KEEPING THE LIGHTS ON: ADDRESSING CYBER THREATS TO THE GRID

HEARING

BEFORE THE

SUBCOMMITTEE ON ENERGY

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

JULY 12, 2019

Serial No. 116–52

Printed for the use of the Committee on Energy and Commerce

govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
40–665 PDF WASHINGTON : 2020

COMMITTEE ON ENERGY AND COMMERCE

FRANK PALLONE, JR., New Jersey
Chairman

BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
DIANA DEGETTE, Colorado
MIKE DOYLE, Pennsylvania
JAN SCHAKOWSKY, Illinois
G. K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJÁN, New Mexico
PAUL TONKO, New York
YVETTE D. CLARKE, New York, *Vice Chair*
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY III, Massachusetts
TONY CÁRDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan
MARC A. VEASEY, Texas
ANN M. KUSTER, New Hampshire
ROBIN L. KELLY, Illinois
NANETTE DIAZ BARRAGÁN, California
A. DONALD MCEACHIN, Virginia
LISA BLUNT ROCHESTER, Delaware
DARREN SOTO, Florida
TOM O'HALLERAN, Arizona

GREG WALDEN, Oregon
Ranking Member
FRED UPTON, Michigan
JOHN SHIMKUS, Illinois
MICHAEL C. BURGESS, Texas
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
TIM WALBERG, Michigan
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina
GREG GIANFORTE, Montana

PROFESSIONAL STAFF

JEFFREY C. CARROLL, *Staff Director*
TIFFANY GUARASCIO, *Deputy Staff Director*
MIKE BLOOMQUIST, *Minority Staff Director*

Subcommittee on Energy

BOBBY L. RUSH, Illinois
Chairman

SCOTT H. PETERS, California
MIKE DOYLE, Pennsylvania
JOHN P. SARBANES, Maryland
JERRY McNERNEY, California, *Vice Chair*
PAUL TONKO, New York
DAVID LOEBSACK, Iowa
G. K. BUTTERFIELD, North Carolina
PETER WELCH, Vermont
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY III, Massachusetts
MARC A. VEASEY, Texas
ANN M. KUSTER, New Hampshire
ROBIN L. KELLY, Illinois
NANETTE DIAZ BARRAGÁN, California
A. DONALD McEACHIN, Virginia
TOM O'HALLERAN, Arizona
LISA BLUNT ROCHESTER, Delaware
FRANK PALLONE, Jr., New Jersey *(ex officio)*

FRED UPTON, Michigan
Ranking Member
ROBERT E. LATTA, Ohio
CATHY McMORRIS RODGERS, Washington
PETE OLSON, Texas
DAVID B. McKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
BILL JOHNSON, Ohio
LARRY BUCSHON, Indiana
BILL FLORES, Texas
RICHARD HUDSON, North Carolina
TIM WALBERG, Michigan
GREG WALDEN, Oregon *(ex officio)*

CONTENTS

Witnesses

Submitted Material

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, DC.

The subcommittee met, pursuant to call, at 9:32 a.m., in the John D. Dingell Room 2123, Rayburn House Office Building, Hon. Bobby L. Rush (chairman of the subcommittee) presiding.

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

Staff present: Jeffrey C. 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 and Technology; Jordan Davis, Minority Senior Advisor; Melissa Froelich, Minority Chief Counsel, Consumer Protection and Commerce; Peter Kielty, Minority General Counsel; Mary Martin, Minority Chief Counsel, Energy and 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.

OPENING STATEMENT OF HON. JERRY McNERNEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

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 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 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 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 cybersecure 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 a 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.

[The prepared statement of Mr. McNerney follows:]

PREPARED STATEMENT OF HON. JERRY MCNERNEY

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'm glad to see DOE, FERC, and others take 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. A reliable grid system is also critical for our national security and clean energy future.

For lawmakers to encourage and enable innovative advancements that can improve the security and reliability of our Nation's energy grid, we must work on a bipartisan basis and actively engage with industry leaders as we are doing today.

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 flow both ways.

Technological advancements are also born from the need to secure the energy grid against potential physical and cyber threats.

For example, technology allowing for the rerouting of power and quick response in the event of attacks 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. 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 along with my good friend from across the aisle, Representative Latta of 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, and 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 electric utilities.

My bill, which I introduced along with Mr. Latta, H.R. 359, the Enhancing Grid Security through Public-Private Partnerships Act, would create a program to enhance the physical and cyber security of electric utilities through assessing security vulnerabilities, increase cybersecurity training, and data collection. It would also require the Interruption Cost Estimate Calculator—which is used to calculate the return on investment on utility investments—to be updated at least every 2 years to ensure accurate calculations.

Mr. Latta's bill, which he introduced along with me, H.R. 360, the 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 a testing and verification program.

The bulk power system supports American industry and provides all the benefits of reliable electric power to the American people.

It is essential that we make this system as secure as possible, as cyber attacks 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 our system.

I thank Mr. Latta for his partnership in these efforts and look forward to continuing to work to ensure a more secure and resilient grid.

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 a 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 Facility 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 utility system.

Thank you and I yield back.

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 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 a lot of——

Mr. RUSH. Thank you.

Mr. UPTON. Yes. Yes. Smart.

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

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 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.

[The prepared statement of Mr. Upton follows:]

Prepared Statement of Hon. Fred Upton

Today's hearing continues the subcommittee's ongoing oversight of cybersecurity threats to the electric grid. While this is the first hearing specifically on that 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 we've done over the past few 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.

The United States has the world's most complex electric grid, and while we have a well-developed system of grid operators to ensure our lights stay on, we're confronting new challenges and adapting to a changing generation mix, new technologies, and consumer preferences. We're 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 the increasing dependence on pipeline infrastructure by electric generating units. Combine this with the rapid expansion of cyber capabilities by more of America's adversaries, and safeguarding transmission infrastructure remains particularly urgent.

Many of the Federal oversight and regulatory structures in place today that ensure the system can mitigate and respond to cyber threats 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 included in the FAST Act to strengthen DOE's energy sector specific authorities and to facilitate sharing of threat information between private sector asset owners and the Federal Government. As the Federal agency with the 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 generating stations to the 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 its jurisdiction. That legislative work is continuing, but fortunately, the Department has used its own authorities to implement enhanced leadership over cybersecurity and to improve interagency coordination.

Against this backdrop, today's hearing provides a great opportunity to update the subcommittee on what DOE, FERC and NERC 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 Ms. Evans testified in September last year, she had been on the job for just a few 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 these entities serve at the front lines of regulatory oversight of electric grid infrastructure protection. I'm particularly interested in learning what measures they are working on to address threats, to ensure best practices, and to coordinate response to cyber incidents.

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

Thank you, Mr. Chairman, for keeping the subcommittee informed on this important topic.

Mr. UPTON. 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.

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

Mr. PALLONE. Thank you, Chairman Rush.

Today we are here to get an 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 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.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Thank you, Chairman Rush, for holding this hearing today on the very important topic of cybersecurity of our Nation's electric grid. We know our enemies are rapidly developing new techniques to compromise and attack our grid. It is important government and industry stay on top of the issue.

I know our witnesses and their agencies—the Department of Energy, the Federal Energy Regulatory Commission, and the North American Electric Reliability Corporation—all take cybersecurity of the grid very seriously and are doing good work. I look forward to today's discussion.

I am pleased Secretary Perry established the Cybersecurity, Energy Security, and Emergency Response, or CESER, office to focus specifically on these pressing issues. Chairman Rush and Mr. Walberg have introduced bill H.R. 362, the Energy Emergency Leadership Act, to enshrine in statute this new focused level of leadership at the Department of Energy. I hope we are able to report this legislation out of the full committee soon.

This bill, along with three other bipartisan bills addressing cybersecurity of our Nation's energy systems, were favorably forwarded to the full committee recently. These bills are a top priority to move, and I am very proud of our strong bipartisan working relationship and the committee's efforts on cybersecurity.

We all understand time is of the essence. March 2019 marks a sobering milestone of the first reported malicious cyber event that disrupted grid operations of a Western utility. Thankfully, there seemed to be very little effect to the transmission grid and no resulting blackouts. We must stay ahead of our enemies and keep it that way.

I appreciate FERC and NERC's work together 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 system hardware, software and services. 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 about cybersecurity relating to our pipelines, I'd 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. DOE, FERC, and NERC's responsiveness to the committee's briefing request and job of oversight is a welcomed change from the stonewalling from TSA who refuse to testify. As I've said before, and my friend from Michigan, Ranking Member Upton has echoed, if TSA does not want to be taken seriously, we may have to look at other options.

I want to thank our witnesses for being here today. I look forward to hearing about CESER's range of work including work on a national strategy and cybersecurity risk assessment of the grid. I also looking forward to hearing about FERC and NERC's continued work to build out a critical infrastructure cybersecurity framework. In general, how are you working to incentivize and implement leading cybersecurity standards? What types of collaborative processes are your agencies working on with industry? And, what can Congress do to support each of your agencies' work?

Thank you, 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. WALDEN. Well, good morning, Mr. Chairman.

Mr. RUSH. Good morning.

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

Mr. WALDEN. 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.

As 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.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Thank you, Mr. Chairman.

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

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 we take very seriously on both sides of the aisle, no matter which party is in the majority.

This morning's oversight hearing continues this important work. It focuses on the status of efforts to address cyberthreats to the electric grid. We will hear testimony from three of the key players for making sure the lights stay on: Department of Energy, the Federal Energy Regulatory Commission, and the North American Electric Reliability Corporation, or NERC.

Each of these organizations has a role in supporting effective information sharing, technical assistance, standard setting, oversight of standards implementation, and sound engineering practices relating to the bulk power system. And I look forward to hearing updates from the witnesses, especially on coordination and sharing among the Federal entities and industry.

Our past oversight has examined 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 mitigate risks. I've seen some of this work at the National Labs, particularly at the Pacific Northwest National Laboratory, in Washington, and at the Idaho National Laboratory, which provide analytical tools, test beds, and other capabilities that are proving very helpful for industry.

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 systematic cyber attacks across the energy sector.

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 risks and operational technology systems—the switches and Supervisory Control and Data Acquisition (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 Upton has noted repeatedly how, because the Nation's pipeline systems are such an integral part of the electricity fuel supply system, harm to pipelines means potential harm to the supply of electricity.

We must think about pipelines as part of a larger energy system—rather than a piece of hardware or a simple mode of transportation. While pipelines fall under separate regulatory regimes, DOE must maintain visibility over pipelines to ensure the delivery of electricity to consumers. That is why this committee has been pushing to codify DOE's emergency response role and strengthen the Department's capabilities to monitor for cyberthreats and to provide technical assistance to industry.

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 be useful today.

As testimony this morning will underscore, the risks to our critical electric 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 that our critical infrastructure protection standards are up to date and sufficiently flexible to meet the risks. We must be sure that we are providing our Federal agencies the tools needed to serve the industry and the Nation more effectively. We have a responsibility here and hearings like this will help us do our job.

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

Mr. WALDEN. And with that, I will 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 her 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 KAREN S. EVANS, ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE, DEPARTMENT OF ENERGY; J. ANDREW DODGE, SR., DIRECTOR, OFFICE OF ELECTRIC RELIABILITY, FEDERAL ENERGY REGULATORY COMMISSION; AND JAMES B. 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:]

Testimony of Assistant Secretary Karen S. Evans

Office of Cybersecurity, Energy Security, and Emergency Response

U.S. Department of Energy

Before the

Committee on Energy and Commerce

U.S. House of Representatives

July 12, 2019

Introduction

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 the 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 non-state 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.

Earlier this year, the Office of the Director of National Intelligence released the Worldwide Threat Assessment, which noted Russia "is now staging cyber attack assets to allow it to disrupt or damage U.S. civilian and military infrastructure during a crisis…" and "…has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effect on critical infrastructure – such as disrupting an electrical distribution network for at least a few hours…" Similarly, it noted that "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure – such as disruption of a natural gas pipeline for days to weeks – in the United States." [1]

The release of the President's National Cyber Strategy (NCS) in September 2018 reflects the Administration's commitment to protecting America from cyber threats. The Department of Energy (DOE) plays an active role in supporting the security of our Nation's critical energy infrastructure in implementing the NCS. These efforts reflect a concerted response to the emergence of energy cybersecurity and resilience as one of the Nation's most important security

[1] Daniel R. Coats, Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community (January 29, 2019): p.5-6

challenges. Fostering partnerships with public and private stakeholders is of utmost importance to me as the Assistant Secretary of CESER.

CESER activated the Emergency Response Organization for multiple natural disasters. In 2018, CESER responded to a wide range of incidents, including six hurricanes, three wildfires, two typhoons, one cyclone, one earthquake, and one volcanic eruption.

Today, I would like to focus my testimony primarily on the cybersecurity function of the office and how CESER meets the priorities of the Administration and works in conjunction with our Federal agency, State, local, tribal and territorial government (SLTT), industry, and National Laboratory partners.

CESER

The Secretary has conveyed that he has no higher priority than to support the security of our Nation's critical energy infrastructure. CESER leads the Department's efforts to secure our Nation's energy infrastructure against all hazards, reduce the risks of and impacts from cyber events and other disruptive events, and assist with restoration activities. This office works closely with the private sector, as well as Federal and SLTT government partners, to enable more coordinated preparedness and response to cyber and physical threats and natural disasters. The office enhances the Department's ability to dedicate and focus attention on DOE's Sector-Specific Agency (SSA) responsibilities and will provide greater visibility, accountability, and flexibility to better protect our Nation's energy infrastructure and support asset owners, as well as the overall critical infrastructure response framework overseen by DHS.

DOE FAST Act Authority

DOE's role in energy sector cybersecurity is established in statute and executive action. In 2015, Congress passed the Fixing America's Surface Transportation Act (FAST Act) (P.L. 114-94), codifying DOE as the SSA for cybersecurity for the energy sector, consistent with existing policy. In 2018, Congress passed the Cybersecurity and Infrastructure Security Agency Act (CISA Act) (P.L. 115-278) establishing CISA within the Department of Homeland Security (DHS). Defined in the CISA Act, "[t]he term 'Sector- Specific Agency' (SSA) means the Federal department or agency designated under this directive to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment in coordination with the Department." Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience states that DHS will "provide strategic guidance, promote a national unity of effort, and coordinates the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure." Specific to cybersecurity, DHS has authorities that support cybersecurity assistance by the federal government to all critical infrastructure sectors, including information sharing and technical assistance. The FAST Act further mandates that the Secretary of Energy coordinate "with the Department of Homeland Security and other relevant Federal departments and agencies" and collaborate with them on, among other things, "providing, supporting, or facilitating technical assistance and consultations for the energy sector to identify vulnerabilities and help mitigate incidents, as appropriate." With the formation of CESER, the Department's role as the SSA is strengthened and has undertaken the responsibilities with the highest degree of dedication and commitment.

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

DOE's Roles and Responsibilities for Energy Sector Cybersecurity

The National Cyber Strategy (NCS) prioritizes risk-reduction activities across seven key areas, which include national security; and energy and power. DOE's cybersecurity activities for the energy sector align to the Secure Critical Infrastructure section of Pillar I – (Protecting the American People, the Homeland, and the American Way of Life) under the category to Prioritize Actions According to Identified National Risks. It states: "The Federal Government will work with the private sector to manage risks to critical infrastructure at the greatest risk. The Administration will develop a comprehensive understanding of national risk by identifying national critical functions and will mature our cybersecurity offerings and engagements to better manage those national risks."

The strategy presents a risk-reduction-based approach to improve the Nation's cybersecurity posture in key areas, and builds on the DOE's ongoing collaboration with other agencies and private sector organizations, including the Federal Government's designated lead agencies for coordinating the response to significant cyber incidents: the DHS, acting through the National Cybersecurity and Communications Integration Center (NCCIC), and the Department of Justice (DOJ), acting through the Federal Bureau of Investigation (FBI) and its National Cyber Investigative Joint Task Force. In the event of a significant cyber incident in the energy sector, DHS and DOJ coordinates with DOE to ensure its deep expertise with the sector is appropriately leveraged.

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

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

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

DOE's Cybersecurity Activities for the Energy Sector

DOE plays an active role in supporting energy sector cybersecurity by enhancing the security and resilience of the Nation's critical energy infrastructure. To address these challenges, it is critical for us to be proactive and cultivate 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 strengthen energy sector cybersecurity preparedness, coordinate cyber incident response and recovery, and accelerate game-changing research, development, and deployment (RD&D) of resilient energy delivery systems.

Strengthening Energy Cybersecurity Preparedness

It is necessary for partners in the energy sector and the government to share meaningful and timely emerging threat data and vulnerability information to help prevent, detect, identify, and thwart cyberattacks more rapidly. CESER is working with government partners and the energy sector to develop a secure platform to provide energy sector-wide situational awareness and actionable information to support the discovery and mitigation of advanced cyber threats to U.S. critical energy infrastructure. The Cyber Analytics Tools and Techniques (CATT ^{TM} 2.0) program will achieve this through automated analysis of voluntarily provided energy sector information technology (IT) and operational technology (OT) data, enriched with classified threat information utilizing unique and sophisticated U.S. Government tools.

Advancing the ability to improve situational awareness of OT including Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems is the key focus of DOE's current activities. Detecting adversary tactics, techniques, and procedures within anomalous traffic on critical energy infrastructure can be the first step in stopping an attack in its early stages. The Department is working with our private sector partners to develop the capability to analyze the data from OT systems via the Cybersecurity for the Operational Technology Environment (CyOTE^{TM}) pilot project. The CyOTE^{TM} pilot will develop into a scalable program for industry to aid in detecting and mitigating cyber risks to OT systems.

Additionally, CESER is implementing a threat-informed, engineering-centric assessment and mitigation activity for the energy sector called Consequence-driven Cyber-informed Engineering (CCE), which is being supported by the Idaho National Labs (INL). The methodology prioritizes high-consequence risks within control systems environments, identifying the most severe consequences, and then identifies the best process design and protection approaches for eliminating the cyber risk. The lessons collected from the upcoming engagements within the energy sector will be shared with our partners to greatly expand the nation's ability to "engineer out" the cyber risk from the most critical energy infrastructure networks and systems.

Cybersecurity vulnerabilities of key control systems and operational technology are an increasing concern for the Nation's critical energy infrastructure owners and operators. The Cyber Testing for Resilience of the Industrial Control Systems (CyTRICS) program will serve as a central capability for DOE's efforts to increase energy sector cybersecurity and reliability through testing and enumeration of critical electrical components. Further, analysis of test results will identify both systemic and supply chain risks and vulnerabilities to the sector through the linkage of threat information with supply chain information and enriching it with other data sources and methods. Through CyTRICS, DOE continues to collaborate with government, National Laboratories, and industry to identify key energy sector industrial control systems components and apply a targeted, prioritized, and collaborative approach to these efforts.

CESER's efforts to develop a collective understanding of systemic and supply chain risks and vulnerabilities are aligned with Executive Order 13873 "Securing the Information and Communications Technology and Services Supply Chain," and support the Administration's priority of securing our Nation from foreign adversaries who are increasingly creating and exploiting U.S. vulnerabilities in information and communications technology.

Facilitating Cyber Incident Response and Recovery

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

As a member of the National Security Council and as the Energy SSA, DOE assesses and analyzes credible threats to reliability and resilience issues facing the security of our Nation's energy infrastructure. These intelligence assessments and analysis often involve classified information; however, DOE works to provide regular unclassified threat briefings to interagency and industry partners, in addition to classified threat briefings to cleared members of the sector.

DOE also maintains a close relationship with the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) to ensure they have the relevant information to execute their missions. DOE also holds regular discussions with the three energy sector Information Sharing and Analysis Centers (ISACs) – which include the Downstream Natural Gas ISAC (DNG-ISAC), the Oil and Natural Gas ISAC (ONG-ISAC) and Electricity ISAC (E-ISAC) – to share emerging and potential threats and disseminate information.

In June, CESER worked with the National Association of Regulatory Utility Commissioners (NARUC) to help State public utility commissioners (PUCs or "commissions") gather and evaluate information from utilities about their cybersecurity risk management practices. These PUC-driven evaluations of utilities in their states help to inform PUC investment decisions regarding the effectiveness of utilities' cybersecurity preparedness efforts and the prudence of related expenditures. The preparedness and evaluation toolkit are publicly available on the NARUC website, benefitting not only commissioners, but other State officials as well. By regularly engaging with utilities through the use of the toolkit materials and analyzing the information received using the tool, commissioners can access the year-over-year change in cybersecurity preparedness of individual utilities within a PUC jurisdiction, promote continuous improvement, and increase the overall awareness and visibility of cybersecurity preparedness and resilience across the utility landscape within their states.

We are continuing to work with NARUC to support regional trainings on cybersecurity, with the goal of building commission expertise to ensure cyber investments are both secure and economically viable.[2]

CESER also recently supported the National Governors Association (NGA) in providing Governors and their energy advisors with policy strategies to protect electricity infrastructure and enhance cybersecurity in the electricity sector. The NGA white paper outlines the roles and responsibilities of key State, industry, and Federal entities and catalogs useful resources.[3]

DOE continues to work with State officials to facilitate state-industry preparedness and response coordination, encourage response plans that help prepare for any potential consequences of a cyber attack, and offer training and exercises to ensure the states are ready and able to mitigate incidents and respond, if needed.

DOE also works closely with our public and private partners with the goal of fully supporting and bolstering the actions needed to help ensure the reliable delivery of energy. We continue to coordinate with industry through the Sector Coordinating Councils (SCCs) to synchronize government and industry cyber incident response playbooks.

CESER engages directly with our government and industry partners to help ensure we are prepared and coordinated in the event of a cyber incident to the industry. The success of the 2018 iteration of DOE's Liberty Eclipse cybersecurity exercise developed in two phases. Phase I was a tabletop exercise focusing on the roles, responsibilities, and authorities, of Federal, State, and energy industry partners in response to a significant cyber attack on energy infrastructure.

Phase II included a seven-day, operations-based exercise conducted on Plum Island in New York. This exercise focused on increasing the country's ability to mitigate adversary cyber degradation of the grid's restoration capability. During Phase II, DOE worked with the Defense

[2] The NARUC toolkit comprises several resources, including the three documents published in June, 1) Understanding Cybersecurity Preparedness: Questions for Utilities; 2) Cybersecurity Preparedness Evaluation Tool; and 3) Glossary, in addition to the "Cybersecurity Strategy Development Guide" published in 2018. (https://www.naruc.org/cpi/cpi-library/#CIP)

[3] NGA White Paper, Smart and Safe, State Strategies for Enhancing Cybersecurity in the Electric Sector (June 2019). https://www.nga.org/wp-content/uploads/2019/04/NGA-Smart-Safe-State-Strategies-for-Enhancing-Cybersecurity-in-the-Electric-Sector.pdf.

Advanced Research Projects Agency (DARPA) and multiple U.S. utilities to test and evaluate tools and capabilities that could enable the recovery of the power grid during a cyber attack. These experiments were held in an isolated and controlled environment with first responders and power engineers on hand. DOE's private sector collaboration ensures DARPA's research results are directly transitioned to industry and translated into greater preparedness from a cyber attack.

DOE continues to sponsor Clear Path, an annual all hazards focused exercise series. These regionally focused exercises highlight the interdependencies between our Nation's energy infrastructure and other sectors.

DOE's most recent exercise, Clear Path VII, took place in Memphis, Tennessee, in April 2019. This iteration examined the energy sector's response and restoration roles, responsibilities, plans, and procedures following a major earthquake along the New Madrid Seismic Zone. The exercise brought together more than 160 individuals from more than 80 organizations representing Federal and State governments; the electricity and oil and natural gas subsectors; the transportation, water, and communications sectors.

It is critical that the results of the exercises inform our response plans on a continuous basis to close identified gaps in coordination with our industry and government partners through the associated coordinating councils. Communication capabilities that are survivable, reliable, and accessible, by both industry and government, will be key to coordinating various efforts showcased in the exercise, including unity of messaging required to recover from a real-life version of the exercise scenario.

In preparation for any future grid security emergency, it is critical we continue working with our government and industry partners to further shape the types of orders that may be executed under current authorities, while also clarifying how we communicate and coordinate the operational implementation of these orders. Continued coordination with Federal, SLTT, and industry partners and participation in preparedness activities like Clear Path enable DOE to identify gaps and develop capabilities to support cyber response.

Accelerating Breakthrough RD&D of Resilient Energy Delivery Systems

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

To select cybersecurity R&D projects, DOE constantly examines the threat landscape and coordinates with partners, like DHS, to provide the most value to the energy sector while minimizing overlap with existing projects.

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

In April 2019, CESER released the "Cybersecurity for Energy Delivery Systems (CEDS) 2019 Research Call" to conduct research, development, integration and demonstrations (RDI&D). This RDI&D will lead to (1) next generation tools and technologies, (2) techniques to implement cybersecurity frameworks and (3) integration of tools and technologies to help provide greater situational awareness that is unavailable today. It will likely become available and widely adopted throughout the energy sector to reduce the risk that a cyber incident could disrupt energy delivery. An estimated $35 million in Federal funding is expected to be available for new awards under this research call.

In May 2019, CESER issued an $8 million funding opportunity announcement seeking innovative approaches to enhance the reliability and resilience of the Nation's energy infrastructure. This includes enhancing the ability of electricity generation, transmission and distribution infrastructure, as well oil and natural gas production, refining, storage, and distribution infrastructure to survive a cyber attack while sustaining critical energy delivery functions. This funding opportunity supports the Administration's directive to secure critical infrastructure as outlined in the National Cyber Strategy, through research and development of real-time intrusion detection, self-healing energy delivery control systems, and innovative technologies that enhance cybersecurity in the energy sector.

Existing CESER projects in Artificial Intelligence and Quantum are aligned with the Executive Order 13800 "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" and Executive Order 13859 "Maintaining American Leadership in Artificial Intelligence." We coordinate this with the Secretary's Artificial Intelligence program to ensure broadest awareness and surface new opportunities. For example, the Cyber Attack Detection and Accommodation for Energy Delivery Systems project has advanced artificial intelligence technology by developing a commercially viable, field demonstrated, self-learning and resilient cyber-attack/anomaly automatic detection and accommodation technology to provide uninterrupted, equipment safe, controlled power generation to the grid even in the presence of attacks. This project is integral to the defense-in-depth strategy to support improved resilience in the national critical energy infrastructure. The Cyber Attack Detection and Accommodation for Energy Delivery project uses feature-based machine learning and control and estimation algorithms to detect, localize and mitigate attacks in real-time with very low false positive rates with multiple heterogeneous data streams.

To advance technologies in quantum computing, researchers at Los Alamos National Laboratory (LANL) have developed several technologies based in Quantum Information Science (QIS) for use in improving the security of the nation's electric grid. Specifically, LANL has demonstrated quantum secured communications over existing installed optical fiber infrastructure. This technology allows entities on a network to prove their identity to one another, and to be sure the messages they send are transmitted faithfully. For example, a utility control center can be certain that data received from a substation was indeed sent by that substation and has not been spoofed or altered in transit.

Additionally, CESER's Cybersecurity Risk Comparison tool is developing a method to quantify cyber risk reduction achieved through the deployment of defensive countermeasures, including selected other CEDS R&D-funded tools and technologies. Using the attack tree developed by the NERC-Critical Infrastructure Protection Committee (CIPC) Cyber Attack Task Force (CATF) and the MITRE ATT&CK framework, the research effort will develop a methodology to quantify the dollar investment associated with reducing the number of cyber attack tree paths that are functionally available to the adversary. It will achieve this through deployment of selected countermeasures, and by comparing it to the number of attack tree paths without deployment of the same countermeasures, for a specified control system architecture.

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

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

Strengthening our Workforce Development

The final area I would like to highlight is one that is truly foundational in nature, cybersecurity workforce development. It is also a national priority outlined in the President's National Cyber Strategy, and further reinforced by Executive Order 13870, "America's Cybersecurity Workforce." Through our State, local, tribal, and territorial workforce development efforts through organizations like the National Association of State Energy Officials (NASEO), we are developing a multifaceted approach including online trainings, playbooks, workshops, and guidance. This builds capacity throughout the sector and guarantees the State energy officials we engage with regularly have the necessary and current skills and resources needed to prepare for and respond to energy disruptions of significance, including cyber emergencies.

Building a culture of cybersecurity throughout the energy sector is critical. Technology is playing an increasingly significant role in the energy sector, requiring a workforce with knowledge of both cybersecurity and power systems. Further encouraged by the President's Executive Order on America's Cybersecurity Workforce, DOE is working in conjunction with NRECA and the American Public Power Association (APPA) to help further enhance the culture of security within their utility members' organizations. With more than a quarter of the Nation's electricity customers served by municipal public power providers and rural electric cooperatives, it is critical that they have the tools and resources needed to address security challenges. To address risks and manage the risks to an acceptable level, APPA and NRECA are developing security tools, educational resources, updated guidelines, and training on common strategies that can be used by their members to improve their cyber and physical security postures. Exercises, utility site assessments, and a comprehensive range of information sharing with their members will all be used to bolster their security capabilities.

DOE is also continuing and expanding our annual collegiate-level cyber defense competition. In 2018, DOE held two competitions to help develop the next generation of cybersecurity professionals to help secure our Nation's critical energy infrastructure. DOE's Cyber Defense Competition (CDC) took place in April, with 25 college and university teams competing at three National Laboratories. In December 2018, DOE hosted the CyberForce Competition™, with 64 college and university teams from 24 states and Puerto Rico competing at seven National Laboratories. The next CyberForce Competition™ will take place in November 2019 at ten National Laboratories, and is expected to expand beyond the collegiate level.

Additionally, CESER is working in coordination with the Office of Management and Budget (OMB), the Office of Personnel Management (OPM) and the Federal Chief Information Officer (CIO) Council, to fully leverage current hiring authorities under the Cybersecurity Enhancement Act of 2014. We intend to do this, in part, by utilizing cyber competitions announcements as preliminary job announcements, and then proceed through competition scores to identify highly qualified cyber professionals for potential placement and retention into the Federal Government.

Conclusion

Establishing CESER is the result of the Administration's commitment to and prioritization of energy security and national security. CESER is working on many fronts collaborating with industry and 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 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.

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, SR.

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 a 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 of 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 protection 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 11 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:]

Testimony of J. Andrew Dodge, Sr., P.E

Director, Office of Electric Reliability, Federal Energy Regulatory Commission

Before the Subcommittee on Energy

United States House of Representatives

July 12, 2019

Introduction

Chairman Rush, Ranking Member Upton, and Members of the Subcommittee, thank you for the opportunity to testify today. My name is Andy Dodge. I am the Director of the Office of Electric Reliability (OER) of the Federal Energy Regulatory Commission (FERC or Commission). I am here today as a Commission staff witness and my remarks do not necessarily represent the views of the Commission or any individual Commissioner.

Today, my testimony will provide a brief overview of the Commission's authorities and activities to oversee and improve the cybersecurity of the nation's bulk-power system. Our work includes mandatory reliability standards, audits of those standards, and best practices to ensure that utilities keep apace of threats. We work closely with the North American Electric Reliability Corporation (NERC), its regional entities, other Federal and state agencies, and responsible entities to carry out this important work.

FERC's Authority to Oversee Reliability

In the Energy Policy Act of 2005, Congress gave the Commission the authority to oversee the development and enforcement of mandatory reliability standards for the Bulk-Power System. The authority pertains to the interconnected electricity system (the "grid") in the United States, and excludes Alaska, Hawaii, and local distribution systems.

Section 215 of the Federal Power Act requires FERC to designate an Electric Reliability Organization (ERO) to develop, with industry, standards to ensure reliable and secure operation of the grid, which it proposes to the Commission for approval. NERC is the Commission-certified ERO. After review and approval by the Commission, compliance with the reliability standards is mandatory by users, owners and operators of the grid in the United States. NERC and its six regional entities enforce the standards and may impose penalties for noncompliance, after notice and opportunity for hearing, subject to review and approval by the Commission. The Commission may also enforce reliability standards independently of NERC.

Importantly, the ERO is responsible for developing and proposing new or modified reliability standards to the Commission. The Commission may approve new or modified reliability standards if it finds them to be "just, reasonable, not unduly discriminatory or preferential, and in the public interest." If a proposed standard does not meet this test, section 215 requires the Commission to remand it to the ERO for revision. The Commission may not write or modify a reliability standard. If the Commission determines that there is a need for a new or modified standard, it may, on its own motion or upon complaint, direct the ERO to develop and submit a standard to meet the identified reliability need.

The Critical Infrastructure Protection (CIP) Reliability Standards

Under section 215 of the Federal Power Act, a reliability standard may include requirements related to cybersecurity protection. The Commission exercises authority in this area by overseeing NERC's development and enforcement of Critical Infrastructure Protection (CIP) reliability standards. In June 2006, NERC proposed eight mandatory critical infrastructure protection reliability standards to replace the earlier voluntary cybersecurity standards. On January 18, 2008 pursuant to section 215 of the Federal Power Act, the Commission issued Order No. 706 approving the eight CIP reliability standards, which after allowing a period of time for entities to achieve compliance. The standards became enforceable in 2010. These were the so-called "version 1" of the CIP standards and they were the first and only mandatory cybersecurity standards covering critical infrastructure. In addition, the Commission directed NERC to develop modifications to the CIP reliability standards to address specific concerns identified in Order No. 706.

Since 2008, NERC has periodically modified the CIP reliability standards, submitting new "versions" of the standards for Commission approval. Notably, in January 2013, NERC filed version 5 of the CIP reliability standards, which proposed to alter the method of identifying and protecting cyber systems by categorizing each grid-related cyber system as having a low, medium, or high impact on the reliable operations. Each of the three categories requires security provisions proportional to the specified category. The Commission approved CIP version 5 on November 21, 2013, in Order No. 791. Now, rather than referring to specific versions of the standards, we simply refer to them as the CIP standards. There are currently 11 active cybersecurity standards and one active physical security standard.

The CIP standards, viewed as a whole, 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 systems. The foundational standard (CIP-002) requires a utility to perform a risk assessment of its assets and to categorize them in terms of low, medium and high impact to the grid. Medium and high impact systems include large control centers, ultra-high voltage transmission lines, large substations and generating facilities. Most requirements apply to the high and medium impact systems. Lower impact systems include the remainder of cyber systems that are not captured in the other two categories. Other CIP standards require utilities to: develop and implement cybersecurity plans; train personnel adequately; establish physical and electronic access perimeters; test and apply patches in a timely manner; identify and report cybersecurity incidents; and develop and implement recovery plans; among others.

The CIP reliability standards continue to be reviewed and updated to address new cybersecurity challenges and technological changes. For example, the Commission recently has taken two additional important actions to further enhance the CIP reliability standards. In October 2018, FERC approved NERC's proposed reliability standards to address supply chain threats. This action is particularly significant given that these specific threats to the energy sector continue to grow. Second, last month, at the June 2019 Commission Meeting, FERC approved a modification to a CIP standard to expand reporting requirements of cybersecurity incidents for critical grid cyber systems. Today, entities are required to report successful cyber intrusions that compromise one or more reliability tasks. The revised standard requires utilities to report both successful and attempted cyber intrusions into critical systems to NERC's Electricity Information Sharing and Analysis Center, as well as to the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC). Requiring entities to report attempted cyber intrusions, as well as successful ones, is an important step toward enhancing the collection and distribution of information on rapidly evolving cyber threats.

FERC Audits the Compliance of Entities with the CIP Reliability Standards

As the ERO, NERC and its regional entities are the primary enforcement authorities for the CIP standards, and carry out a compliance program, which includes audits of utilities' compliance with the CIP standards. Starting in 2016, the Commission has been auditing a sample of utilities with respect to their CIP compliance. The audits assessed compliance with version 5 of the CIP reliability standards, which became effective on July 1, 2016. In particular, the Commission focused on utilities for whom compliance with CIP would be new, or for whom the nature of their CIP programs would have to change significantly given the risk-based approach of version 5. NERC and the relevant region participate in the audits with Commission staff.

Because the CIP standards do not prescribe how entities should comply to achieve the stated objective of a given CIP standard or requirement, there are a range of approaches that utilities implement based on the particular configuration of their electrical and computer systems. In the course of performing the audits, our staff, working with NERC and regional entity staff, observe both best practices for CIP implementation and also ways in which entities could improve their security posture and avoid issues of non-compliance. In October 2017 and again in March 2019, the Commission issued a report that describes the lessons learned from the audits, including insights into the cybersecurity and CIP compliance issues encountered by the audited entities. By publishing publicly these lessons learned we hope to help other utilities improve their compliance with the CIP reliability standards, as well as their overall cybersecurity. These lessons include:

- Making sure that a utility's security processes are well-documented and followed;
- Ensuring that cyber systems connected to generators and shared facilities are included in their risk assessments;
- Ensuring that contractors employ appropriate practices for vetting staff;
- Clearly mapping physical and electronic access rights to control rooms and electronic access systems;
- Ensuring that cybersecurity events are completely and accurately logged;
- Implementing procedures to detect and investigate unauthorized changes to cyber systems; and

- Replacing or upgrading "End-of-Life" system components, which can pose significant vulnerabilities.

FERC Works with Agencies and Utilities to Keep Abreast of Threats and Promote Best Practices

Ensuring security of the grid requires more than CIP standards compliance, especially in such a dynamic area as cybersecurity. Implementing effective cybersecurity requires a well thought-out, documented, and disciplined cybersecurity program that aligns with the mission of the organization. This means putting structure around how organizations align IT (and cybersecurity) strategy with business strategy, ensuring that they stay on track to achieve their strategies and goals, and implementing repeatable measures for their cybersecurity performance. Therefore, the Commission has adopted a two-prong approach to address threats to energy infrastructure: mandatory reliability standards overseen by our Office of Electric Reliability, and voluntary initiatives overseen by our Office of Energy Infrastructure Security (OEIS). OEIS engages with partners in industry, states, and other federal agencies to develop and promote best practices for critical infrastructure security. These initiatives include, among other things, voluntary architecture assessments of interested entities, classified briefings for state and industry officials, and joint security programs with other government agencies and industry.

Because the responsibility for securing critical infrastructure is shared across industry, federal, and state governments, the Commission continues to work collaboratively in this area. For example, on March 28, 2019 the Commission hosted a joint technical conference with the Department of Energy to discuss investments for cyber and physical security with federal, state and industry experts. The conference explored current threats against energy infrastructure, best practices for mitigation, current incentives for investing in physical and cybersecurity protections, and cost recovery practices at the state and federal level.

OEIS works closely with other agencies, including the Department of Energy, the NCCIC, the DHS National Risk Management Center, the Transportation Security Administration, the National Security Council, and others to ensure that the Commission understands evolving cybersecurity threats to FERC-jurisdictional infrastructure and that best practices in ensuring cybersecurity are identified and disseminated.

Conclusion

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 (mandatory) and a collaborative (voluntary) approach to ensuring the reliable and secure operation of the grid. I thank the Committee for the opportunity to participate in this hearing and look forward to answering your questions.

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 multipronged 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 continentwide 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 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:]

Testimony of James B. Robb, President and Chief Executive Officer
North American Electric Reliability Corporation

Before the House Committee on Energy and Commerce
Subcommittee on Energy

"Keeping the Lights On: Addressing Cyber Threats to the Grid"

July 12, 2019

Introduction

Good morning Chair Rush, Ranking Member Upton, members of the Committee and fellow panelists. My name is Jim Robb and I am the President and CEO of the North American Electric Reliability Corporation (NERC). NERC's mission, as the Electric Reliability Organization (ERO) certified by the Federal Energy Regulatory Commission (FERC), is to assure the reliability and security of the bulk power system (BPS) in North America. I have been at NERC for over a year and, prior to NERC, served as the CEO of Western Electricity Coordinating Council, one of six regions in the reliability enterprise. I have more than 30 years of experience working with the electricity industry and am pleased to speak with you today about NERC's responsibilities for grid security.

The threat from cyber attacks by nation states, terrorist groups, and criminals is at an all-time high. Now more than ever, grid security is inextricably linked to reliability. The North American BPS is among the nation's most critical infrastructures. Virtually every critical sector depends on electricity. The BPS is also one of the largest, most complex systems ever created. It is robust and highly reliable. Nevertheless, conventional and non-conventional factors do present risks to the BPS.

Summary

The security landscape is dynamic, requiring constant vigilance and agility. NERC assures grid security through a comprehensive series of complementary strategies involving mandatory standards, reliability guidelines, alerts, information sharing, and partnerships. NERC's mandatory critical infrastructure protection standards (CIP standards) are a foundation for security practices. They provide universal, baseline protections. Due to the ever-evolving nature of cyber threats, security cannot be achieved through standards alone. Vigilance also requires the agility to respond to new and rapidly changing events. Accordingly, NERC's Electricity Information Sharing and Analysis Center (E-ISAC) serves as the information sharing conduit for North America's electricity industry, partnering with cross-sector and international ISACs from electricity and other critical infrastructures, and sharing information between the electricity industry and government for cyber and physical security threats. The E-ISAC facilitates communication of important or actionable information through a secure portal, and strives to determine and maintain "ground truth" during rapidly evolving security events. The E-ISAC also plays a key role in cross-sector coordination, focusing on sectors with which electricity has interdependencies, such as natural gas, water, and other critical infrastructure. Mandatory standards, coupled with effective mechanisms to share information, provide robust and flexible tools to protect the BPS. NERC works closely with the U.S. Department of Energy (DOE), the U.S. Department of Homeland Security (DHS), FERC, and the Electricity Subsector Coordinating Council (ESCC) to further the public-private partnership that is so important to addressing security. NERC's biennial security exercise, GridEx, is the largest of its kind in the sector and enables industry and government to exercise their emergency response plans, and drive new and innovative approaches to reduce security risk to the grid.

About NERC

NERC is a private nonprofit corporation founded in 1968 to develop voluntary operating and planning criteria and standards for the users, owners and operators of the North American BPS. Pursuant to Section 215 of the Federal Power Act (FPA) (16 U.S.C. §824o) and the criteria included in Order No. 672 for designating an ERO, FERC certified NERC as the ERO for the United States on July 20, 2006. On March 16, 2007, FERC issued Order No. 693, which approved the initial set of reliability standards. These reliability standards became mandatory in the United States on June 18, 2007. The first CIP standards were approved by FERC in January 2008 in Order No. 706.

NERC develops and enforces reliability standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; analyzes system performance; and educates, trains, and certifies industry personnel. NERC performs a critical role in real-time situational awareness and information sharing to protect the electricity industry's critical infrastructure against threats to the BPS. NERC's area of responsibility spans the continental United States, Canada, and Mexico. Our jurisdiction includes users, owners, and operators of the BPS, which serves nearly 400 million people. Although we do not have hands on any controls, the work of FERC, NERC, and the Regional Entities strengthens the fabric of the industry.

Critical Infrastructure Protection Standards

With oversight from FERC, NERC is responsible for developing and enforcing mandatory reliability standards for the BPS. The CIP standards provide a common, universal foundation for security. They are robust and comprehensive, covering a wide range of priorities and threats.

More than a decade ago, Congress had the foresight to anticipate the emerging risk posed by cyber security threats to the BPS by defining reliability standards to include "cybersecurity protection." NERC's CIP standards are developed in concert with industry subject matter experts through an open, transparent stakeholder process, subject to approval by NERC's Board of Trustees (Board) and FERC. In addition, FERC can order NERC to develop a standard and has done so on topics such as geomagnetic disturbances, physical security, and supply chain cyber security risk management.

The CIP standards group includes the following 12 topics addressing cyber and physical security:[1]

CIP-002 – Cyber System Identification and Categorization requires entities to identify their cyber systems that perform reliability functions and must be protected under the CIP standards. Using bright-line criteria, this standard also requires entities to categorize these systems as high-, medium-, or low-impact based on the risk to the BPS if the system were compromised. This categorization forms the basis for determining the level of controls applied to those systems under the applicable CIP standards.

CIP-003 – Security Management Controls and Requirements for Lower Risk Cyber Systems requires entities to adopt and maintain cyber security policies to establish responsibility and accountability for protecting critical cyber systems. This standard also identifies the security controls for those systems identified as low impact focusing on: cyber security awareness; physical access controls; electronic access controls; cyber security incident response; and protections for transient electronic devices (e.g., thumb drives, laptop computers).

CIP-004 – Personnel and Training establishes rules for authorizing personnel, including contractors and service vendors, for electronic or unescorted physical access to high- and medium-impact cyber systems. It also establishes rules for ensuring these personnel have the appropriate level of training and security awareness.

CIP-005 – Electronic Security Perimeters establishes rules for managing electronic access to high- and medium-impact cyber systems through use of electronic security perimeters that delineate a "trust zone." This standard also establishes rules for remote access to these cyber systems.

CIP-006 – Physical Security of Cyber Systems establishes rules for managing physical access to high- and medium-impact cyber systems.

CIP-007 – Systems Security Management addresses system security by specifying technical, operational, and procedural requirements in support of protecting high- and medium-impact cyber systems.

CIP-008 – Incident Reporting and Response Planning specifies incident reporting and response requirements.

CIP-009 – Recovery Plans specifies recovery plan requirements to help ensure that reliability functions are recovered following a cyber security incident.

[1] To view NERC CIP standards, see http://www.nerc.com/pa/Stand/Pages/AllReliabilityStandards.aspx?jurisdiction=United%20States.

CIP-010 – Change Management and Vulnerability Assessments specifies system configuration management and vulnerability assessment requirements to help prevent and detect unauthorized changes to high- and medium-impact cyber systems.

CIP-011 – Information Protection establishes rules to prevent unauthorized access to cyber system information by specifying information protection requirements.

CIP-013 – Cyber Security Supply Chain Management will require entities to develop and implement a plan to address supply chain cyber security risks during the planning and procurement of industrial control system hardware, software, and services. This standard was approved by FERC on October 18, 2018, and will become effective on July 1, 2020.

CIP-014 – Physical Security of Critical Transmission Substations and Associated Control Centers that pose the greatest risk to reliability if they are damaged or rendered inoperable due to physical attack. The standard requires entities to determine what facilities are critical, assess the physical security threats to and vulnerability of those critical facilities, and implement a plan to mitigate those threats and vulnerabilities.

As experience and technology continue to grow, NERC, with FERC oversight, continues to refine and improve the CIP standards to ensure their effectiveness and timeliness. For example, pending before FERC is a new CIP standard, CIP-012, that would require enhanced protections of sensitive data transmitted between critical control centers.

In June, FERC issued an order approving Reliability Standard CIP-008-6 - Cyber Security – Incident Reporting and Response Planning, noting that the approved standard enhances the security of the Bulk Electric System (BES). The approved standard expands mandatory reporting requirements to include cyber security incidents that either compromise or attempt to compromise electronic security perimeters and electronic access control or monitoring systems (EACMS) associated with medium- and high-impact BES cyber systems. The revised standard also addresses the information to be included in cyber security incident reports and any subsequent updates. Reports and updates from U.S. entities will be sent to the E-ISAC and DHS's National Cybersecurity and Communications Integration Center. The broadened reporting requirements help to enhance awareness of existing and future cyber security threats or vulnerabilities.

NERC is also currently working with industry experts to consider modifications to the CIP standards to better account for technological innovation. As discussed at FERC's June 27 reliability technical conference, these activities include safeguarding information whether on-site or cloud-stored and the need to look at changes to the standards to address these topics for NERC's registered entities.

Supply Chain Risk

In addition to developing the new cyber security supply chain standard, NERC is addressing supply chain risk in several different ways. In 2018-2019, NERC staff prepared a report on cyber security supply chain risks with recommendations for future actions. NERC worked with the

Electric Power Research Institute to provide an independent assessment of industry supply chain risks and presented a final report to the NERC Board in May 2019. Recognizing the complex and evolving nature of supply chain risks, this report contains several recommendations for additional study including Reliability Standards development work to address EACMS and physical access control systems connected to high- and medium-impact BES cyber systems. In addition, NERC will seek approval from its Board at the August meeting to issue a mandatory data request to gather more information on potential supply-chain threats to cyber security.

Also, NERC is currently developing a Level 2 alert regarding Chinese equipment suppliers, including Huawei and ZTE. The alert is a follow-up to the "all-points bulletin" the E-ISAC issued in March. To provide better analysis of the threat and suggested mitigations, the Level 2 alert and the bulletin enable us to provide strategic warning about the potential risk to industry of compromised supply chains, and to get a better sense of the scope of the threat. With this information, the E-ISAC is able to provide better analysis and suggested mitigation.

Finally, NERC's Critical Infrastructure Protection Committee's (CIPC) Supply Chain Working Group has drafted five security guidelines on different aspects of supply chain security including secure equipment delivery, risk considerations for open source software, lifecycle risk management, provenance, and vendor risk management lifecycle. These guidelines are anticipated to be approved by the CIPC and published in September.

Electricity Information Sharing and Analysis Center

NERC's CIP standards provide a universal foundation for security practices. Yet security cannot be achieved through these standards alone. Because of the emerging and dynamic nature of malicious cyber threats, reliability assurance also requires constant situational awareness, prompt information sharing, and real time communication. The E-ISAC provides these services and supports these industry capabilities.

The mission of the E-ISAC is to reduce cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership, and collaboration. It accomplishes this mission by sharing trusted information and analysis in a timely, credible, and actionable manner with asset owners and operators across the continent.

Operated by NERC, and working in collaboration with DOE and the ESCC, the E-ISAC is the central information sharing hub for the electricity industry. The E-ISAC uses a secure portal as the primary means for communicating with its more than 1,000 electricity industry member organizations, and the number continues to grow. The portal was revamped in 2017 and is constantly undergoing upgrades to enhance the user experience. The new portal functions, plus greater outreach with key industry stakeholder groups through our Industry Engagement Program, has improved bi-directional information sharing and allows members greater access to more information.

In addition to coordination with DOE and FERC's Office of Infrastructure Security, the E-ISAC promotes cross-sector coordination through work with the DHS and other agencies and ISACs.

In particular, to further enhance cross-sector collaboration in light of electric and natural gas interdependencies, the E-ISAC continues to expand its partnership with the Downstream Natural Gas ISAC. In the past year, the E-ISAC added partnerships with other interdependent sectors, including the Oil and Natural Gas ISAC, the Water ISAC, and the Multi-State ISAC. Security is a global priority, and because NERC is an international organization, the E-ISAC works with Natural Resources Canada, Public Safety Canada, and the recently established Canadian Centre for Cyber Security to provide cross-border outreach and collaboration. In October 2018, NERC announced a trilateral memorandum of understanding among the E-ISAC, the Japan Electricity ISAC, and the European Energy ISAC with the intention of expanding sources of information and opportunities for analysis with partners who face similar adversarial threats. As the E-ISAC moves to 24/7 watch operations, these international partnerships will provide valuable context and awareness of emerging threats for overnight analysts to share with North American grid operators.

Cybersecurity Risk Information Sharing Program (CRISP)

Managed by the E-ISAC and in partnership with DOE, CRISP uses innovative technology and leverages DOE and its National Laboratories' analytical capabilities. CRISP provides timely two-way sharing of unclassified and classified threat information and develops situational awareness tools to enhance the electricity industry's ability to identify, prioritize, and coordinate the protection of their critical infrastructure and key resources. CRISP companies cover more than 75% of U.S. customers and participation continues to grow. To address the challenge of reaching smaller utilities, the E-ISAC has worked with DOE on including these entities in the CRISP program. CRISP information is shared in a secure fashion through the E-ISAC portal, and allows non-CRISP member companies to benefit from the shared indicators and threat actor activity captured by the program. CRISP information also supports the development of situational awareness to enhance the industry's ability to identify, prioritize, and coordinate the protection of its critical infrastructure and key resources. In addition to CRISP, the E-ISAC is pursuing cyber automated information sharing systems as well as a malware analysis repository and threat information exchange to provide for more advanced information sharing capabilities.

NERC Alerts, Critical Broadcasts, and Briefings

In addition to the secure portal, the E-ISAC shares information through a number of forums to increase awareness of threats, and to recommend mitigation. When there is a significant security concern, NERC and the E-ISAC communicate with the electricity industry via two distinct platforms.

NERC alerts provide concise, actionable security information to the electricity industry. Security alerts communicate unclassified sensitive information and mitigation measures. Alerts are divided into three levels:

- **Level One – Industry Advisory**: Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary.
- **Level Two – Recommendation to Industry**: Recommends specific action be taken by registered entities. Requires a response from recipients as defined in the alert.

- **Level Three – Essential Action:** Identifies actions deemed to be "essential" to BPS reliability and requires NERC Board of Trustees approval prior to issuance. Like recommendations, essential actions require recipients to respond as defined in the alert.

NERC determines the appropriate alert notification based on risk to the BPS. Generally, NERC distributes alerts broadly to users, owners, and operators of the North American BPS using its compliance registry. Entities registered with NERC are required to provide and maintain updated compliance and cyber security contacts. NERC also distributes the alerts beyond BPS users, owners, and operators to include other electricity industry participants who need the information. Alerts may also be targeted to groups of entities based on their NERC-registered functions (e.g., balancing authorities, transmission operators, generation owners, etc.). Alerts are developed with the strong partnership of federal technical organizations, including FERC, DOE and their National Laboratories, DHS, and BPS subject matter experts. Since 2009, NERC has issued 46 security-related alerts, 41 of which were cyber-related (41 Industry Advisories and five Recommendations to Industry). Those alerts covered items such as sabotage events, pandemic, Aurora, Night Dragon, malware targeting electric assets in Ukraine, and heightened awareness and reporting guidance of suspicious activity. Responses to alerts and mitigation efforts are identified and tracked, with follow-up provided to individual owners and operators and key stakeholders.

In addition to NERC alerts, the E-ISAC uses the Critical Broadcast Program (CBP). This program was launched in 2018 to rapidly share information with members, either through conference calls or "all-points-bulletins". The CBP leverages E-ISAC staff and stakeholder expertise to obtain and share the best available information and potential mitigation strategies to address developing security threats and events in a timely manner. The information is shared through conference calls, the E-ISAC portal and other means, as necessary.

The E-ISAC also hosts regular monthly threat briefings, unclassified threat workshops, classified forums for its clearance-holding members, and allows asset owners and operators to interact with our analysts and each other to share trend analysis and context on common threats to the electricity sector. These activities allow members to discuss emerging threats, learn from security experts, and provide feedback directly to the E-ISAC—which serves to improve E-ISAC's products and services.

Recently, the E-ISAC coordinated closely with the DHS Cybersecurity and Infrastructure Security Agency (CISA) on reported threats to critical infrastructure from Iranian actors in response to geopolitical developments. We produced an all-points bulletin within three hours of the first public reporting of the threat, and followed the next day with a technical indicators bulletin provided by CISA to asset owners and operators.

GridEx

Consistent with our mission to promote a strong learning environment, NERC hosts a grid security exercise every two years – grid security exercise (GridEx) – which simulates widespread, coordinated cyber and physical attacks on critical electric infrastructure designed to overwhelm even the most prepared organizations. GridEx is the largest geographically distributed grid security exercise for the electricity industry. It consists of a two-day distributed play exercise and a separate executive tabletop session. GridEx allows participants to:

- Exercise crisis response and recovery;
- Improve communication;
- Identify lessons learned; and
- Engage senior leadership.

In 2017, 6,500 individuals and 450 organizations participated in GridEx IV, including industry, law enforcement, and federal and state government agencies. The executive tabletop included 42 participants from a cross-section of industry executives and senior officials from federal and state governments. Participating organizations are encouraged to identify their own lessons learned and share them with NERC. NERC uses this input to develop observations and propose recommendations to help the electricity industry enhance the security and reliability of North America's BPS. We are deep into planning for GridEx V, which will take place November 13-14, 2019.

GridSecCon

Consistent with promoting a learning environment and information exchange, NERC hosts the annual Grid Security Conference (GridSecCon). This widely attended conference brings together cyber and physical security experts from industry and government to share emerging security trends, policy advancements, and lessons learned related to the electricity industry. While the specific agenda varies, general objectives include:

- Promoting reliability of the BPS through training and industry education;
- Delivering cutting-edge discussions on security threats, vulnerabilities, and lessons learned from senior industry and government leaders; and
- Informing industry with discussions on security best practices, reliability concerns, risk mitigation, and cyber and physical security threat awareness.

Cybersecurity Trends

These engagements and analytical capabilities have increased the E-ISAC's insight into threats to the grid. This greater insight has translated into more security products for industry, as well as more member-originated information submitted to the E-ISAC and more sharing.

As the E-ISAC looks to the future, we anticipate certain trends:

Credential harvesting: Tactics to acquire legitimate user credentials to gain initial access to targeted networks and establish persistence mechanisms will continue to be popular because it helps evade detection. Sophisticated spear phishing activity to harvest credentials is the most common technique observed by members.

Exploitation of the trust relationship between targeted organizations and their business partners: Recent incidents have demonstrated that nation-state adversaries are targeting the electricity industry and other industries by compromising the networks of third parties with which the intended targets have established business relationships. This tactic is a type of supply chain attack, and increases the success rate of tactics used to initially compromise the intended target.

Network device targeting: From the high profile reports on VPNFilter to the state-sponsored actors targeting network devices, switches and routers located on the edge of networks are a prime target for threat actors capable of intercepting and processing a large amount of information. Because these devices are placed at the boundary between internal networks and the internet, and exist to allow controlled access to the internal network, they will most likely continue to be a target of reconnaissance.

Use of native tools: Adversaries will likely continue to use tools and capabilities already present on a compromised network – such as PowerShell or Windows Management Infrastructure (WMI) – to conduct reconnaissance, lateral movement, and privilege escalation. The presence or use of these tools on a targeted network is unlikely to raise alarm, so their inappropriate use helps evade detection.

Conclusion

Reliability is NERC's mission, and grid security is inextricably linked to reliability. To date, there has not been any loss of load in North America that can be attributed to a cyber attack. At the same time, the security landscape is dynamic, requiring constant vigilance and agility. NERC addresses cyber threats through a comprehensive range of complementary strategies. Our partnership with DOE is critical to the electricity industry's priority for security. Mandatory CIP standards provide a universal foundation for security and is a shared priority with FERC and industry. Through the E-ISAC, NERC provides situational awareness, and sharing of timely, actionable intelligence with industry and government. Strong public private partnerships are key to successful information sharing within the electricity sector and across sectors. NERC remains keenly focused on our mission to assure reliability of the BPS.

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 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 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 continentwide, 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 followup 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 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 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, yes, 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. OK.

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—takes this threat enormously seriously. So 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. WALDEN. 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. WALDEN. 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. WALDEN. So will that give purchasers of the technology in the systems—can you give them an assurance that what they are buying is certified safe——

Ms. EVANS. It is——

Mr. WALDEN [continuing]. 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. WALDEN. Right.

Ms. EVANS [continuing]. 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. WALDEN. Yes. 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 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. WALDEN. 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. WALDEN. Because I know we have some of this equipment in different telecommunication systems today.

Ms. EVANS. Absolutely.

Mr. WALDEN. And it gets very expensive to take it out. And you don't want, you know, buy the next piece of equipment 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 are 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. WALDEN. Thank you, Mr. Chairman. Thank you.

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. OK. 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 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 as 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 cybersecure 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 a 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 freshmen, sophomores 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. Yes. 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. Yes. 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 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. Fifty 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 of requests, FOIA requests, for CEII-related information, including the entities who have violated some of the CIP standards. We reviewed them in excruciating 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 appears at the conclusion of the hearing.]

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 areas 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-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. OK.

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 we as a 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 program 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 had 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 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 in 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 ESEC, 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 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 cochair 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, "OK, 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-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. OK. 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 the $3 million amendment for CESER past 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 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. WALDEN. Mr. Dodge, if I could, has FERC looked at this issue as well?

Mr. DODGE. [Off mic.]

Mr. WALDEN. OK. 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 underway 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. 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. OK. 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. OK. 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?

Ms. EVANS. Oh, OK. 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. Yes. It has been that way since 1999, when I retired. 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. OK.

Mr. Robb, quickly.

Mr. ROBB. Yes. 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. OK. 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 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. OK. 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 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 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.

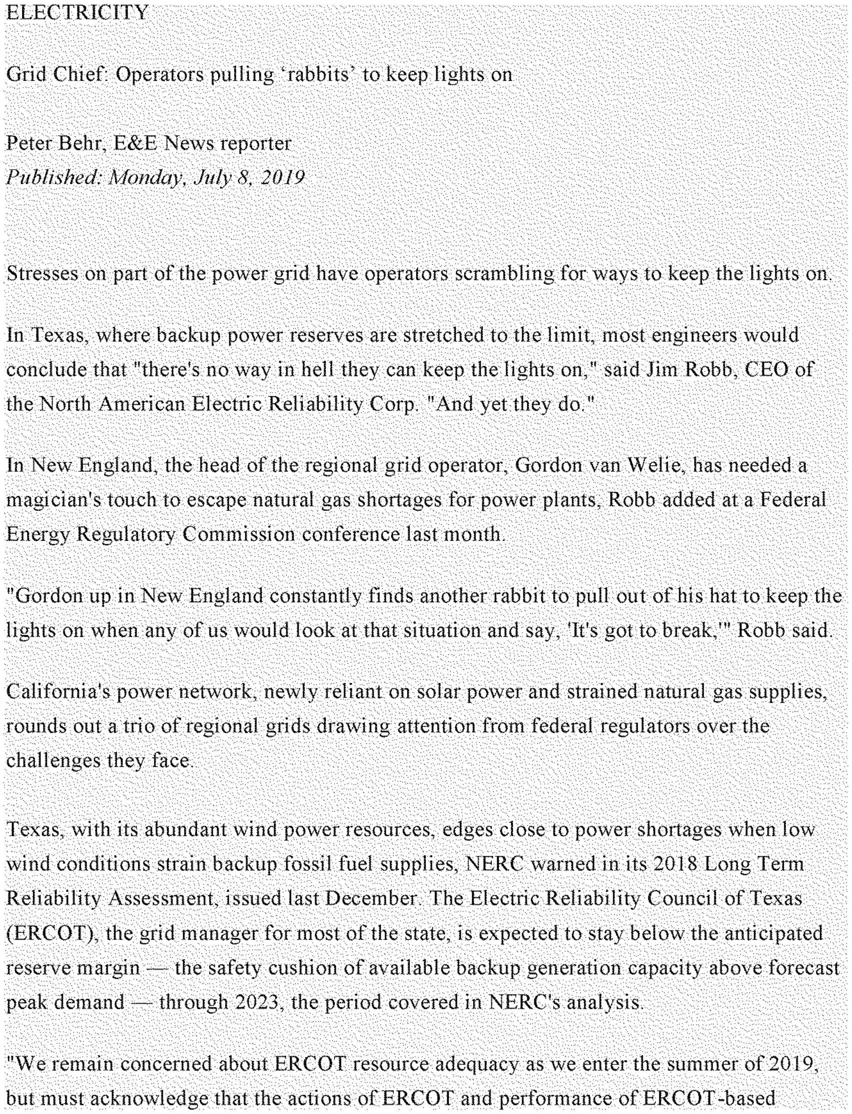
Without objection, so ordered.

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

Mr. RUSH. And the subcommittee now stands adjourned.

[Whereupon, at 11:40 a.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]



ELECTRICITY

Grid Chief: Operators pulling ‘rabbits’ to keep lights on

Peter Behr, E&E News reporter
Published: Monday, July 8, 2019

Stresses on part of the power grid have operators scrambling for ways to keep the lights on.

In Texas, where backup power reserves are stretched to the limit, most engineers would conclude that "there's no way in hell they can keep the lights on," said Jim Robb, CEO of the North American Electric Reliability Corp. "And yet they do."

In New England, the head of the regional grid operator, Gordon van Welie, has needed a magician's touch to escape natural gas shortages for power plants, Robb added at a Federal Energy Regulatory Commission conference last month.

"Gordon up in New England constantly finds another rabbit to pull out of his hat to keep the lights on when any of us would look at that situation and say, 'It's got to break,'" Robb said.

California's power network, newly reliant on solar power and strained natural gas supplies, rounds out a trio of regional grids drawing attention from federal regulators over the challenges they face.

Texas, with its abundant wind power resources, edges close to power shortages when low wind conditions strain backup fossil fuel supplies, NERC warned in its 2018 Long Term Reliability Assessment, issued last December. The Electric Reliability Council of Texas (ERCOT), the grid manager for most of the state, is expected to stay below the anticipated reserve margin — the safety cushion of available backup generation capacity above forecast peak demand — through 2023, the period covered in NERC's analysis.

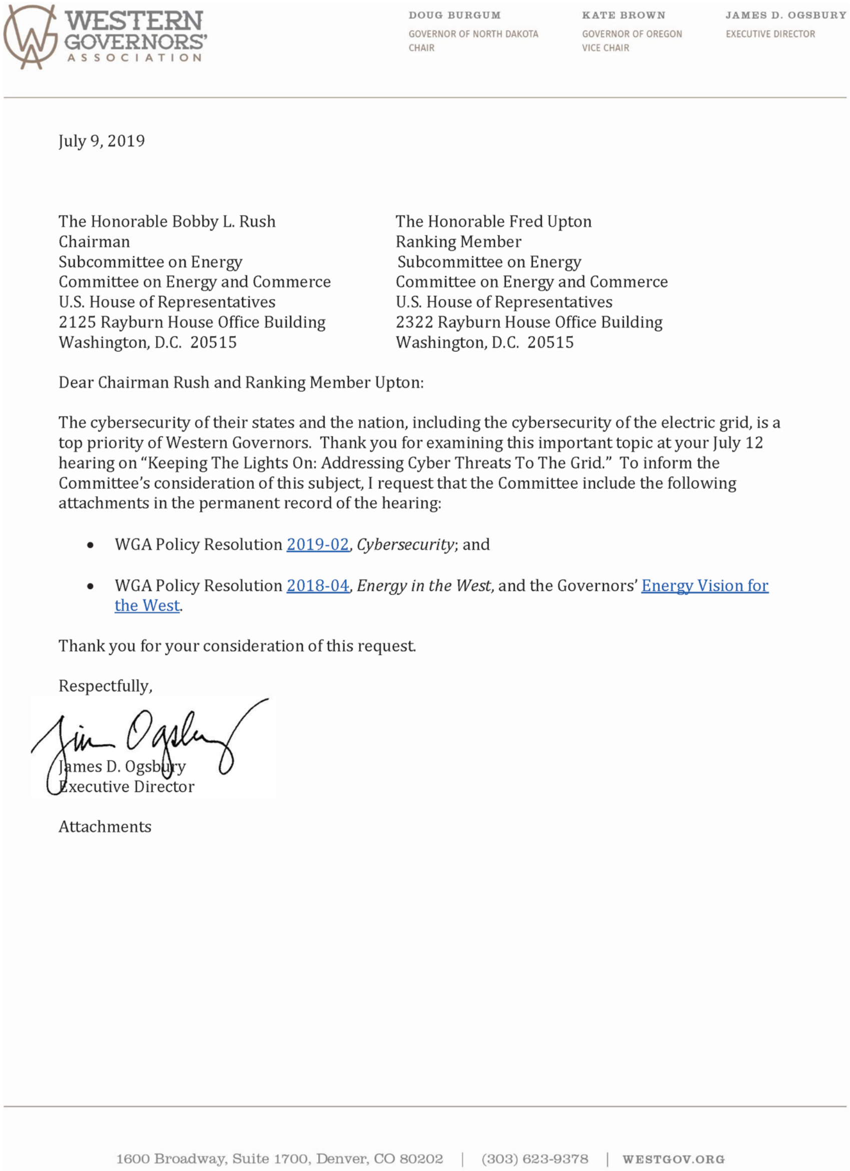
"We remain concerned about ERCOT resource adequacy as we enter the summer of 2019, but must acknowledge that the actions of ERCOT and performance of ERCOT-based generation in the past would indicate they have the tools needed to navigate this upcoming season," Robb and Lauby said in prepared testimony for the June 27 meeting.

ERCOT has called for a 13.75% reserve margin. But the figure this summer is estimated to drop below 9%, primarily due to retirements of over 4,000 megawatts of coal and natural generation over the past two years and delays in bringing new plants online, according to NERC, whose favored safety margin is 15%.
Supporters of a goal of achieving 100% renewable power supplies — without fallback support from gas or nuclear power — put faith in the widespread installation of battery power units to fill in behind renewable energy.

In California's shortage scenarios, the cost would be huge, according to the Wood Mackenzie analysts.

While battery storage could help meet load during sundown, a pipeline rupture in the U.S. Southwest would require investments "of a tremendous scale" to offset, they concluded.

"Nearly 15,000 megawatts of 4-hour battery storage, likely requiring capital investments on the scale of $12 to $18 billion, would be needed," the Wood Mackenzie consultants said.



WESTERN GOVERNORS' ASSOCIATION

DOUG BURGUM
GOVERNOR OF NORTH DAKOTA
CHAIR

KATE BROWN
GOVERNOR OF OREGON
VICE CHAIR

JAMES D. OGSBURY
EXECUTIVE DIRECTOR

July 9, 2019

The Honorable Bobby L. Rush
Chairman
Subcommittee on Energy
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Fred Upton
Ranking Member
Subcommittee on Energy
Committee on Energy and Commerce
U.S. House of Representatives
2322 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Rush and Ranking Member Upton:

The cybersecurity of their states and the nation, including the cybersecurity of the electric grid, is a top priority of Western Governors. Thank you for examining this important topic at your July 12 hearing on “Keeping The Lights On: Addressing Cyber Threats To The Grid.” To inform the Committee’s consideration of this subject, I request that the Committee include the following attachments in the permanent record of the hearing:

- WGA Policy Resolution 2019-02, *Cybersecurity*; and

- WGA Policy Resolution 2018-04, *Energy in the West*, and the Governors’ Energy Vision for the West.

Thank you for your consideration of this request.

Respectfully,

Jim Ogsbury

James D. Ogsbury
Executive Director

Attachments

WESTERN GOVERNORS' ASSOCIATION

Policy Resolution 2019-02

Cybersecurity

A. BACKGROUND

1. In the age of automation, digitization, big data, artificial intelligence, and machine-to-machine learning, the United States' capabilities to prevent, detect and respond to cyberattacks are of ever-growing importance to our society. The cybersecurity of our nation is an all-of-government and industry-wide endeavor.

2. Cybersecurity is especially imperative for critical infrastructure, which includes the nation's electric grid, energy resource supply and delivery chains, finance, communications, election systems, the chemical industry, commercial facilities, critical manufacturing, defense industrial base, emergency services, food and agriculture, government facilities, healthcare and public health, information technology, transportation, and water and wastewater systems.

3. Addressing cybersecurity needs across critical infrastructure sectors is further complicated by the increasing interdependency and interconnectedness of our nation's data systems to myriad of non-critical infrastructure systems and a dynamic threat environment. Effective cybersecurity programs require strategic and functional relationships and information-sharing between federal, state and local levels of government, and the public and private sectors.

4. The cybersecurity of their states and the nation is a high priority of Western Governors. State governments are responsible for securing public networks, the state's digital assets, and citizen data, as well as coordinating their cybersecurity efforts with federal agencies and potentially-affected private entities (e.g., utilities, financial institutions, transportation, and health). Governors lead efforts to plan and implement state cybersecurity programs, respond to cyberattacks, and investigate intrusions.

5. State election systems remain targets of foreign interference. As Governors, we remain committed to protecting our states' election systems. There is nothing more fundamental to the enduring success of our American democracy, and we take seriously our responsibility to protect the integrity and security of our elections. This is an imminent national security threat that transcends party lines. This is a matter of protecting and preserving fair elections – the underpinning of our democracy.

6. The Office of Management and Budget and Department of Homeland Security (DHS) May 2018 Federal Cybersecurity Risk Determination Report and Action Plan concluded that 71 of 96 federal agencies are at risk or high risk of cyber intrusions. It also determined that federal agencies are not equipped to determine how threat actors seek to gain access to their information. This deficiency results in ineffective allocations of the agencies' limited cyber resources.

7. Currently, there is a severe deficit of cyber workers, especially in government. Our nation cannot defend itself without a well-trained, experienced cyber workforce. The public sector

must dedicate resources to cybersecurity education, training, and recruitment programs and encourage the private sector to do the same through effective policy.

B. GOVERNORS' POLICY STATEMENT

1. Western Governors urge Congress to improve coordination of congressional oversight and legislative activity on cybersecurity. The federal government has a responsibility to provide adequate funding for states to meet election security needs. Western Governors encourage Congress and the Administration to work cooperatively with states in developing election security legislation and mandates, and to fully fund implementation.

2. Federal agencies must engage in early, meaningful, substantive, and ongoing consultation with Governors or their designees on all aspects of cybersecurity. The federal government must also continue to clarify the roles and responsibilities of federal agencies in preventing, preparing for, and responding to cyberattacks. Centralized authority, points of contact, and formalized communication pathways are necessary to address increasingly complex threats. In addition, these pathways must occur at each level within government and other organizations.

3. The increasing number and inconsistency of federal security regulations puts an unnecessary burden on state governments and is an inefficient use of often-constrained security resources. The federal government should establish a working group with representatives from states and federal agencies, as well as restore the position of the White House cybersecurity coordinator, to harmonize disparate agency regulations.

4. Western Governors recommend that the federal government continue the DHS State, Local, Tribal, and Territorial Engagement Program, which provides cybersecurity risk briefings and resources to Governors and other officials. The Governors also support DHS's Office of Cybersecurity and Communications, with which state chief information officers regularly interact.

5. The National Institute for Standards and Technology (NIST) Cybersecurity Framework and other standards can facilitate effective, consistent, and risk-based decision-making in government and industry. Real-world simulations of attacks on critical infrastructure are essential to prepare our nation for potential threats.

6. The federal government should use the full range of economic tools, including travel and financial sanctions, to deter cyberattacks organized or supported by nation-states.

7. The public and private sectors must take steps to mitigate global supply chain risks (e.g. installation of malicious software or hardware). Government and industry should also increase the cybersecurity awareness of government and private employees through training and education.

8. The Administration should propose, and Congress should provide, long-term authorization and sufficient appropriations for high-quality cybersecurity education and workforce development programs to grow and sustain the cybersecurity workforce. The federal government should also expand the CyberCorp: Scholarship for Service program and continue to support educational initiatives, such as NIST's Initiative for Cybersecurity Education and National Centers of Academic Excellence in Cyber Defense.

9. Western Governors support policies that incentivize the private sector to improve cybersecurity and share information regarding cyber threats as early as possible, including policies to improve access to information or create common standards for information-sharing. The federal government should emphasize the benefits of information-sharing, while alleviating private sector concerns with this essential communication. The federal government and states should continue to investigate liability protections, such as safe harbor provisions, for entities that report cyber intrusions.

10. Our nation requires innovation in detecting, preventing, and responding to continually-evolving cyber threats. More research is required to understand the use of blockchain and encryption by perpetrators and its utility for defense against cyber threats, and address vulnerabilities of other emerging technologies, including connected vehicles and Internet of Things devices. The federal government should provide funding and technical assistance for these and other types of cybersecurity research and development.

C. GOVERNORS' MANAGEMENT DIRECTIVE

1. The Governors direct WGA staff to work with congressional committees of jurisdiction, the Executive Branch, and other entities, where appropriate, to achieve the objectives of this resolution.

2. Furthermore, the Governors direct WGA staff to consult with the Staff Advisory Council regarding its efforts to realize the objectives of this resolution and to keep the Governors apprised of its progress in this regard.

Western Governors enact new policy resolutions and amend existing resolutions on a bi-annual basis. Please consult westgov.org/resolutions for the most current copy of a resolution and a list of all current WGA policy resolutions.

Western Governors' Association
Policy Resolution 2018-04

Energy in the West

A. <u>BACKGROUND</u>

1. Energy policy and the development of sustainable energy resources are major priorities for every Western Governor.

2. Western Governors recognize that approaches to energy use and development vary among our states, territories, and flag islands. However, the Governors remain committed to the development of policies and utilization of state energy endowments that result in the maximum benefit for their citizens, the region, and the nation.

3. Western energy production is indispensable to meeting national energy demands. The West is the energy breadbasket of the United States:

   a. Western states have all high-yield geothermal energy capacity in the continental United States.

   b. Western states supply the majority of non-federal United States petroleum.

   c. Western states are at the forefront of unconventional natural gas production.

   d. The Pacific Northwest produces the largest output of hydropower in the nation.

   e. Western states have the largest contiguous areas of wind power resources in the nation.

   f. The Southwest has some of the highest-identified solar energy resource areas in the United States.

   g. Western states produce the largest portion of coal in the United States, which is the fuel that constitutes the largest share of the national electricity generation mix.

   h. The West has the largest contiguous areas of high-yield biomass energy resource potential in the nation.

   i. Western states have nuclear power generation facilities and produce all domestic uranium.

4. Western states, Pacific territories, and flag islands have the resources to drive job creation and economic development through broad growth in the energy industry.

5. The Merchant Marine Act of 1920 has prevented certain noncontiguous states, territories, and flag islands from being supplied with domestically produced energy commodities.

B. GOVERNORS' POLICY STATEMENT

1. Western Governors recognize the following as energy policy priorities for the West:

   a. Secure the United States' energy supply and systems, and safeguard against risks to cybersecurity and physical security.

   b. Ensure energy is clean, affordable, and reliable by providing a balanced portfolio of renewable, non-traditional, and traditional resources.

   c. Increase energy efficiency associated with electricity, natural gas, and other energy sources and uses to enhance energy affordability and to effectively meet environmental goals.

   d. Advance efficient environmental review, siting, and permitting processes that facilitate energy development and the improvement and construction of necessary electric grid (transmission and distribution) and pipeline infrastructure, while ensuring environmental and natural resource protection.

   e. Improve the United States' electric grid's reliability and resiliency.

   f. Protect western wildlife, natural resources, and the environment, including clean air and clean water, and strive to reduce greenhouse gas emissions.

   g. Make the West a leader in energy education, technology development, research, and innovation.

   h. Utilize an all-of-the-above approach to energy development and use in the West, while protecting the environment, wildlife, and natural resources.

2. Western Governors support increasing the development and use of energy storage, alternative transportation fuels, and alternative vehicles.

3. Western Governors call on the federal government to lift a barrier to domestic free trade between the contiguous United States and the noncontiguous states, territories and U.S. flag islands by the Merchant Marine Act of 1920 by allowing those jurisdictions to receive energy commodities produced in the mainland but transported by foreign vessels, should those jurisdictions, and the jurisdictions whose ports are being used to ship these materials, desire it.

4. Redundant federal regulation of energy development, transport, and use is not required where sufficient state, territorial, or flag island regulations exist. Existing state authority should not be replaced or impeded by Congress or federal agencies.

C. GOVERNORS' MANAGEMENT DIRECTIVE

1. The Governors direct WGA staff to work with Congressional committees of jurisdiction, the Executive Branch, and other entities, where appropriate, to achieve the objectives of this resolution.

2. The Governors also direct WGA staff to consult with the Western Interstate Energy Board to recommend updates to the 10-Year Energy Vision that provide detail on the Governors' energy policy objectives outlined in this resolution.

3. Furthermore, the Governors direct WGA staff to consult with the Staff Advisory Council regarding its efforts to realize the objectives of this resolution and to keep the Governors apprised of its progress in this regard.

Western Governors enact new policy resolutions and amend existing resolutions on a biannual basis. Please consult www.westgov.org/policies for the most current copy of a resolution and a list of all current WGA policy resolutions.

WESTERN GOVERNORS' ASSOCIATION

Energy Vision for the West

Introduction

The resource-rich West supplies a majority of the country's energy resources and electric power. The United States is currently projected to become a net energy exporter within five years. The increase in natural gas developed in the West, coupled with increased investment in renewable and alternative energy sources, have positioned the region and its Governors to play a central role in the nation's economy and energy policy.

The West's vast energy resources and the Governors' role in the development of energy policy underscores the value of a regional energy policy, the *Energy Vision for the West.* This policy does not impede states or territories from approaching energy choice and industry growth based on their own resource endowments and policies. It illustrates that Western Governors have coalesced around common issues and specific goals, despite diverse geography, resources, and politics. The *Energy Vision for the West* elaborates on the Governors' objectives set forth in WGA Policy Resolution 2018-04, *Energy in the West.*

Western Governors support a comprehensive energy portfolio for the West to ensure that energy is clean, affordable, and reliable. They are also committed to energy policies that promote economic growth and protect the environment. This approach facilitates a strong economy and jobs across a variety of professions, skill sets, and educations.

This approach also recognizes that there are challenges and opportunities associated with every type of energy resource and use, the costs and benefits of which must be considered in policymaking. One such opportunity – and challenge – is creating an effective state-federal partnership in energy development, lands management, and environmental protection. This regional policy is a guide for realizing opportunities to advance the West as the nation's principal energy provider and a leader in energy innovation and effective policy.

Goal 1: Secure the United States' energy supply and systems, and safeguard against risks to cybersecurity and physical security.

Addressing threats to the nation's energy systems and resources is a high priority of Western Governors. Coordination between states, the federal government, and the private sector on energy emergency planning and response is vital to addressing physical and cybersecurity impacts on the West's energy systems and resources. To this end, the Governors establish the following objectives:

- Work with the Department of Defense to meet its national security mission by ensuring safe and secure onsite and off-site electricity generation for key defense installations.

- Continue to reduce reliance on non-North American oil imports from unstable foreign sources through individualized state-by-state solutions, such as increasing North American production, improving fuel efficiency, and developing renewable and alternative fuels.

- Ensure there is sufficient domestic energy supply, including domestic renewable electric generation, to meet existing and new market demand.

- Identify security and other vulnerabilities of energy infrastructure and create programs and standards to defend infrastructure from cyber and physical attacks, as well as natural disasters.

- Encourage effective relationships between state agencies, federal agencies, public utilities, and the private sector to prevent and prepare for risks to the region's energy supply and systems, as well as to respond to and recover from disruptions.

- Partner with the federal government to ensure the provision of adequate funding and access to resources for state emergency planning, response, and recovery.

- Expand, upgrade, and secure transmission and pipeline infrastructure, as well as ensure that all federal pipeline safety measures are efficiently implemented.

Goal 2: Ensure energy is clean, affordable and reliable by providing a balanced portfolio of renewable, non-traditional and traditional resources.

Western Governors believe that a balanced energy portfolio should consist of energy sources that are clean, affordable and reliable, that maintain system reliability, and limit rapid rate increases. These resources also require the maintenance and expansion of transmission and distribution infrastructure. To this end, the Governors establish the following objectives:

- Recognize the importance of western renewable (wind, solar, biomass, biofuels, geothermal, hydropower), nuclear, coal and natural gas resources, and the generation facilities that utilize those resources.

- Adapt utility regulation to changing markets, technologies, and resources.

- Encourage the addition of renewable, low-carbon, and clean generation, including utility-scale and distributed generation.

- Promote, advance and fund the evolution of new technologies, including carbon capture and advancements in renewable energy.

- Maintain the Rural Energy for America (REAP) program, which has benefited farmers, ranchers and rural businesses that are often underserved by other federal energy efforts.

Goal 3: Increase energy efficiency associated with electricity, natural gas, and other energy sources and use to enhance energy affordability and to effectively meet environmental goals.

Eliminating waste and using resources wisely are cornerstones of a sound energy strategy. State and local governments, utilities, households, and businesses are currently realizing the economic and other benefits of energy efficiency, but there are still substantial gains to be made. To this end, the Governors establish the following objectives:

- Prioritize energy efficiency associated with electricity, natural gas, and vehicle transportation.

- Enhance utility rate designs, including time-varying rates, and cost-effective utility energy efficiency programs that deliver electricity and natural gas savings to consumers.

- Support energy efficiency programs that provide incentives and rebates to lower the incremental up-front costs of energy efficiency technologies; Energy Service Company (ESCO) programs; and where successful, utility ratepayer-funded energy efficiency programs, including the use of rate decoupling.

- Encourage the retrofit of residential and commercial buildings and improve the energy efficiency of new buildings, such as through building energy codes and programs that stimulate energy efficient construction.

- Decrease energy intensity using tools such as combined heat and power and waste heat to power systems.

- Incorporate systems strategies to improve efficiency throughout the building lifecycle and to improve grid connectivity, including energy systems that enable two-way, automated utility-to-customer communications to facilitate demand response programs.

- Maintain funding and support long-term authorization for the State Energy Program (SEP), Weatherization Assistance Program (WAP), and Low-Income Home Energy Assistance Program (LIHEAP).

Goal 4: Advance efficient environmental review, siting and permitting processes that facilitate energy development and the improvement and construction of necessary electric grid (transmission and distribution) and pipeline infrastructure, while ensuring environmental and natural resource protection.

Responsible energy development and a robust, well maintained energy delivery system are vital to the economy and quality of life in the West. To this end, the Governors establish the following objectives:

- Encourage responsible leasing and development of energy resources and infrastructure.

- Create a clear and transparent process for regulation and permitting, coordinated among well-trained and adequately funded federal, state and local agencies.

- Streamline project-permitting reviews to minimize timelines, without compromising environmental and natural resource protection or states' roles in those processes.

- Maintain state and local decision-making authority over transmission line siting and permitting.

- Encourage regional transmission planning organizations to conduct interconnection-wide planning with the full participation of the states and with consideration of state energy policies.

- Create functional partnerships among states, federal agencies, tribal governments and local jurisdictions to solve conflicts that hinder energy infrastructure and resource development.

- Increase cooperation on interstate projects through interstate compacts and other tools.

- In the West-wide energy corridor process, ask federal agencies to guarantee: ongoing, substantive, and meaningful state consultation; consideration of state plans, processes, priorities, and policies; and integration of other streamlining efforts.

Goal 5: Improve the United States electric grid's reliability and resiliency.

Changes in energy generation, distribution, and management are transforming the nation's electric grid. But these advancements also highlight the need for grid level investment, along with associated updates for electricity regulation and policy. To this end, the Governors establish the following objectives:

- Protect state authority to determine the type and amount of new generation facilities and the programs used to procure new generation, recognizing that each state has their own priorities and portfolios.

- Protect state authority to encourage continued operation of existing generation facilities through long-term contracts, retail utility contracting, or other incentives.

- Encourage regional reliability organizations, utilities, state agencies and public utility commissions to assess the provision of essential reliability services under future scenarios that include a changing resource mix in the West.

- Support grid operator situational awareness of distributed energy resources by promoting coordination between utilities and distributed energy resource developers.

- Preserve areas of exclusive state authority regarding distributed energy resources, including storage, and improve utility distribution systems planning for distributed energy resources to enhance grid reliability and resilience.

- Improve understanding of grid resources and services and the need for new power production facilities and transmission/distribution infrastructure through data, analysis, and coordination.

- Prepare for potential disruptions to the grid from wildfires, flooding, earthquakes, tornadoes, cyberattacks and other disturbances and emergencies, as well as increase the grid's ability to withstand and reduce the magnitude of such events.

- Enable utilities to take necessary actions to enhance grid reliability and reduce the threat of wildfires to and from electric transmission and distribution rights-of-way.

Goal 6: Protect western wildlife, natural resources and the environment, including clean air and clean water, and strive to reduce greenhouse gas emissions.

Western states have long assumed a stewardship role for the natural environment and have worked across state lines to protect air, land, wildlife and water. Western Governors are committed to ensuring that energy development is done in an environmentally responsible manner. To this end, the Governors establish the following objectives:

- Promote energy technologies and sources that lower emissions.
- Continue advancing air and water quality improvements and plans in each state and across state lines.
- Foster environmental cooperation that: protects the state-federal partnership; provides for sustainable environmental protection; is nimble and flexible; and ensures that state governments play a key role in regulation.
- Acknowledge that a productive economy and responsible development can support environmental protection by providing additional funding and opportunities for public-private partnership.
- Encourage technologies that reduce water consumption, prioritize water consumption for traditional activities (drinking water, agriculture, habitat conservation/restoration), and contribute to the responsible development of new energy resources.
- Achieve a balance between the responsible development of energy projects and wildlife conservation.
- Urge the federal government to identify and approve solutions for the long-term storage and permanent disposal of spent nuclear fuel and nuclear waste.
- Encourage the development and deployment of a full range of technologies that offer the potential for cost-effective reductions in greenhouse gas emissions from energy production and use, including carbon capture and storage, energy efficiency, zero emissions generation sources, and other emerging options.

Goal 7: Make the West a leader in energy education, technology development, research, and innovation.

Effective energy policy is facilitated by an understanding of a common set of impartial facts and scientific evidence. Furthermore, the advancement of technology will play a critical role in realizing a clean energy future. To this end, the Governors establish the following objectives:

- Leverage the vast expertise in the West's industry, academic institutions, and national laboratories to make the region an international hub for new energy technology research and development, as well as energy education.
- Encourage Congress and the Department of Energy to support and fund research, development, demonstration, and deployment of advanced energy technologies.
- Create public-private research and development partnerships among industry, academia, the national labs, and federal agencies to identify promising new technologies, including energy efficiency technologies that advance clean energy with reduced environmental impacts.
- Encourage market operators, reliability organizations, and utilities to appropriately share electric system operational data with researchers, educators, and entrepreneurs to promote

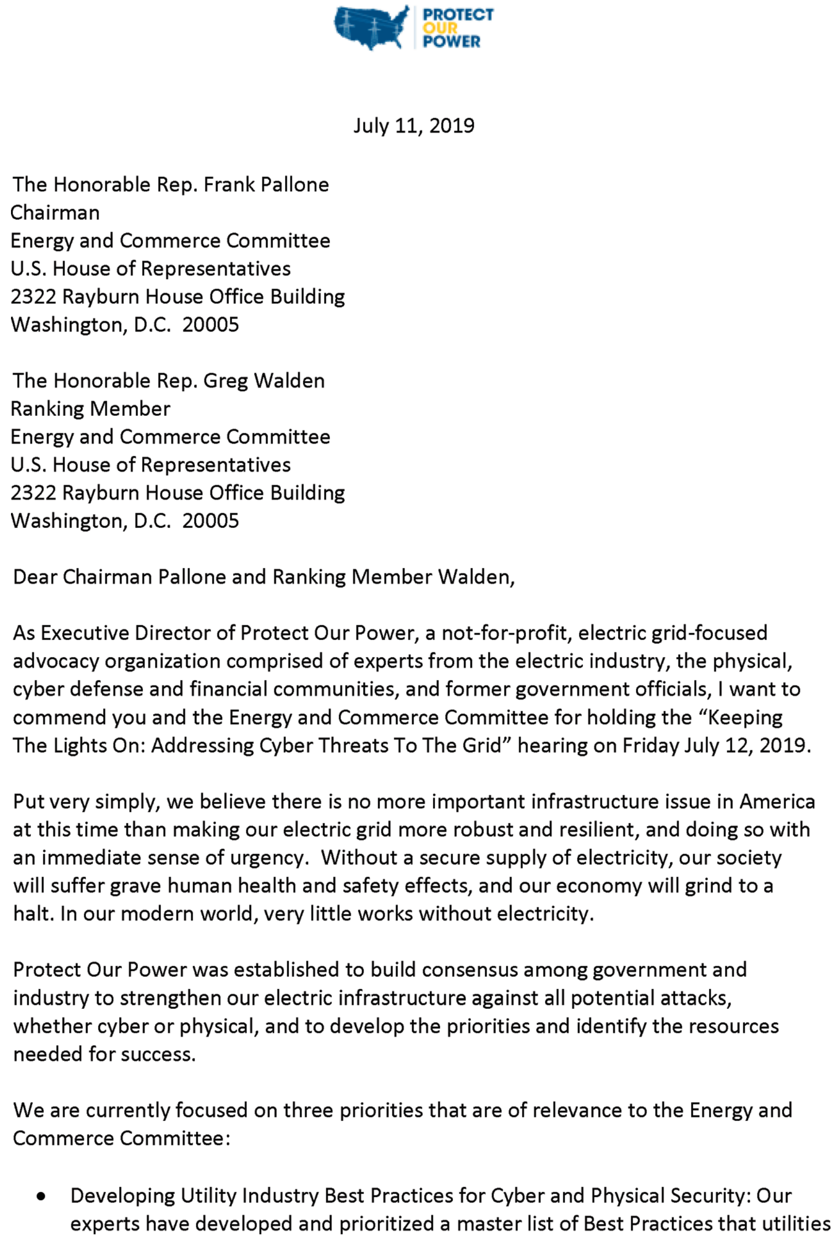
electric system innovation and technology development, while still safeguarding against risks to cybersecurity and physical security.

- Encourage training and education in energy-related fields and ensure there is an adequate workforce operating under the highest safety standards.
- Facilitate the creation of employment opportunities for displaced energy sector workers.
- Educate the public regarding: the role of energy in maintaining a high standard of living and quality of life; trade-offs and externalities associated with all types of energy development and consumption; the coexistence of a healthy environment and a thriving economy; and how federal policy on public lands impacts energy and infrastructure development.

Goal 8: Utilize an all-of-the-above approach to energy development and use in the West, while protecting the environment, wildlife and natural resources.

A diverse energy portfolio is essential to the provision of clean, affordable, secure, and reliable energy. Western Governors support a comprehensive energy portfolio, including: oil, gas, coal, nuclear, biomass, geothermal, hydropower, solar, wind, and conservation and energy efficiency. To this end, the Governors establish the following objectives:

- Reduce costs and risks for the environmentally sound development of all energy resources.
- Ensure competition in the market for all resources.
- Recognize the growing importance of consumer choice in driving energy policy.
- Support consumer choice of distributed energy resources to achieve affordability, environmental, and other objectives.
- Increase the development and use of alternative transportation fuels and vehicles, including the necessary infrastructure for those vehicles.
- Encourage innovation and application of energy storage, including pumped hydro storage, battery storage, and compressed air energy storage where cost-effective.
- Support the responsible and efficient development and use of traditional and renewable resources.
- Increase the amount of electricity generated from new, retrofitted, or relicensed hydroelectric facilities, including small, irrigation, and flood control hydropower projects.
- Restore financing for the geothermal exploration program financed by the Department of Energy.
- Accelerate the introduction of small modular reactors into the marketplace.



PROTECT
OUR
POWER

July 11, 2019

The Honorable Rep. Frank Pallone
Chairman
Energy and Commerce Committee
U.S. House of Representatives
2322 Rayburn House Office Building
Washington, D.C. 20005

The Honorable Rep. Greg Walden
Ranking Member
Energy and Commerce Committee
U.S. House of Representatives
2322 Rayburn House Office Building
Washington, D.C. 20005

Dear Chairman Pallone and Ranking Member Walden,

As Executive Director of Protect Our Power, a not-for-profit, electric grid-focused advocacy organization comprised of experts from the electric industry, the physical, cyber defense and financial communities, and former government officials, I want to commend you and the Energy and Commerce Committee for holding the "Keeping The Lights On: Addressing Cyber Threats To The Grid" hearing on Friday July 12, 2019.

Put very simply, we believe there is no more important infrastructure issue in America at this time than making our electric grid more robust and resilient, and doing so with an immediate sense of urgency. Without a secure supply of electricity, our society will suffer grave human health and safety effects, and our economy will grind to a halt. In our modern world, very little works without electricity.

Protect Our Power was established to build consensus among government and industry to strengthen our electric infrastructure against all potential attacks, whether cyber or physical, and to develop the priorities and identify the resources needed for success.

We are currently focused on three priorities that are of relevance to the Energy and Commerce Committee:

- Developing Utility Industry Best Practices for Cyber and Physical Security: Our experts have developed and prioritized a master list of Best Practices that utilities large and small should adopt, and we are continuing efforts to identify and categorize qualified vendors who can provide related services and products to the utility industry to help implement Best Practices and strengthen the grid.

- Completing Phase 2 of a study on state regulation of utilities, focused on developing recommendations for regulatory improvements and uniformity, including model regulations and legislation. The study was commissioned by Protect Our Power and is being conducted by the Institute for Energy and the Environment at Vermont Law School.
- Commissioning an in-depth analysis on vulnerabilities in the utility industry supply chain, to be conducted by Ridge Global, one of the nation's top security consulting firms headed by former Homeland Security Secretary Tom Ridge.

More broadly, we believe a comprehensive, "moonshot"-style approach is needed to improve and upgrade the grid, one in which we marshal the level of talent, money, focus and determination equal to that which made it possible for us to land on the moon 50 years ago. This moonshot effort must be driven by a well-funded partnership between government and the private sector, and the costs must be borne by all collectively.

We are working to develop an innovative, flexible funding mechanism to incentivize large and small utilities to make necessary investments in cyber security and implement best practices on a sustained basis. We recognize that the impact on electric utility ratepayers will need to be carefully overseen by state regulatory agencies, but we also believe that utilities need to have some reasonable measure of guarantee that effective, prudent expenditures for cyber upgrades will be recouped. We look forward to continuing to share our thinking on this with the Committee in the near future.

In closing, we commend the Energy and Commerce Committee for holding this important hearing and we encourage the Committee to pursue efforts that bring parties in both the public and private sectors together in our shared national interest to protect our nation's electric grid against both physical and cyber threats.

Sincerely,
Jim Cunningham
Executive Director
Protect Our Power

July 12, 2019

The Honorable Bobby Rush,
Chairman
Subcommittee on Energy
U.S. House of Representatives
2188 Rayburn House Office Building
Washington, DC 20515

The Honorable Fred Upton
Ranking Member
Subcommittee on Energy
U.S House of Representatives
2183 Rayburn House Office Building
Washington, DC 20515

Chairman Rush, Ranking Member Upton and Members of the Committee:

Thank you for holding this hearing on the cybersecurity of the United States' power grid. In a world where society is increasingly dependent on electricity to maintain the fabric of daily life, the United States is vulnerable to new methods of attack from hostile actors. A cyberattack that denies service to significant portions of America's population could potentially overwhelm our current ability to respond. Energy companies and electric grid operators must therefore be sufficiently incentivized to install defenses against cyberthreats to the grid, while federal and state government officials must develop better recovery strategies in case a blackout occurs.

My name is Kathryn Waldron, and I am a fellow with the national security and cybersecurity team at the R Street Institute. The R Street Institute is a nonprofit, nonpartisan public policy research organization whose mission is to engage in policy research and outreach to promote free markets and limited, effective government. Our scholars have written extensively on the issues of energy, cybersecurity and the national security implications of today's global supply chain.

The U.S. power grid is the vast network that allows for electricity to be delivered to businesses and individuals across the nation. It includes generators, power stations, transmission lines, distribution lines, and all of the manual and digital systems employed by utility companies. The United States is currently in the process of switching to a smart grid system as different parts of the grid are modernized. (The current grid system was built in the 1890s.) The smart grid would incorporate digital technology that would allow for two-way flows of both electricity and information.[1]

Nations have long recognized the strategic importance of national power grids. For example, countries have frequently targeted a rival's power grid during wartime. The strategy of attacking power grids was discussed frequently in the 1930s by the U.S. Air Corps Tactical School and eventually became the "bedrock upon which the World War II strategic bombing campaigns were first designed."[2] Electrical grids were an appealing target at the time as strategists hoped the loss of electricity would simultaneously reduce production capacity, hinder military ability and dampen civilian morale, eroding support for any war efforts.[3]

The German power grid was a major military target for Allied forces in World War II. While the Allies did not successfully manage to disrupt Germany's access to electricity, power grids continued to be targeted in subsequent military conflicts. In 1952, during the Korean War the United States bombed and destroyed approximately 90 percent of North Korea's power generating infrastructure, leading to a two-week blackout. The U.S. military also attacked the North Vietnamese power grid during the Vietnam War. Destruction of the Iraqi power grid by U.S. forces during the Gulf War lead to devastating civilian casualties, with some reports attributing 70,000 deaths to the blackout.[4]

In today's world, the most pressing threats to the power grid come from malicious cyber actions rather than strategic bombing campaigns. In December 2015, malicious cyber activities against three energy companies in Ukraine left approximately 225,000 people without power for several hours. Spear-phishing emails facilitated intrusions into the computer and supervisory control and data acquisition (SCADA) systems that controlled the Ukrainian systems, allowing intruders to seize control. The intrusion, which occurred as part of the ongoing conflict between Russia and Ukraine, is generally attributed to the Russian group Sandworm.[5] Ukraine's power grid was hacked again the following year, resulting in part of Kiev going without power for

[1] Office of Electricity Delivery and Energy Reliability, "What is the Smart Grid?" U.S. Department of Energy, accessed July 9, 2019. https://www.smartgrid.gov/the_smart_grid/smart_grid.html.

[2] Thomas E. Griffith Jr., "Strategic Attack of National Electrical Systems," October 1994, p. 15. https://media.defense.gov/2017/Dec/29/2001861964/-1/-1/0/T_GRIFFITH_STRATEGIC_ATTACK.PDF.

[3] ibid.

[4] Ibid, pp. 34-47.

[5] "Analysis of the Cyber Attack on the Ukrainian Power Grid," E-ISAC, March 118, 2016. https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

approximately an hour. While the 2015 intrusion allowed hackers to infiltrate networks in order to manually shut down an electrical substation, the 2016 intrusion was fully automated.[6]

Although the United States has not seen cyber-instigated power outages like the events in Ukraine, segments of the American energy grid have been targeted frequently by malicious cyber actors. In 2003, the safety monitoring system of a nuclear power plant in Ohio was infected by malware known as "Slammer worm." No damage occurred, as the power plant was offline at the time.[7] In 2008, then-CIA analyst Tom Donahue revealed that hackers compromised the computer systems of utility companies in several U.S. cities, attempting to extort money by threatening to cause blackouts.[8] And just this year hackers launched "denial-of-service" cyber activities that disabled the SCADA component of power grid control systems in Utah, Wyoming and California.[9]

The U.S. Department of Homeland Security (DHS) has reportedly been warning electrical utility executives about Russian threats for over five years. In 2018, the Wall Street Journal reported that Russian hackers working for the state-sponsored group Energetic Bear had successfully infiltrated the control rooms of some U.S. electrical utility companies. The hackers accessed supposedly secure, "air-gapped" systems by worming their way in through the utility supply chain. Jonathan Homer, chief of industrial-control-system analysis for DHS, stated about the hackers, "They got to the point where they could have thrown switches."[10]

Yet despite continued reports of Russian probing of the U.S. power grid, Russia has refrained from any sort of cyber activity along the lines of the Ukraine outages. This may be due in part to the threat of mutual retaliation from the United States. Last month *The New York Times* reported that U.S. Cyber Command had successfully infiltrated the Russian power grid. While the United States allegedly has put cyber reconnaissance probes into the control systems of the Russian power grid since 2012, this latest move adds a new level of aggression to America's cyber strategy.[11] President Trump, who was not consulted on Cyber Command's actions

[6] Andy Greenberg, "'Crash Override': The Malware That Took Down A Power Grid*," Wired*, June 12, 2017. https://www.wired.com/story/crash-override-malware/.

[7] Candid Wueest, "Targeted Attacks Against the Energy Sector," Symantec, January 13, 2014. https://bluekarmasecurity.net/wp-content/uploads/2014/09/Symantec_Targeted-Attacks-Against-the-Energy-Sector_whitepaper.pdf.

[8] Ellen Nakashima and Steven Mufson, "Hackers Have Attacked Foreign Utilities, CIA Analyst Says," *The Washington Post,* January 9, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/01/18/AR2008011803277_pf.html.

[9] Blake Sobczak, "Experts assess damage after first cyberattack on U.S. grid," *E&E News*, May 6, 2019. https://www.eenews.net/stories/1060281821.

[10] Rebecca Smith, "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say," *Wall Street Journal*, July 23, 2018. https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110.

[11] David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *The New York Times*, June 15, 2019. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

according to the article, denied American infiltration, tweeting that the article was “NOT TRUE” and calling the New York Times desperate for a story.[12] The U.S. Cyber command is not legally required to inform the president before carrying out cyber activities of this nature. However, the lack of unity among government officials and leaders on this issue makes the United States look weak when it comes to national security and cybersecurity, making the grid a more appealing target for hackers. Therefore, it is all the more important to update the security of the grid.

Smart Grids

The switch to smart grid systems is sometimes touted as adding resiliency to the electric system, since it will increase the flow of information and more easily allow rerouting in the case of limited failures. The U.S. Department of Energy (DOE) has put forth a number of projects and initiatives related to the grid's cybersecurity, including its Cybersecurity for Energy Delivery Systems program and their National SCADA Test Bed, “which provides testing environments to help industry and government identify and correct vulnerabilities in SCADA equipment and control systems.”[13] The DOE has also partnered with the National Institute for Standards and Technology (NIST) to issue “Guidelines for Smart Grid Cybersecurity.” The guidelines provide a framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of smart grid-related characteristics, risks and vulnerabilities.[14]

However, increased reliance on digital systems means more access or disruption points for hackers. This has led some politicians to advocate for mandating the inclusion of "retro" technology in the power grid. Last month the Securing Energy Infrastructure Act (SEIA) passed the Senate. The bill's supporters hope the inclusion of analog and manual technology will isolate critical parts of the grid from cyberattacks, arguing that the power outages in Ukraine “could have been worse if not for the fact that Ukraine relies on manual technology to operate its grid.”[15]

Industry reaction to SEIA has been mixed. While some experts are not opposed to the concept of analog backup systems, others view the SEIA bill as sidestepping the real issue by proposing a solution that hampers development and superior provision of energy. According to James Scott, co-founder and senior fellow at the Institute for Critical Infrastructure Technology,

[12] Staff, “Trump calls NYT report on U.S. intrusions into Russia power grid 'virtual act of treason',” *The Japan Times*, June 17, 2019. https://www.japantimes.co.jp/news/2019/06/17/world/trump-calls-nyt-report-russia-power-grid-intrusions-virtual-act-treason/#.XSUiq-hKg2w.

[13] Office of Electricity Delivery and Energy Reliability, “Cybersecurity,” U.S. Department of Energy, accessed July 10, 2019. https://www.smartgrid.gov/recovery_act/overview/cyber_security.html.

[14] National Institute of Standards and Technology, “Guidelines for Smart Grid Cybersecurity,” U.S. Department of Commerce, September 2014. https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

[15] Angus King, “Senate Passes King Bill Protecting Energy Grid from Cyber-Attacks,” June 28, 2019. https://www.king.senate.gov/newsroom/press-releases/senate-passes-king-bill-protecting-energy-grid-from-cyber-attacks.

"Legislation that eschews modern systems in favor of antiquated technologies is a step in the wrong direction because it amounts to significantly crippling the U.S. energy sector instead of addressing the threats."[16]

Worries about the U.S. grid based on the attacks in Ukraine may be overblown, as the Ukrainian grid is far more unified than its American counterpart. Any discussion of the national security of the power grid would be incomplete without acknowledging its uniquely fragmented nature. The U.S. grid is primarily split into three main parts—the Eastern Interconnection, the Western Interconnection and Texas—and each part has its own web of interconnected investor-owned utility companies. As a result, it would be challenging (although not impossible) for any individual, group or nation to cause a complete shutdown of the entire U.S. grid at one time. The private-sector elements of U.S. energy provision thereby strengthen the grid's protection, especially when compared to a unified national system.

Moving Forward

Determining how best to protect the U.S. power grid is a challenging and complex undertaking. In order to reliably and securely provide electrical power to all Americans, it is critically important that Congress play an active oversight and legislative role to better ensure that the grid can withstand even the most sophisticated cyber intrusion. In the event of a successful intrusion that results in the interruption of electrical service, it is also essential that the operators of the power grid have the capacity to promptly remediate any damage to the system and restore full operability. Below are a few suggestions of ways the United States can strengthen the grid's security.

First, utility companies should be encouraged to carefully vet their own supply chain. Protecting the American power grid is, in part, a matter of supply chain security. Utility companies have their own vendors and suppliers, and these suppliers can carry risks. In the case of Energetic Bear compromising the U.S. power grid discussed above, hackers were able to infiltrate by attacking less secure, yet still trusted vendors.

Second, state governments can also seek to align their security concerns with the incentives of local utility companies. My colleague Travis Kavulla at the R Street Institute has written previously on the need for economic regulation of utility companies to incentivize investment in safety protections against natural disasters like wildfires. This methodology can be applied to cyberthreats as well as natural public-safety risks. In order to align incentives, Kavulla advocates tying regulated utilities' compensation to safety outcomes:

[16] Alex Crees, "Dumbing down the electric grid: the answer to cybersecurity concerns?" *Choose Energy*, accessed July 10, 2019. https://www.chooseenergy.com/news/article/dumbing-electric-grid-answer-cybersecurity-concerns/.

> If safety improvements were obtainable primarily through increased capital spending, it would be reasonable to persist with the status quo, in which a utility's profit is a function of its "used and useful" capital investment. The existing regulatory model, which rewards a utility's equity investment, whether at 10 percent or 17 percent, ensures that. But if safety improvements will result primarily from operational improvements, then the cost-of-service, rate-of-return regulatory model appears misaligned to it. This would seem to be a powerful argument for tying a potentially substantial amount of the corporation's existing or incremental profit opportunity to safety performance.[17]

Cybersecurity inputs can often be difficult to measure and increased spending does not necessarily equal increased security. (Consider, for example, how installing more than one antivirus program often makes a computer system less safe by confusing the programs downloaded.)[18] Tying funding to results instead of merely increasing spending is therefore more likely to send utility companies searching for the right security programs instead of simply adding more security programs.

Third, U.S. government agencies devise strategies to deal with worst-case scenarios in the case of a successful attack on the grid. While progress has been made in this area, there remains more to be done. Last December the president's National Infrastructure Advisory Council (NIAC) released a report concluding "that existing national plans, response resources, and coordination strategies would be outmatched by a catastrophic power outage."[19] One simple recommendation proposed by NIAC is to clarify emergency authority in the case of a "cyber-physical disaster," which the report states is understood at a high level but not at the level of implementation. (The term "cyber-physical disaster" refers to cyber activities cause damage in the physical world.)

I thank the Committee for its recognition of the importance of ensuring the cybersecurity of the power grid. If I or any of my colleagues at the R Street Institute can be of assistance to members of the Committee, please feel free to contact me.

Kathryn Waldron
Fellow, Cybersecurity and National Security
kwaldron@rstreet.org

[17] Opening Statement of Travis Kavulla, California Public Utilities Commission, Forums on Governance, Management, and Safety Culture, April 26, 2019. https://www.rstreet.org/wp-content/uploads/2019/04/Final-edit-Remarks-CPUC-April-2019-PGE.pdf.

[18] "Why Using Multiple Antivirus Programs is a Bad Idea," *Kaspersky Daily*, September 9, 2013. https://www.kaspersky.com/blog/multiple-antivirus-programs-bad-idea/2670/.

[19] The President's National Infrastructure Advisory Council, "Surviving a Catastrophic Power Outage," December 2018. https://www.dhs.gov/sites/default/files/publications/NIAC%20Catastrophic%20Power%20Outage%20Study_508%20FINAL.pdf.