both classified and unclassified briefings, so that they can -- the more you can say in a classified environment is great, but you really want to be able to give them information that is actionable so that they can go back and talk to their entire company and what kind of actions they can take and what kind of risks they are posing.

And so we work at multiple levels to make sure that we can get the best information in the hands of those who can then turn it into actionable information for their constituents.

Mr. Veasey. Thank you very much.

Mr. Chairman, I yield back.

Mr. Rush. The gentleman yields back.

And that concludes the witness questions. And I certainly want to thank all the

witnesses for your participation in today's hearing.

I remind members that pursuant to the committee rules, they have 10 business days to submit additional questions for the record to be answered by the witnesses who have appeared. And I will ask each witness to respond promptly to any such questions that you may receive.

The chair now requests unanimous consent to enter into the record the following documents: A letter from the Western Governors' Association, a letter from Protect Our Power, and a letter from the R Street Institute.

Without objection, so ordered.

And the subcommittee now stands adjourned.

[The information follows:]

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

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