

**THE FUTURE OF ELECTRICITY DELIVERY:
MODERNIZING AND SECURING OUR
NATION'S ELECTRICITY GRID**

HEARING
BEFORE THE
SUBCOMMITTEE ON ENERGY
COMMITTEE ON SCIENCE, SPACE, AND
TECHNOLOGY
HOUSE OF REPRESENTATIVES
ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

July 17, 2019

Serial No. 116-40

Printed for the use of the Committee on Science, Space, and Technology



Available via the World Wide Web: <http://science.house.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

37-037PDF

WASHINGTON : 2019

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. EDDIE BERNICE JOHNSON, Texas, *Chairwoman*

ZOE LOFGREN, California	FRANK D. LUCAS, Oklahoma,
DANIEL LIPINSKI, Illinois	<i>Ranking Member</i>
SUZANNE BONAMICI, Oregon	MO BROOKS, Alabama
AMI BERA, California,	BILL POSEY, Florida
<i>Vice Chair</i>	RANDY WEBER, Texas
CONOR LAMB, Pennsylvania	BRIAN BABIN, Texas
LIZZIE FLETCHER, Texas	ANDY BIGGS, Arizona
HALEY STEVENS, Michigan	ROGER MARSHALL, Kansas
KENDRA HORN, Oklahoma	RALPH NORMAN, South Carolina
MIKIE SHERRILL, New Jersey	MICHAEL CLOUD, Texas
BRAD SHERMAN, California	TROY BALDERSON, Ohio
STEVE COHEN, Tennessee	PETE OLSON, Texas
JERRY McNERNEY, California	ANTHONY GONZALEZ, Ohio
ED PERLMUTTER, Colorado	MICHAEL WALTZ, Florida
PAUL TONKO, New York	JIM BAIRD, Indiana
BILL FOSTER, Illinois	JAIME HERRERA BEUTLER, Washington
DON BEYER, Virginia	JENNIFFER GONZALEZ-COLÓN, Puerto
CHARLIE CRIST, Florida	Rico
SEAN CASTEN, Illinois	VACANCY
KATIE HILL, California	
BEN McADAMS, Utah	
JENNIFER WEXTON, Virginia	

SUBCOMMITTEE ON ENERGY

HON. CONOR LAMB, Pennsylvania, *Chairman*

DANIEL LIPINSKI, Illinois	RANDY WEBER, Texas, <i>Ranking Member</i>
LIZZIE FLETCHER, Texas	ANDY BIGGS, Arizona
HALEY STEVENS, Michigan	RALPH NORMAN, South Carolina
KENDRA HORN, Oklahoma	MICHAEL CLOUD, Texas
JERRY McNERNEY, California	VACANCY
BILL FOSTER, Illinois	
SEAN CASTEN, Illinois	

C O N T E N T S

July 17, 2019

	Page
Hearing Charter	2
Opening Statements	
Statement by Representative Conor Lamb, Chairman, Subcommittee on Energy, Committee on Science, Space, and Technology, U.S. House of Representatives	6
Written Statement	7
Statement by Representative Randy Weber, Ranking Member, Subcommittee on Energy, Committee on Science, Space, and Technology, U.S. House of Representatives	8
Written Statement	9
Written statement by Representative Eddie Bernice Johnson, Chairwoman, Committee on Science, Space, and Technology, U.S. House of Representatives	10
Witnesses:	
The Honorable Karen Evans, Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy	
Oral Statement	12
Written Statement	14
Mr. Juan J. Torres, Associate Laboratory Director, Energy Systems Integration, National Renewable Energy Laboratory and Co-Chair, Grid Modernization Lab Consortium	
Oral Statement	28
Written Statement	30
Ms. Kelly Speakes-Backman, CEO, Energy Storage Association	
Oral Statement	40
Written Statement	42
Ms. Katherine Hamilton, Chair, 38 North Solutions and Executive Director, Advanced Energy Management Alliance	
Oral Statement	50
Written Statement	52
Discussion	61
Appendix I: Answers to Post-Hearing Questions	
The Honorable Karen Evans, Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy	78
Mr. Juan J. Torres, Associate Laboratory Director, Energy Systems Integration, National Renewable Energy Laboratory and Co-Chair, Grid Modernization Lab Consortium	80
Ms. Kelly Speakes-Backman, CEO, Energy Storage Association	82
Ms. Katherine Hamilton, Chair, 38 North Solutions and Executive Director, Advanced Energy Management Alliance	84

Appendix II: Additional Material for the Record

Letter submitted by Representative Conor Lamb, Chairman, Subcommittee on Energy, Committee on Science, Space, and Technology, U.S. House of Representatives	88
---	----

**THE FUTURE OF ELECTRICITY DELIVERY:
MODERNIZING AND SECURING OUR
NATION'S ELECTRICITY GRID**

WEDNESDAY, JULY 17, 2019

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ENERGY,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:03 p.m., in room 2318 of the Rayburn House Office Building, Hon. Conor Lamb [Chairman of the Subcommittee] presiding.

**COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON ENERGY
U.S. HOUSE OF REPRESENTATIVES
HEARING CHARTER**

The Future of Electricity Delivery: Modernizing and Securing our Nation's Electricity Grid

Wednesday, July 17, 2019

2:00 PM EST

2318 Rayburn House Office Building, Washington, D.C. 20015

PURPOSE

The purpose of this hearing is to examine research needs to modernize and secure our nation's electricity grid. The hearing will focus on two draft bills. The first, the Grid Modernization Research and Development Act of 2019, sets out a research, development, and demonstration agenda on grid resilience and emergency response; smart grid modeling, visualization, architecture, and controls; grid-scale energy storage; hybrid energy systems; and integration of renewable energy sources, vehicles, and buildings onto the electric grid. The second, the Grid Cybersecurity Research and Development Act of 2019, authorizes a research, development, and demonstration program on cybersecurity research in the electricity sector; directs DOE to develop standards, protocols, and roadmaps on grid cybersecurity; authorizes a technical assistance program to help utilities identify and address cybersecurity concerns; establishes an education and workforce training program for cybersecurity professionals; and creates an interagency Task Force on Grid Cybersecurity.

WITNESSES

- **The Honorable Karen Evans**, Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy
- **Mr. Juan J. Torres**, Associate Laboratory Director, Energy Systems Integration, National Renewable Energy Laboratory and Co-Chair, Grid Modernization Lab Consortium
- **Ms. Kelly Speakes-Backman**, CEO, Energy Storage Association
- **Ms. Katherine Hamilton**, Chair, 38 North Solutions and Executive Director, Advanced Energy Management Alliance

BACKGROUND

Our nation's electricity grid is undergoing a series of transformations, which includes adapting to a changing electricity generation mix¹; an increase in "smart grid" technologies to help develop an intelligent electric power system²; and a growing need to improve the resilience of the electric power grid.³ Additionally, the recent milestone of the very first report of a cybersecurity threat on the U.S. electricity grid on March 5, 2019 has elevated the importance of upgrading our nation's resilience to cybersecurity attacks on our electricity systems.⁴ The Department of Energy has an important role to play in the development of technologies and other supporting programs to achieve these goals.

Prior to 2018, the Department of Energy research programs on grid modernization and grid cybersecurity were housed under a single office called the Office of Electricity and Energy Reliability. On February 14, 2018, Secretary Perry announced that this office would be split into two offices: the Office of Electricity (OE) and a new Office of Cybersecurity, Energy Security, and Emergency Response (CESER).⁵ CESER was formed to "support the Administration's commitment to protecting energy infrastructure security" and this new organization structure was reflected in the President's FY19 budget request.⁶ The sections below summarize the roles of these two offices.

Department of Energy, Office of Electricity (OE)

The DOE Office of Electricity's main mission is to support grid modernization and resilience through programs that improve the planning and operational capabilities of the electrical sector at both the transmission and distribution level. This includes research on a variety of technologies related to: the smart grid, demand response, microgrids, energy storage, renewable energy integration, transformer resilience, grid planning, sensor development, and power flow controllers. OE also provides technical assistance to States, regional entities, and tribes on a variety of topics to assist with the development and implementation of their electricity-related policies and handles permitting of cross-border transmission lines and coordinating Federal transmission permitting on Federal lands.

The President's Fiscal Year 2020 budget request would, if enacted, increase federal support for OE R&D activities by 17% from the FY19 enacted level. Most programs receive an increase in

¹ <https://www.eia.gov/todayinenergy/detail.php?id=38053#>

² CRS, *The Smart Grid: Status and Outlook*. <https://www.crs.gov/Reports/pdf/R45156>

³ National Academies of Science, Engineering, and Medicine, *Enhancing the Resilience of the Nation's Electricity System*. <https://www.nap.edu/catalog/24836/enhancing-the-resilience-of-the-nations-electricity-system>

⁴ DOE Electric Emergency and Disturbance Report. <https://www.oe.netl.doe.gov/download.aspx?type=OE417PDF&ID=79>

⁵ <https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency>

⁶ CRS, *DOE Office of Electricity Delivery and Energy Reliability: Organization and FY2019 Budget Request*. <https://www.crs.gov/reports/pdf/IF10874>

funding and the request also includes a 30% cut for research on resilient distribution systems (RDS).⁷ The major decrease in funding for RDS research would result from cutting programs that support research on low cost distribution sensors and development of Internet of Things (IOT) devices for use on the electric grid. The FY20 budget also includes a proposal for a new “Advanced Energy Storage Initiative,” described as an “intra-Departmental initiative” that “aligns shared R&D across the Offices of Fossil Energy, Electricity, and Energy Efficiency and Renewable Energy in energy storage”.⁸

FY 2019 Enacted:	\$ 156 million
FY 2020 Budget Request:	\$ 182.5 million

Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

The DOE’s Office of Cybersecurity, Energy Security, and Emergency Response (CESER) mission is to lead “the Department of Energy’s emergency preparedness and coordinated response to disruptions to the energy sector, including physical and cyber-attacks, natural disasters, and man-made events”.⁹ CESER programs support improving cybersecurity preparedness in the energy sector; coordinating responses and recovery from cyber incidents; detecting and mitigating cyber risks for energy sector owners and operators; and sharing of threat information among energy sector partners, in addition to a variety of other activities. CESER partners with other federal agencies, including DHS, DOD, and NIST, and industry partners in carrying out its mission.

The President’s Fiscal Year 2020 budget request would, if enacted, increase federal support for CESER R&D activities by 30.4% from the FY19 enacted level.

FY 2019 Enacted:	\$ 120 million
FY 2020 Budget Request:	\$ 156.5 million

LEGISLATION

Draft Grid Modernization Research and Development Act of 2019

This draft bill authorizes a broad research, development, and demonstration agenda on several topics relating to grid modernization. It would authorize existing activities at the DOE pertaining to grid resilience, emergency response, and modeling and visualization activities. It would also

⁷ https://www.energy.gov/sites/prod/files/2019/04/f61/foe-fy2020-budget-volume-3-part-1_0.pdf

⁸ <https://www.energy.gov/ceser/ceser-mission>

provide programmatic direction on emerging research areas including hybrid energy systems, which are systems composed of two or more energy sub-systems that provide services such as thermal energy storage, desalination, and chemical production. The draft bill also authorizes research on the integration of various technologies and systems onto the electric grid, including renewable energy, vehicles, and buildings. Lastly, this draft bill would authorize a cross-cutting research program on grid-scale energy storage, which incorporates language from the Promoting Grid Storage Act (H.R. 2909), introduced this Congress by Mr. Casten, Mr. Luján, Mr. Doyle, Mr. McNerney, Mr. Bacon, Mr. Tonko, Mr. Foster, and Mr. Welch, and the Better Energy Storage Technology (BEST) Act (H.R. 2986), introduced this Congress by Mr. Foster, Mr. Casten, Ms. Herrera Beutler, and Mr. Gonzalez.

Draft Grid Cybersecurity Research and Development Act of 2019

The current draft of the Grid Cybersecurity Research and Development Act of 2019 is an updated version of H.R. 4120 from the 115th Congress, which was introduced in 2017 by Mr. Bera, now-Chairwoman Johnson, Mr. Lipinski, Ms. Bonamici, and Ms. Rosen. This bill would authorize a cross-agency research and development program to advance cybersecurity capabilities for the electricity sector across the Department of Energy, Department of Homeland Security, National Institute of Standards and Technology, and National Science Foundation. This draft would include authorization of test bed facilities to test and improve cybersecurity devices, components, and processes; development of an Interagency Strategic Plan to advance cybersecurity capabilities for the electricity sector; and authorization of an education and workforce training program led by DOE to identify core skills used by industrial control system (ICS) cybersecurity professionals and to develop methods to retrain electricity sector personnel.

Chairman LAMB. All right, this hearing will come to order. Without objection, the Chair is authorized to declare recess at any time. Good afternoon, welcome to today's hearing, "The Future of Electricity Delivery: Modernizing and Securing Our Nation's Electricity Grid." I want to thank all of our witnesses for joining us here today. This is such an important topic.

I'm a young guy, as you can tell, but I have read some history about what it was like when we first started building the electric grid, over a century ago now. I don't think we could have imagined the technologies that we would use to power our homes, and businesses, and hospitals, and everything today. And I think the challenge is different. You know, back then the real challenge was just extending power itself throughout every corner of our society, and there was a challenge, which was that those providing power knew they could make money in the cities, in well-populated areas, in places with a lot of business and commercial opportunities, but it was not as profitable to take electric power out into the countryside, into the hill country of Texas, for example. And so the government made a basic deal, which was that they would provide, essentially, a monopoly over providing power in a lot of these areas. Firms would make quite a bit of money, utilities would, and in exchange they would carry their product everywhere that it needed to be. And I think in the 21st century, we have a similar dilemma on our hands, but there's a similar deal to be made, which is today the challenge is not just to provide power itself everywhere, but to provide power in a way that is clean, and efficient, and allows us to stay economically competitive, even as we become a society much less dependent on carbon. And although electricity demand has been flat, we should see electricity demand increase as we electrify more segments of our society in order to accomplish those goals.

But to get there it's clear that we have to change the energy sector. We know that as we do that, for example, there are going to be much more serious threats to our electric grid, from cyberattacks and otherwise. We know that the economics of this whole thing are changing, as natural gas resources have come online. That's good for constituents like mine, who are saving money, but as all this stuff changes, we're going to have to invest to really upgrade the system that is meant to integrate all these new sources of energy, and to strike a balance between them in real time, which has become one of the big challenges with battery storage especially. That's a computing challenge, is a technological challenge. It's a challenge when it comes to making the basic infrastructure investment, and that's what we're here to talk about today.

I was definitely alarmed to hear, as I'm sure many of you were, about the first serious cyberattack on our Nation's electric grid back in March, or at least it was reported in March. As far as we know, no customers lost power in that attack, but it obviously is a warning sign of the incredibly serious damage that could happen if we don't take action on this issue. And by the time one happens when somebody does lose power, it'll be much too late, and so the choice facing all of us today is whether we can get the legislative machinery to work in such a way that we can really make a serious investment, and try to protect folks from the cyberattacks that we

all know are going to come. We know that Russia, and China, and other adversaries are actively probing our defenses, and they would love to have in their back pocket the ability to shut down parts of our grid when it's convenient for them, and the decision facing us is whether we will allow that to happen. And I think I speak for every Member of this Committee when I say that we will not.

That's why I'm looking forward to talking about these subjects today. We have the draft *Grid Modernization Research and Development Act of 2019*, which will allow us to set forth a wide array of research opportunities on topics like grid modernization, resilience, emergency response, modeling, which we know is going to be so important to be able to manage the new type of grid that we have, and better integration of buildings, vehicles, and renewable sources. Several Members of this Committee, including Mr. Casten and Mr. Foster, have already introduced legislation on these subjects, and we are happy to incorporate elements of those into these drafts that we'll continue working on making sure we do that.

We're also looking at the *Grid Cybersecurity Research and Development Act of 2019*, which updates a bill previously introduced by Mr. Bera. This would authorize a cross-agency research and development (R&D) program to do exactly what I've discussed, which is harden and mitigate the electric grid from cyberattacks. It would be carried out in partnership with Department of Homeland Security (DHS), the National Institute for Standards and Technology, and the National Science Foundation would involve technical assistance, education, and workforce.

One of the aspects of cybersecurity that I think is often underappreciated is the fact that it is also a workforce issue. We don't have enough people trained and working in cybersecurity today as we need, and there will be tens of thousands, or even hundreds of thousands, more openings in the next few years, many of which in my home area of Pittsburgh, because of the great work done at Carnegie Mellon, but also the University of Pittsburgh's Cyber Law Institute, among others, really training people up for this. And so that's what these kind of programs are going to authorize. We're excited to talk about them.

[The prepared statement of Chairman Lamb follows:]

Good afternoon and thank you to all our witnesses joining to discuss a critical topic to our nation: the electric grid. When we were first started building the grid over a century ago, we couldn't have imagined the technologies we'd use to power our homes and businesses - much less the technologies that would depend upon electricity. And despite the incredible advancements our scientists, researchers, companies and universities have pioneered since, many of the basic principles of our grid's design and operation remain unchanged.

One thing I've heard both sides of the aisle emphasize is the need for increased infrastructure investment. Any infrastructure plan must include the grid, and we need new technology solutions to upgrade the backbone of the energy system for the 21st century.

It's clear the energy sector is changing as our grid faces challenges like cyber threats and climate change. We also know that the generation resources used to power our grid are changing. The costs of electricity have continued to drop as we found new ways to develop natural gas resources and made breakthrough advancements in renewable resources like wind and solar. These generation changes have saved constituents money and are lowering carbon emissions - critical as we continue to try and mitigate the effects of climate change.

Our economy and civilization increasingly rely on electricity. It only makes sense to invest in the delivery system for what powers our hospitals and schools, our factories and homes. And it makes sense to invest in the research that allows for ad-

vancements and adoption of new technology and protects this critical infrastructure from adversaries or natural disasters.

I was alarmed to hear, as I am sure many were, of the first incident of a cyber attack on our nation's electricity grid, reported to the Department of Energy by an anonymous Western utility on March 5th, 2019. While no customers lost power, this attack portends the potential damage to come and the importance of bolstering our grid's security.

This is why I'm looking forward to discussing two important legislative drafts at this hearing today that will guide the Department's research and development activities on grid modernization and cybersecurity. The draft *Grid Modernization Research and Development Act of 2019* would set forth a comprehensive research agenda on several important topics in grid modernization, including grid resilience, emergency response, modeling and visualization, and the better integration of buildings, vehicles, and renewable energy sources onto the electric grid.

I understand that several members of this committee, led by Mr. Casten and Mr. Foster, have introduced legislation on energy storage, elements of which are also incorporated into these drafts.

The second draft bill we are here to discuss, the draft *Grid Cybersecurity Research and Development Act of 2019*, updates a bill that was previously introduced by my colleague on this Committee, Mr. Bera. This bill authorizes a cross-agency research and development program to harden and mitigate the electric grid from cyber attacks. This research program would be carried out in partnership with the Department of Homeland Security, the National Institute for Standards and Technology, and the National Science Foundation and includes technical assistance, education and workforce programs, and interagency coordination as tools to achieve these important security goals. I hope we're able to work together in a bipartisan way to develop and advance these bills to ensure our grid remains reliable, resilient, and secure.

Chairman LAMB. And, with that, I will now recognize the Ranking Member, Mr. Weber, for an opening statement.

Mr. WEBER. Thank you, Chairman Lamb, for hosting this hearing. I was asking what the population of Pittsburgh is. The metro area is about 1.5 million. Is that about right? So that's a lot of electricity. Well, we appreciate you hosting this hearing. This afternoon we will hear from expert witnesses on the existing strengths and weaknesses of our Nation's electric grid, and the impact that potential attacks and incidents could have on our grid reliability and national security. Our witnesses today will also discuss advances in the research and development of new grid tools and technologies, and hopefully provide insight, I know you will, on how the Federal Government can work alongside of American industries to strengthen our energy sector.

The reliability of America's power grid is one of our greatest economic strengths. I like to say that the things that make America great are the things that America makes. How do we do that? We have a strong, reliable energy supply, that's how we do it. In my home State of Texas, reliable and affordable power serves a population that is increasing by more than 1,000 a day. Chairman Lamb, that's what I was asking you. We literally get 30,000 people a month into Texas. Now multiply times 12, and you figure out real quick what that does in a year. One thousand people per day, and it supports the energy-intensive industries that drive the United States consumption of energy. Texas is by far the Nation's largest producer and consumer of electricity, and keeping its power grid reliable and secure is absolutely key to maintaining U.S. economic growth. But even in Texas, it is common knowledge that our electric grid faces significant and diverse threats to the reliability and resiliency of power delivery.

Put simply, we cannot predict when a cyberattack would threaten our power supply, that you referenced, Mr. Chairman, and we do not know when the next natural disaster might occur. In 2017, we were reminded of this fact by the impact of Hurricane Harvey, a devastating Category 4 hurricane that hit the Texas Gulf Coast and caused significant generator and transmission line outages for many on the Texas Gulf Coast and the Texas Interconnection. However, due to proper planning and management by what we call ERCOT, the Electric Reliability Council of Texas, the Texas grid was able to recover quickly from this devastating storm.

Since it's not a question of if, but a question of when that same power grid will face significant physical and cyber threats, the modernization of the national electricity system must be our priority. According to the Department of Energy, DOE, the U.S. electric grid must be updated within the next decade to address challenges, including aging U.S. energy infrastructure, changes in demand for energy, emerging threats, and fundamental shifts in the U.S. energy supply portfolio as energy sources, rightfully so, like renewables and nuclear increase. Again, we can see these changes taking place in my very own home State, where today nuclear generation is our most reliable source of energy, in fact running at more than 93 percent of the time over the last 3 years. And where we also lead the Nation in wind energy, and we're number five in solar energy, by the way.

As next generation energy technologies continue to come online, and as cybersecurity capabilities continue to grow and evolve, we must take our action to counter our grid vulnerabilities, and provide necessary updates to this very critical and necessary infrastructure. Thankfully, DOE funds broad research and development programs to support grid modernization and security technologies through departmentwide collaborations like the Grid Modernization Initiative, or GMI, and the Grid Modernization Lab Consortium, GMLC. DOE also funds robust research in novel grid technologies and computational modeling efforts through its Office of Electricity, OE, and cybersecurity technology for energy delivery systems through its Office of Cybersecurity, Energy Security, and Emergency Response, CESER. We are grateful to have two witnesses representing these important efforts here this afternoon, the Honorable Karen Evans, Assistant Secretary of CESER, and Mr. Juan Torres, an Associate Laboratory Director at the National Renewable Energy Laboratory, and co-Chair of Grid Modernization Lab Consortium. Welcome to both of you, welcome to all of you.

Modernizing our grid will require these important programs, along with cooperation from many Federal agencies, States, and industry. I trust our witnesses can share their expertise, and provide valuable insight on how Congress can best support these very collaborative efforts. I want to thank the Chairman again for holding this hearing. I look forward to very productive and, dare I say, electrifying discussion. And, Mr. Chairman, I yield back.

[The prepared statement of Mr. Weber follows:]

Thank you, Chairman Lamb, for hosting this hearing. This afternoon, we will hear from expert witnesses on the existing strengths and weaknesses of our nation's electric grid, and the impact that potential attacks and incidents could have on our grid reliability and national security.

Our witnesses today will also discuss advances in the research and development of new grid tools and technologies and provide insight into how the federal government can work alongside American industry to strengthen our energy sector.

The reliability of America's power grid is one of our greatest economic strengths. In my home state of Texas, reliable and affordable power serves a population that is increasing by more than 1,000 people per day and supports the energy intensive industries that drive U.S. consumption of energy. Texas is by far the nation's largest producer and consumer of electricity and keeping its power grid reliable and secure is key to maintaining U.S. economic growth.

But even in Texas, it is common knowledge that our electric grid faces significant and diverse threats to the reliability and resilience of power delivery. Put simply, we cannot predict when a cyberattack would threaten our power supply and we don't know when the next natural disaster will occur.

In 2017, we were reminded of this fact by the impact of Hurricane Harvey, a devastating Category 4 hurricane that hit the Gulf Coast and caused significant generator and transmission line outages for many on the Texas Interconnection.

Due to proper planning and management by the Electric Reliability Council of Texas (ERCOT), the Texas grid was able to quickly recover from this devastating storm. But since it is not a question of "if" but a question of "when" the power grid will face significant physical and cyber threats, the modernization of the national electricity system must be our priority.

According to the Department of Energy (DOE), the U.S. electric grid must be updated within the next decade to address challenges including aging U.S. energy infrastructure, changes in demand, emerging threats and fundamental shifts in the U.S. energy supply portfolio as energy sources like renewables and nuclear increase.

Again we can see these changes taking place in my home state, where today, nuclear generation is our most reliable source of energy, running at more than 93% of the time over the past three years - and where we lead the nation in wind energy.

As next-generation energy technologies continue to come online, and as cybersecurity capabilities continue to evolve, we must take action to counter our grid vulnerabilities and provide necessary updates to this critical infrastructure.

Thankfully, DOE funds broad research and development programs to support grid modernization and security technologies through Department-wide collaborations like the Grid Modernization Initiative (GMI), and the Grid Modernization Lab Consortium (GMLC).

DOE also funds robust research in novel grid technologies and computational modeling efforts through its Office of Electricity (OE) and cybersecurity technology for energy delivery systems through its Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

We are grateful to have two witnesses representing these important efforts here this afternoon: the Honorable Karen Evans, Assistant Secretary of CESER, and Mr. Juan J. Torres, an Associate Laboratory Director at the National Renewable Energy Laboratory and Co-Chair of Grid Modernization Lab Consortium.

Modernizing our grid will require these important programs, along with cooperation from many federal agencies, states, and industry. I hope our witnesses can share their expertise and provide valuable insight on how Congress can best support these collaborative efforts.

I want to again thank the Chairman for holding this hearing, and I look forward to a productive discussion today.

Chairman LAMB. It wouldn't be the first time that electricity was powered by a lot of hot air from Texas.

Mr. WEBER. Or the last.

Chairman LAMB. Had to include that for the Ranking Member's granddaughter in the audience today. We welcome her. And I do think it is important to note the bipartisan nature of this discussion. As it often is on this Committee on these subjects, Mr. Weber and I both are big supporters of nuclear energy, and a sort of all-of-the-above-type strategy. It's one thing that doesn't always break through the headlines, but is a beacon of hope here in Washington some days.

[The prepared statement of Chairwoman Johnson follows:]

Good afternoon and thank you, Chairman Lamb, for holding this hearing on two important and related issues that our nation's energy infrastructure is now con-

fronting: The resilience of our electric grid and its security from cyber and physical attacks.

A few months ago, this committee held a hearing where we discussed the need for renewable energy research and development, specifically focusing on wind and solar energy. I am always excited to talk about how Texas leads the U.S. in installed wind energy capacity, with over 24 gigawatts of wind energy. However, significant work needs to be done to our electric grid to help utilize all this energy in the most efficient way we can, and in coordination with all of the other types of energy that are now being integrated into the grid.

I am pleased that the President's budget request reflects significant increases in research and development activities for both the Office of Electricity, where the Department performs its grid modernization work, and the Office of Cybersecurity, Energy Security, and Emergency Response, which leads its grid cybersecurity work. I am disappointed, however, that the request also includes a 30% cut for research on resilient distribution systems within the Office of Electricity.

This would ultimately take money away from research on low cost distribution sensors, and it would cut the development of smart devices that can help minimize the impacts of local disruptions to our energy systems. If we are to successfully transform our Nation's grid to support the technologies of the future, we need to be sufficiently funding R&D in these areas as well.

The two drafts of legislation we will be discussing today would provide important guidance and support for these critical programs over the next several years. The Grid Modernization Research and Development Act of 2019 authorizes a broad research, development, and demonstration program on a wide variety of grid modernization topics, including advanced hybrid energy systems and a grid-scale energy storage initiative. The Grid Cybersecurity Research and Development Act of 2019 is an updated version of a bill that Mr. Bera and I introduced, along with many of my Science Committee colleagues, in the previous two Congresses. This bill would authorize a cross-agency research and development program to advance electric grid cybersecurity efforts.

I am looking forward to hearing from the experts assembled here today on what we can do to improve the electric grid so that we are ready for the electricity needs of the future. This Committee is fortunate to be able to focus on supporting the development of a wide range of exciting, cutting-edge energy technologies. But the grid really is the backbone energy infrastructure of our Nation, and we should be doing everything we can to ensure that it is robust enough to utilize these new technologies in a safe and reliable way.

With that, I yield back.

Chairman LAMB. So at this time I would like to introduce our witnesses. The Honorable Karen Evans is Assistant Secretary of the Office of Cybersecurity, Energy Security, and Emergency Response, CESER, at the U.S. Department of Energy. Before leading CESER, Mrs. Evans was the national director of the U.S. Cyber Challenge, a public-private program designed to help address the skills gap in the cybersecurity field. She also worked for the George W. Bush Administration, where she was an IT official at the Office of Management and Budget, and served as the Department of Energy's Chief Information Officer.

Mr. Juan Torres is the Associate Laboratory Director for Energy Systems Integration at NREL (National Renewable Energy Laboratory), and the Co-Chair of the Grid Modernization Laboratory Consortium, which is a partnership of 14 national labs to advance modernization of the U.S. power grid. Prior to joining NREL, Mr. Torres held a variety of positions over the course of a 27-year-long career at Sandia National Lab, where he worked on securing our energy infrastructure, among other topics.

Ms. Kelly Speakes-Backman is the CEO of the Energy Storage Association (ESA). Kelly has spent over 20 years working in energy and environmental issues in the public, NGO, and private sectors, including United Technologies, Sun-Edison, and Alliance to Save Energy. She is a former Commissioner of the Maryland Public

Service Commission, where she also served as Chair of the Board of Directors of the regional Greenhouse Gas Initiative, co-Vice Chair of the NARUC (National Association of Regulatory Utility Commissioners) Committee on Energy Resources and the Environment, and a member of the EPRI (Electric Power Research Institute) Energy Efficiency and Grid Modernization Public Advisory Group.

And Ms. Katherine Hamilton is the Chair of 38 North Solutions, a public policy consultancy specializing in clean energy and innovation, and the Executive Director of the Advanced Energy Management Alliance. She previously ran the Gridwise Alliance, was policy director to the Energy Storage Association, and worked at the National Renewable Energy Laboratory. Katherine worked in buildings research and government relations. She also spent a decade at an investor-owned utility designing electrical systems for commercial and residential developments.

As our witnesses should know, you will each have 5 minutes for your spoken testimony. Your written testimony will be included in the record. When you have completed your spoken testimony, we will begin with questions, and each Member will then have 5 minutes for questions. We will start with the testimony of Ms. Evans.

**TESTIMONY OF THE HONORABLE KAREN EVANS,
ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY,
ENERGY SECURITY, AND EMERGENCY RESPONSE,
U.S. DEPARTMENT OF ENERGY**

Hon. EVANS. Chairman Lamb, Ranking Member Weber, and Members of the Subcommittee, it is an honor and a privilege to serve at the Department of Energy as the Assistant Secretary for the Office of Cybersecurity, Energy Security, and Emergency Response. Thank you for the opportunity to testify on behalf of the Department. One of the most critical missions at DOE is developing the science and technology to successfully counter the ever-evolving increasing threat of cyber and other attacks on our networks, data, facilities, and infrastructure. DOE works closely with our Federal agencies, State, local, tribal, and territorial governments, industry, and our National Laboratory partners to accomplish this mission.

Another critical mission for DOE is ensuring the resilience of our electric grid, and successfully countering the ever-evolving increasing threat of physical and cyberattacks. DOE recently announced an \$8 million investment in innovations that will enhance the reliability and the resiliency of our Nation's energy infrastructure. This R&D partnership opportunity will spur the development of the next generation of tools and technologies that will become widely adopted throughout the energy sector. As we protect our infrastructure from cyber threats, we are also working to improve and complete the resilience of our electricity systems.

Our Office of Electricity also supports transmission system resilience and generation diversity and is exploring new architecture approaches for the electric grid. This includes the development of the North American Energy Resilience Model, which aims to provide unique and groundbreaking national-scale energy planning, and real-time situational awareness capabilities to enhance secu-

rity and resilience. A large component of DOE's work is pursuing cutting-edge innovation in Big Data, artificial intelligence, and grid-scale energy storage based on new technology.

Grid-scale storage will be an important enabler for renewable integration, and for clean-based load power. While today's technologies are already providing value to the grid, there are physical limitations to the traditional batteries and pumped hydro that will be surpassed by the next-generation technologies. Efforts in grid-scale energy storage are already producing important advancements. Grid-scale energy storage technologies have been demonstrated using new generation of advanced flow batteries that rely on lower cost electrolytes. We are also continuing to advance energy storage through our Advance Energy Storage Initiative, which includes the development of the new grid storage launch pad, aimed at accelerating materials development, testing, and independent evaluation of battery technologies for grid applications.

The DOE National Laboratories support the development of technologies that strengthen and improve energy infrastructure so that consumers have access to reliable and secure sources of energy. Another program driving enabling technologies is DOE's Grid Modernization Initiative, GMI, which focuses on the integration of increasing amounts of variable generation into the grid through R&D investments at our national labs. One noteworthy GMI effort will accelerate the conversion of the National Wind Technology Center campus into an experimental micro-grid capable of testing grid integration at megawatt scale.

These are just a few of the examples of how the United States is approaching its commitment to updating and improving its energy infrastructure and environmental responsibility within its own border, but these same issues are also at the heart of so many of our partnerships and work abroad. Reliant and resilient energy infrastructure is critical to the U.S. economy's competitiveness, innovation, and leadership. Our long-term approach will strengthen our national security and positively impact our economy. I appreciate the opportunity to appear before this Subcommittee, and I'm happy to answer questions at the appropriate time.

[The prepared statement of Hon. 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 Science, Space, and Technology
Subcommittee on Energy
United States House of Representatives
July 17, 2019

Introduction

Chairman Lamb, Ranking Member Weber, and Members of the Subcommittee, it is an honor and a privilege to serve at the Department of Energy (DOE or the Department) as Assistant Secretary for the Office of Cybersecurity, Energy Security, and Emergency Response (CESER). Thank you for the opportunity to testify on behalf of the Department.

A reliable and resilient electric grid is critical to U.S. economic competitiveness and leadership, as well as the overall safety and security of our Nation. However, our Nation's energy infrastructure has become a primary target for hostile cyber actors, both state- 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

One of the most critical missions at DOE is developing the science and technology to successfully counter the ever-evolving, increasing threat of cyber and other attacks on our networks, data, facilities, and infrastructure. DOE works closely with our Federal agency, State, local, tribal and territorial (SLTT) governments, industry, and National Laboratory partners to accomplish this mission.

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

Below are some highlights and perspectives regarding the legislation being discussed today, followed by highlights of the work we are doing to advance the modernization and protection of our electric grid.

Grid Modernization Research and Development Act of 2019

The Grid Modernization Research and Development Act of 2019 focuses on eight areas, including enhancing grid resilience and emergency response; smart grid modeling, visualization, architecture, and controls; a technology demonstration grant program; grid-scale energy storage; hybrid energy systems; grid integration; grid cybersecurity (H.R. 4120 from 115th Congress); and protection of sensitive grid information.

Maintaining a modern, flexible, and secure network of electric power transmission and distribution lines, oil and natural gas pipelines, and storage facilities is essential to keeping energy accessible and affordable for businesses and consumers, promoting growth across all sectors, and supporting the continued health of the country's domestic energy industry.

Since taking office, the President has prioritized ensuring our infrastructure keeps pace with our energy abundance. He announced the Civil Nuclear Review to enable revitalization of the nuclear energy sector, while supporting R&D efforts on behalf of renewables, storage, and energy efficiency.

The Department has provided technical comments on this bill.

H.R. 4120 - Grid Cybersecurity Research and Development Act

This bill directs the Secretary to coordinate with appropriate Federal agencies, the Electricity Subsector Coordinating Council (ESCC), SLTT governments, private sector vendors, and other relevant stakeholders to:

- Carry out a research, development, and demonstration initiative to harden the electric grid and mitigate the consequences of cyber attacks by increasing the cybersecurity capabilities of the electricity sector and accelerating the development of cybersecurity technologies and tools.
- Coordinate the development of guidance documents for research and demonstration activities to improve the cybersecurity capabilities of the electricity sector through participating agencies.
- Leverage the research facilities and expertise of the National Laboratories to utilize voluntary vulnerability testing and provide technical assistance to increase cyber resilience.
- Develop education and workforce training research and standards by identifying core skills used by electricity sector industrial control systems cybersecurity professionals; and develop assessment methods and tools to identify existing personnel that show competence in those skills.
- Work in collaboration with the Secretary of Homeland Security, other appropriate Federal agencies, and energy sector stakeholders to conduct a study to analyze cyber

attacks on electricity sector industrial control systems and identify cost-effective opportunities to improve cybersecurity.

The Department is reviewing the proposed language, and we look forward to working with the Committee. DOE applauds Congress for recognizing that our national security depends on a resilient electric grid, and that reducing the risks to this critical infrastructure is one of our Nation's most urgent security challenges.

Another critical mission for DOE is ensuring the resilience of our electric grid and successfully countering the ever-evolving and increasing threat of physical and cyber-attacks on networks, data, facilities, and infrastructure.

CESER was established to help research and develop the tools and best practices to make our electric power grid and other energy infrastructure more resilient to these threats.

DOE recently announced an \$8 million investment in innovations that will enhance the reliability and resiliency of our nation's energy infrastructure. This R&D partnership opportunity will spur the development of the next generation of tools and technology that will become widely adopted throughout the energy sector.

As we protect our infrastructure from cyber threats, we are also working to improve the complete resilience of our electricity systems.

Our Office of Electricity also supports transmission system resilience and generation diversity, and is exploring new architecture approaches for the electric grid. This includes the development of the North American Energy Resilience Model that aims to provide unique and ground-breaking national-scale energy planning and real-time situational awareness capabilities to enhance security and resilience.

A large component of DOE's work is pursuing cutting-edge innovation in big data, A.I., and grid-scale energy storage based on new technology.

Grid-scale storage will be an important enabler for renewable integration and for clean baseload power. While today's technologies are already providing value to the grid, there are physical limitations to traditional batteries and pumped hydro that will be surpassed by next-generation technologies.

Efforts in grid-scale energy storage are already producing important advancements. Grid-scale energy storage technologies have been demonstrated using a new generation of advanced flow batteries, which rely on lower cost electrolytes.

We are also continuing to advance energy storage through our Advanced Energy Storage Initiative (AESI), which includes development of a new Grid Storage Launchpad aimed at accelerating materials development, testing, and independent evaluation of battery technologies for grid applications.

In addition, the R&D at DOE's National Laboratories supports the development of technologies that strengthen and improve energy infrastructure so that consumers have access to reliable and secure sources of energy.

Another program driving enabling technologies is DOE's Grid Modernization Initiative (GMI), which focuses on integrating an increasing amount of variable generation into the grid through R&D infrastructure investments at our National Labs. One noteworthy GMI effort will accelerate the conversion of the National Wind Technology Center campus into an experimental micro-grid capable of testing grid integration at the megawatt scale.

These are just some of the examples of how the United States is approaching its commitment to updating and improving its energy infrastructure and environmental responsibility within its own border, but these same issues are also at the heart of so many of our partnerships and work abroad.

Energy Storage

Energy storage is a technology of national interest and the backbone of a future resilient energy system. With benefits extending to transportation, the power grid, and throughout the economy, DOE has been proactive in developing new tools and technologies to accelerate energy storage development, such as through GMI, AESI, and the Grid Storage Launchpad (GSL).

In May of this year, DOE issued its most recent Grid Modernization Lab Call, with Energy Storage and System Flexibility as one of the major topic areas. The lab call placed a particular emphasis on developing the storage functions that enhance system resilience and flexibility.

The proposed GSL will extend U.S. R&D leadership in energy storage through validation, collaboration, and acceleration. By validating new technologies at earlier maturity stages, the GSL will lower the time and expense of storage chemistry innovations. Through collaboration with universities and the commercial sector, the GSL will augment the industry with enhanced testing protocols and in-operando characterization capabilities. Finally the GSL will accelerate and de-risk new technologies by propagating rigorous grid performance requirements to all stages of storage development, from benchtop to systems.

DOE established the Mission Need for the GSL at Critical Decision 0 (CD-0) in November of 2018. We anticipate finalizing the preferred alternative facility and cost range as part of CD-1 this summer.

The FY 2020 Budget requested funds for design and construction planning of the GSL. The FY 2020 Budget also proposes an AESI led by DOE's Offices of Electricity (OE) and Energy Efficiency and Renewable Energy (EERE), in conjunction with the Offices of Fossil Energy (FE) and Nuclear Energy (NE). AESI will provide a platform to coordinate R&D activities across these programs—and existing energy storage efforts in the Office of Science (SC) and the Advanced Research Projects Agency (ARPA-E)—to establish aggressive, achievable, and measurable goals for cost-competitive energy storage technologies, services, and applications. In

FY 2020, AESI will establish application-specific cost and performance metrics to align research objectives and to coordinate the development of new energy storage and flexibility technologies.

Finally, OE's Energy Storage Program continues to conduct research and development to expand storage capabilities and shared industry knowledge. From performance breakthroughs in batteries based on earth-abundant materials to evaluation tools and workshops for state regulators, OE is at the forefront in helping communities realize the benefits of energy storage.

CESER

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. DOE is the lead SSA for cybersecurity for the energy sector as provided in the Fixing America's Surface Transportation Act of 2015 (P.L. 114-94). CESER provides greater visibility, accountability, and flexibility to better protect our Nation's energy infrastructure and support asset owners, as well as the overall critical infrastructure response framework overseen by the Department of Homeland Security (DHS).

DOE's Roles and Responsibilities for Energy Sector Cybersecurity

The release of the President's National Cyber Strategy (NCS) in September 2018 demonstrates the Administration's commitment to strengthening our Nation's cybersecurity capabilities, specifically securing critical infrastructure. The NCS prioritizes risk-reduction activities across seven key areas, including national security and energy & power. DOE's cybersecurity activities for the energy sector align to the Secure Critical Infrastructure section of Pillar 1 – (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 improving the Nation's cybersecurity posture in key areas, and builds on 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: 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 coordinate 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 ESCC, the Oil and Natural Gas Subsector Coordinating Council (ONG SCC), and the Energy Government Coordinating Council (EGCC). The ESCC and ONG SCC represent the interests of their respective industries. The EGCC, led by DOE and DHS, is where the interagency partners, States, and international partners come together to discuss the important security and resilience issues for the energy sector. This forum ensures that we are working together in a whole-of-government response.

The SCCs, EGCC, and associated working groups operate under DHS's Critical Infrastructure Partnership Advisory Council 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 cyber attacks 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™ 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™) pilot project. The CyOTE™ 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 Laboratory (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, the 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 industry. 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 electrical grid. 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 three energy sector Information Sharing and Analysis Centers (ISACs) – which include the Electricity ISAC (E-ISAC) – to share emerging and potential threats and disseminate information.

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.²

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 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 to a cyber attack.

² 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>.

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, and 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

A key to CESER's efforts to secure the Nation's electric grid against cyber attacks is supporting DOE's Grid Modernization Initiative. The Grid Modernization Initiative is introducing new technologies to better manage increasingly complex transmission and distribution systems. CESER has a central role in the Department's plan for integration of cybersecurity activities across DOE, and coordinates with other DOE offices through the Grid Modernization Laboratory Consortium (GMLC). An Executive Committee comprised of DOE leadership oversees the GMLC, through which we engage our leading experts and resources at DOE National Laboratories, collaborating on the goal of modernizing the Nation's electric grid. GMLC employs an integrated approach to ensure that DOE-funded studies and research and development are coordinated efficiently to reap the greatest return for the taxpayer dollar.

Through the GMLC, DOE's National Laboratories are assembling technical expertise to address specific cybersecurity challenges facing the electric grid. For example, GMLC is developing advanced analytics of cyber data to assist in differentiating between cyber and non-cyber-caused incidents.

In alignment with 2019 Executive Order 13865, "Coordinating National Resilience to Electromagnetic Pulses" (Mar. 26, 2019), CESER also works closely with the private sector, as well as Federal and SLTT government partners to enable more coordinated preparedness for and

response to disruptions caused by electromagnetic pulses (EMPs) and geomagnetic disturbances (GMDs). An EMP can be created by non-nuclear events and by the high-altitude detonation of a nuclear weapon, which have the potential to damage power delivery assets and impact bulk-power system reliability over a wide area. GMDs, caused by Coronal Mass Ejection from the Sun, may result in geomagnetically-induced currents (GIC) in man-made structures such as rail lines, pipelines, electric transmission lines, and some communications lines. DOE is concerned about the impacts of GIC flows on power transformers. Transformer damage, although highly unlikely even in the most extreme storms, is possible and in certain situations can destabilize the electric grid if proactive measures are not undertaken (e.g., reducing load).

CESER is leading efforts within DOE to address EMP and GMD risks, using a multi-pronged approach: sharing knowledge and expertise with industry on a timely basis; allowing the electric subsector to advance readiness for potential EMP impacts through research to quantify the risk; and scientific development of mitigation strategies, and analysis of the policies needed for the future. CESER is fully committed to helping forge the grid of the future that will be more resilient to all hazards, including EMP/GMD. Continued progress in grid modernization is vital to helping us protect the grid from EMP/GMD.

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 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.

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 SLTT 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 that 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 National Rural Electric Cooperative Association (NRECA) and the American Public Power Association (APPA) to help further enhance the culture of security within their utility members' organizations. With more than a quarter of the Nation's electricity customers served by municipal public power providers and rural electric cooperatives, it is critical 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

Reliable and resilient energy infrastructure is critical to U.S. economic competitiveness, innovation, and leadership. 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 electrical 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 Subcommittee to discuss cybersecurity in the energy sector, and I applaud your leadership. I look forward to working with you and your respective staffs to continue to address physical and cybersecurity challenges to the grid.

Honorable Karen S. Evans

Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy

Karen S. Evans was sworn in by U.S. Deputy Secretary of Energy Dan Brouillette as the Assistant Secretary for the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) on September 4, 2018. Mrs. Evans was confirmed as Assistant Secretary for CESER by the U.S. Senate on August 28, 2018.

Before being nominated by President Donald J. Trump to lead the Department of Energy's cybersecurity efforts, Mrs. Evans was the National Director of the U.S. Cyber Challenge, a public-private program designed to help address the skills gap in the cybersecurity field. She also served as an independent director and outside manager for publicly-traded companies.

Mrs. Evans was previously a top IT official at the Office of Management and Budget under President George W. Bush in the position that is now known as the Federal CIO and also served as the Department of Energy's Chief Information Officer.

She received her MBA and BA in Chemistry from West Virginia University.

Chairman LAMB. Thank you. Mr. Torres?

**TESTIMONY OF JUAN TORRES,
CO-CHAIR, GRID MODERNIZATION LAB CONSORTIUM,
AND ASSOCIATE LABORATORY DIRECTOR,
ENERGY SYSTEMS INTEGRATION,
NATIONAL RENEWABLE ENERGY LABORATORY**

Mr. TORRES. Thank you. Chairman Lamb, Ranking Member Weber, Members of the Subcommittee, thank you for this opportunity to discuss the critical challenge of grid modernization and cybersecurity, and the crucial research needed to create a flexible, more secure, and more resilient U.S. power system. I'm Juan Torres. I serve as the Associate Laboratory Director for Energy Systems Integration at the Department of Energy's National Renewable Energy Laboratory, or NREL, in Golden, Colorado. I've been affiliated with Federal research in our National Laboratory system for more than 29 years. In my current position, I direct NREL's efforts to strengthen the security, resilience, and sustainability of our Nation's electric grid. In addition, I'm Co-Chair of the DOE Grid Modernization Laboratory Consortium, or GMLC, and team lead for the GMLC security and resilience research.

I commend the Committee for this timely discussion, given that every aspect of our economy, our national security, and critical infrastructure in the U.S. is deeply dependent on the reliable operation of our electrical system. I'm often asked, when will you be finished with modernizing the grid? The answer is that grid modernization is a journey. It's not a single destination. As long as we need electricity to remain economically competitive, to defend our Nation against evolving threats, and to maintain our way of life, we'll need to continually advance our electric infrastructure. Fundamentally, the research we're conducting must assure that our future grid has greater resilience to hazards of all types. Improved reliability for everyday operations, enhanced security from increasing and evolving threats, continued affordability to maintain our economic prosperity, superior flexibility to respond to the variability and uncertainty of conditions at different time scales, including a range of energy futures.

We've come a long way in a few short years of investment through the DOE's Grid Modernization Initiative, but there remains much work to do. Research within the GMLC has the opportunity to strengthen the trajectory of our grid's development. This work will in turn inform the investment decisions we make today so we can increase the impact of the new technologies that will serve the grid for decades to come. The steps we take now can move us toward enabling the grid of the future to address pressing challenges, such as a changing mix of generation types, a need for cost-effective energy storage, extreme weather events, increasing cyber and physical threats, electrification of our transportation system, and growing use of digital and communication technologies.

I'd like to highlight just a few examples of the important work that is ongoing around the National Labs system through DOE support. The National Labs' deep modeling capability is providing the basis for the DOE Office of Electricity's North American energy

resilience model that will, in the future, help us understand the state of resilience for the power grid and natural gas infrastructure. With DOE's Solar Technologies Office, we are developing a road map that will guide cybersecurity to confront the unique needs of the growing solar energy sector, and other distributed energy systems. And as I speak with you, NREL, in partnership with the DOE Wind Energy Technologies Office and the International Electrotechnical Commission, today is hosting a cybersecurity workshop at the National Wind Technology Center at NREL's Flat Iron campus. This event is bringing key government and industry players together for the first time to address the cybersecurity needs of the growing wind power industry.

Finally, I applaud the Subcommittee for the commitment and insight you have shown in holding this hearing, and with pending legislation that addresses the critical challenges of our future electric grid. The benefits of technical solutions cannot be fully realized without the appropriate business models, regulatory structure, and policies to support and enable them. Given the importance of these very issues to DOE, to the National Laboratories, and of course to Congress, I'd like to invite you to attend the National Lab Day on Capitol Hill next week, July 24, in the Rayburn House Office Building. The event will be focused exclusively on grid modernization and cybersecurity, and many grid researchers, other experts from the labs, as well as myself, will be on hand for a discussion and a series of exhibits that will highlight much of the work I'm discussing today. Thank you for the privilege to address this Committee, and I look forward to answering any questions you may have.

[The prepared statement of Mr. Torres follows:]

**Prepared Statement of Juan Torres
Associate Laboratory Director for Energy Systems Integration
National Renewable Energy Laboratory**

**For the U.S. House of Representatives Committee on Science, Space, & Technology,
Subcommittee on Energy
Hearing on "The Future of Electricity Delivery: Modernizing and Securing Our Nation's
Electricity Grid"**

July 17, 2019

Chairman Lamb, Ranking Member Weber, members of the Subcommittee, thank you for this opportunity to discuss the critical challenge of grid modernization and cybersecurity and the steps we can take from a research perspective to create a flexible, more secure, and more resilient U.S. power system.

I am Juan Torres, and I serve as the associate laboratory director for Energy Systems Integration at the U.S. Department of Energy's (DOE's) National Renewable Energy Laboratory, or NREL, in Golden, Colorado. I have been affiliated with federal research and our national laboratory system for nearly 30 years. In my current position, I direct NREL's efforts to strengthen the security, resilience, and sustainability of our nation's electric grid. In addition, I am co-chair of the DOE Grid Modernization Laboratory Consortium (GMLC) and technical lead for the GMLC's security and resilience team. The GMLC is a partnership of 14 national laboratories working to advance modernization of the U.S. power grid. Prior to joining NREL, I served for many years in various technical and managerial roles at Sandia National Laboratories, advancing cybersecurity, energy, and power grid research, most recently as deputy to the vice president for energy programs. Earlier in my career, I also served on the DOE task force that developed a plan to protect U.S. energy infrastructure in response to Presidential Decision Directive 63 on Critical Infrastructure Protection.

NREL was established in 1977 to advance renewable energy technologies as a commercially viable option. Over the years, our groundbreaking advanced energy research has contributed to transformational scientific advancements, exponential decreases in the cost of renewable energy, and more renewable installed capacity than ever before. We are continually looking ahead to understand how advanced technology options can enable a balanced national energy portfolio. From our perspective, grid modernization is one of the most crucial and urgent energy challenges our nation must address.

Why Grid Modernization

Every aspect of the economy, national security, and critical infrastructure in the United States is deeply dependent on the reliable operation of our electrical system. Yet the basic design of our country's

energy infrastructure has not changed much since the earliest electric grids were developed in the late 1800s—our grid is still largely built around the concept of one-way centralized generation and control. To put that into perspective, this approach to generating and delivering electricity predates the first automobiles.

The electric grid has served our country well for a very long time. However, the energy landscape—both in the United States and around the globe—is changing quickly. Cost-competitive renewables are making up a larger share of the energy mix. The grid edge, where consumers and energy users connect to the grid, is transforming into a dynamic space where energy is not just passively consumed, but generated, stored, managed, and traded. And infrastructures that once operated in silos, such as electricity, transportation, communications, and fuels, are increasing their overlap and interdependencies with each other.

These exciting dynamics are creating many opportunities, but also present urgent challenges in assuring our grid can meet evolving consumer needs, leverage technological advances, and mitigate today's and tomorrow's threats. Managing, optimizing, securing, and adding resilience to the future power system will require new technologies and control techniques, advanced sensing and data analytics, more sophisticated models and validation techniques, as well as effective business models and other institutional support. It will also require the electric grid to operate differently than it has for more than a century, with more flexibility and resilience to withstand both cyber and physical attacks as well as disruptions from natural disasters.

The magnitude and importance of this challenge cannot be overstated. Our country's continued security and economic growth simply depend on it. There is no time to delay. These fast-moving changes, along with growing cyber threats, require immediate and sustained action.

What Does a Modern Grid Look Like?

DOE's Grid Modernization Initiative was established to work with the electricity sector to address this question and leverage our national resources to drive solutions.

The Initiative has laid out these key characteristics that a modern grid must have:

- Greater **resilience** to hazards of all types
- Improved **reliability** for everyday operations
- Enhanced **security** from an increasing and evolving number of threats
- Additional **affordability** to maintain our economic prosperity
- Superior **flexibility** to respond to the variability and uncertainty of conditions at one or more timescales, including a range of energy futures.

Getting there will require an unprecedented level of research, collaboration, and innovation. For this reason, DOE partnered with its national labs to form the Grid Modernization Laboratory Consortium. The GMLC—co-led by NREL and the Pacific Northwest National Laboratory (PNNL)—acts as the boots on the ground to execute critical research that is already delivering solutions today, with plans to continue to do so well into the future.

The Focus and Impact of GMLC Research

The GMLC has proven to be a galvanizing and impactful initiative. Since its inception in 2015, it has jumpstarted grid modernization research and collaboration in the energy sector and transitioned technologies and concepts to the power sector not otherwise possible on such an accelerated timeframe.

Although it is not possible to highlight all the impressive achievements of GMLC projects here, it is worth noting a few real-world benefits that have already been realized:

- Developed an advanced microgrid design tool kit to increase the resilience of critical loads to major grid disruptions
- Developed concepts to improve the black start capability for recovery after a major power outage
- Developed the Hierarchical Engine for Large-scale Infrastructure Co-Simulation (HELICS) framework to couple grid transmission, distribution, and communications models to understand cross-domain effects
- Advanced 13 different sensing technologies across the end-use sector, transmission and distribution, and asset monitoring
- Developed a valuation framework that will allow stakeholders to conduct and interpret valuation studies of grid technologies with high levels of transparency, consistency, and extensibility
- Developed analytic tools to differentiate between cyber- and noncyber-initiated events
- Provided microgrid design support to Puerto Rico and the U.S. Virgin Islands after the devastation of Hurricane Maria
- Leveraged grid modeling tools and expertise toward development of the North American Energy Resilience Model (NAERM).

We have come a long way in a few short years, but there remains much work to do. Research within the GMLC has the opportunity to strengthen the trajectory of our grid's development at this timely juncture when investment decisions that our nation makes today will likely remain with us for decades to come. Steps taken now can help establish the modern grid of the future by positioning our grid with inherent resilience and flexibility to accommodate new trends and challenges, such as:

- A changing mix of generation types
- Extreme weather events
- Increasing cyber and physical threats
- Opportunities for customers to participate in electricity markets
- Growing use of digital and communication technologies.

I will touch on a few of the most important areas of future research in the following sections.

I commend the Subcommittee for the commitment and insight you have shown in addressing the critical challenges of developing the electric grid we need to meet the burgeoning demands of the future. Reflecting the importance of these very issues to DOE, to the national laboratories, and, of course, to Congress, I'd like to invite you to attend the National Lab Day on Capitol Hill next week, July 24, in the Rayburn House Office Building. The event will be focused exclusively on grid modernization, and many grid researchers, other experts from the labs, as well as myself will be on hand for discussion at a series of exhibits that will highlight much of the work I am discussing today.

Keeping Pace with Cybersecurity

The grid that we know today was designed before we could foresee today's cyber vulnerabilities, and the grid that we evolve to must be resilient to tomorrow's threats. The increasing use of digital technology in our power grid is driving new system configurations, operating strategies, market structures, and business models, but at the same time, increasing our cybersecurity attack surface.

It is paramount that we keep pace with advanced cyber solutions to protect evolving energy systems.

Cybersecurity is not only a top priority for NREL; it is critical to the success of DOE's missions, from maintaining the nation's nuclear deterrent, reducing the threat of nuclear proliferation, overseeing the nation's energy supply, and managing the science and technology powerhouse of the 17 national laboratories.¹

Secretary Perry has identified protection of the energy infrastructure from cyber threats as one of DOE's highest priorities. Across the national laboratory complex, we acknowledge the challenges, opportunities, and responsibility we have to advance the science and technology of cybersecurity to detect, protect, and mitigate against threats to our energy systems.

Sandia National Laboratories has developed SCEPTRE, a cyber-physical environment to analyze how cyber-initiated events affect the physical world. At Argonne National Laboratory, the Dynamic Application Rotational Environment (DARE) rotates web applications across multiple attack servers, allowing analysts to further understand the complexities and intricacies of national security in the cyber realm. Los Alamos National Laboratory is developing technologies designed to defeat today's intrusions into both government and critical infrastructure systems, expanding unique capabilities such as steganography and quantum-enabled security. With Pacific Northwest National Laboratory's cybersecurity test bed, analysts can provide hands-on workshops to teach cybersecurity best practices so that defenders can practice their skills against a safe adversary in a controlled environment. The Idaho National Lab's cybersecurity test bed includes a full-scale transmission loop to assess vulnerabilities and assess impacts on the power grid.

¹ "U.S. Department of Energy Cybersecurity Strategy," 2018–2020.
<https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf>

At NREL, we are developing a virtual environment that will allow us to emulate millions of digital, cloned devices working with physical grid devices, including solar inverters, batteries, and other components throughout our Energy Systems Integration Facility (ESIF) and our Flatirons Campus. In this virtual world, researchers will be able to evaluate the performance of these devices operating simultaneously, while safely launching cyberattacks in a controlled grid environment. Learning to think like an adversary in future grid scenarios will be critical, and it will require the right environment for simulated cyberattacks to highly complex systems.

Protecting Critical Infrastructure

As we have recently witnessed from a multitude of threats across different sectors, malicious actors have demonstrated willingness to employ large-scale cyberattacks, which can be crippling and costly. Reliable power generation keeps our hospitals operating, transportation systems moving, and emergency systems responding, and it provides our homes with power and water.

Stories about cyber breaches to major global companies, government agencies, and electricity systems are becoming all too familiar—such as the 2015 attack on Ukraine’s power grid and the \$10 billion price tag of the malware attack NotPetya.²

Just a few months ago, a western utility in the United States experienced a denial-of-service attack, which caused disruption to grid operations in their region. Although no harm to power generation was reported, the instance led to a temporary loss in visibility to parts of the utility’s SCADA (supervisory control and data acquisition) system.³ Gaining access to a utility’s SCADA system, which is used to manage energy infrastructure, could open the door to multiple substations and other distribution assets.

Directed research is needed in scalable cyber data analysis, advanced encryption, adversary isolation, in-depth assessments, and security for future autonomous systems. In NREL’s expertise of distributed energy systems, the attack surface is increasing around the communications and control of devices, such as rooftop solar, grid-connected vehicles, grid-interactive buildings, and microgrid systems. In the coming years, it will be critical to invest in research capabilities that keep our power systems inherently secure and ahead of cyber adversaries.

The Need for Energy Resilience

With every first line of defense, there must be a second. Alongside the concern for cyber threats, there are other significant sources of disruption to the electric grid—both natural and human—that are just as relevant. These include intensifying weather events, geomagnetic storms from solar flares, and deliberate physical interruption.

² Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *Wired*, August 22, 2018.

³ Bob Sobczak, “Experts assess damage after first cyberattack on U.S. grid,” *E&E News*, May 6, 2019.

When a disruption occurs and energy services are interrupted, we must be prepared to recover quickly. Resilience can be defined as the ability to “prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.”⁴ Energy resilience contributes to the strategic goal of energy security: ensuring sustained energy services with minimal interruptions.

As we have seen from recent storms in Puerto Rico, the Virgin Islands, and other coastal regions throughout the United States, weather alone can interrupt energy systems from multiple entry points and lead to cascading impacts on power systems, water systems, transportation systems, and businesses. We must also be aware of physical interruptions to energy delivery services and the looming potential of an electromagnetic pulse or geomagnetic disturbance event, which could cause a large-scale grid disruption within minutes.

These evolutions give urgency to a better understanding of underlying science and engineering principles that are foundational to designing more inherently resilient energy systems. We need advancements in resilience science—a study of the possibilities for protective and resilient design, and, in the event of a disruption, an effective path to restoring energy services with minimal economic costs and societal impacts. For an in-depth look at the challenges and opportunities around grid modernization, I would call your attention to a study DOE-supported study by the National Academies of Sciences: “Enhancing the Resilience of the Nation’s Electricity System.”⁵

Resilience Through Autonomous Systems

One of the ways NREL is working to strengthen reliability and resilience on the future electric grid is through its research and development into autonomous energy systems—fast-reacting energy systems that are managed through artificial intelligence. These systems could have greater precision and speed than a human-controlled system could ever achieve. For the hundreds of millions of grid devices that are on pace to come online in the coming years, autonomous distributed control appears to offer the most resilient framework.

With highly advanced monitoring and control technologies, autonomous energy systems are being researched for strength against a broad spectrum of threats, even offering resilience against potential threats that we may not yet understand.

The autonomous energy systems platform is built on basic research in optimization theory, control theory, big data analytics, and complex system theory. Unlike current systems that rely on centralized computing platforms for grid control, autonomous energy systems could self-organize and manage themselves.

For an autonomous energy system to perform optimally, it would rely on scalable cellular blocks—essentially variably sized microgrids—that self-optimize when islanded and participate in optimal operation when interconnected to a larger grid. NREL has developed and tested several algorithms that

⁴ “Presidential Policy Directive (PPD)-21—Critical Infrastructure Security and Resilience,” 2013.

⁵ <https://www.nap.edu/catalog/24836/enhancing-the-resilience-of-the-nations-electricity-system>

have advanced the optimization and control of networked systems and significantly reduced the time of the optimization. Scaling these algorithms to a realistic power system is the next line of research.

By furthering our investments to advance innovative solutions like this, we will be better equipped to adapt, withstand, and recover from current and anticipated sources of power disruption.

Adapting to Sustainable Sources With Flexibility

Grid modernization includes building on our existing generation mix, such as natural gas and nuclear, with emerging generation resources. For example, DOE programs are promoting research into more novel resources such as tidal energy⁶ and hydrogen fuel cells. By powering our nation with a mix of energy sources, we can strengthen our energy security and achieve energy independence. But to get there means adapting our infrastructure and markets around energy that includes both centralized power plants and distributed and variable generation.

In Hawaii and California, two states where rooftop solar is extensive, we are experiencing firsthand how consumer and industry-driven growth in new energy resources needs parallel efforts in grid modernization. NREL has supported this energy transition in both states, prominently through our leadership in publishing solar energy's most important standard for interconnection, *IEEE 1547*. Revising this standard, which was part of our GMLC portfolio, has brought consensus across sustainable energy's many stakeholders, ultimately helping the market keep its momentum.

What we have learned from our partnerships with utilities, planning authorities, and product vendors is that there are many angles to adopting a broader energy mix. But above all, we need institutional collaboration and proper planning tools so that strides in sustainable energy technologies are met by a prepared grid and a prepared workforce.

Finding Solutions for Energy Storage

Developing reliable, cost-effective technology to store electrical energy so it can be available to meet demand whenever needed would be a major breakthrough in the existing power grid. The addition of variable sustainable energy sources presents a new challenge requiring continued research.

At solar energy's most productive hours, utilities in California curtail significant energy generated—at times, more than enough energy to power the same distribution system. Likewise, wind gusts do not always correspond to customer electricity demand. How to reserve this energy for later use, whether for emergency backup or efficient day-to-day use, is a priority across both industry and DOE's grid modernization efforts.

As with much of our grid's transition, energy storage is largely driven by private industry. Storage technologies from diverse vendors are entering the grid at both customer and utility scales, with varying

⁶ <https://www.energy.gov/articles/us-department-energy-awards-25-million-next-generation-marine-energy-research-projects>

performance and configuration, leaving a gap in understanding of how storage can best serve our power systems, economically and reliably.

Furthermore, energy storage comes in more than one flavor. Hydrogen and lithium-ion are relevant modes of storage for vehicles, while renewably produced natural gas may function for community-scale storage. A pumped-storage hydropower plant in Virginia has a generation capacity of nearly 3 gigawatts,⁷ while the much drier and sunnier climate of Nevada is better suited for storing solar energy thermally. The federal government can help power system planners across the nation understand how energy storage could fit into their systems.

Growth in energy storage could mean dramatic cost savings and critical importance to grid resiliency—but only if power system operators are well equipped to use storage assets. Hawaii's island of Kauai, for example, has just launched a record-setting "storage plus solar" plant.⁸ But prior to launch, the plant's developer, AES Corporation, needed to arrange the storage for Kauai's grid. Only with NREL's advanced hardware and computing infrastructure was AES able to validate the new plant for Kauai. Similar configuration will be necessary for the many megawatts of energy storage that will soon be coming online.

For an NREL overview of energy storage in grid modernization, see "The Role of Storage and Demand Response."⁹ For a high-level examination of emerging energy storage trends, please see the article "Maintaining Balance: The Increasing Role of Energy Storage for Renewable Integration,"¹⁰ co-written by NREL energy storage analyst Paul Denholm.

Summarizing the Grid's Future Needs

Since the first power lines were installed, our nation's grid has never experienced a transition like the present. Through decades of industry-spanning partnerships at NREL, we have been granted perhaps the best perspective of how our nation's energy system is changing and how we can adapt.

Though many of the technological changes to our grid are being carried by private industry, we identify an important role for government to guide and facilitate the transition, and to do so with respect to our national interests of energy independence and security.

At its core, our future grid must be resilient against threats, both known and unknown. We have the opportunity to shape our power systems to be inherently secure and efficient. We need systems that minimize damage done when events do occur, and systems that use breakthroughs in artificial intelligence and data science to react flexibly and precisely to grid changes. At their foundations, these

⁷ <https://www.dominionenergy.com/company/making-energy/renewable-generation/water/bath-county-pumped-storage-station>

⁸ <https://www.greentechmedia.com/articles/read/aes-completes-its-record-breaking-solar-and-battery-plant-on-kauai#gs.of9dqd>

⁹ <https://www.nrel.gov/docs/fy15osti/63041.pdf>

¹⁰ <https://ieeexplore.ieee.org/document/8070540>

power systems will be adaptable to the complex mix of technologies and energy types that are emerging.

To arrive at such a grid, the nation's future utility workforce will need new tools and training. The growing complexity of the grid will create demand for a dynamic workforce that is up to the task of building, operating, and maintaining future power systems. This pipeline of education and mentorship will need to be complemented by tools for decision support and situational awareness, as well as autonomous systems that can overcome contingency events.

Research into grid modernization needs to be ongoing and based on evolving needs. It needs to match the rapid technical advancements spurred by industry, and the intensity and spectrum of threats that are mounting against power systems. Our nation's next steps in grid modernization could be the most important yet.

I am appreciative of this opportunity to appear before the Subcommittee on a topic of vital national importance, and I look forward to answering any questions you may have.



Juan J. Torres

**Associate Laboratory Director, Energy Systems Integration
National Renewable Energy Laboratory**

Mr. Juan Torres is the Associate Laboratory Director for Energy Systems Integration at the National Renewable Energy Laboratory. In this role, he oversees continuing efforts at the laboratory's Energy Systems Integration Facility (ESIF) to modernize and strengthen the security, resilience and sustainability of the nation's electrical grid. Mr. Torres is Co-Chair for the Department of Energy's Grid Modernization Laboratory Consortium (GMLC), a partnership of 14 national laboratories to advance modernization of the U.S. power grid. In 2018, Mr. Torres provided testimony to the U.S. Senate Energy and Natural Resources Committee on the topic of blackstart, the process of returning energy to the power grid after a system-wide blackout.

Prior to joining NREL in June 2017, Torres served in a variety of technical and management positions throughout his 27-year career at Sandia National Laboratories, most recently as deputy to Sandia's vice president for Energy and Climate programs. At Sandia, Mr. Torres led research efforts and vulnerability assessments in cybersecurity, guided research in advanced microgrid and renewable energy, and led the security and resilience team under the DOE's GMLC efforts. In 2004, Mr. Torres co-led the establishment of the DOE National SCADA Test Bed to secure power grid control systems from cyber attack. In 1998, Mr. Torres served as a member of the DOE task force that developed a national plan to secure the U.S. energy infrastructure in response to PDD-63 Critical Infrastructure Protection. From 1993-1995, Mr. Torres served as Sandia's engineering liaison to the Air Force Materiel Command at Peterson Air Force Base, CO, for development and deployment of mobile command and control systems in support of US Space Command and NORAD missions.

Mr. Torres holds a bachelor's degree in electronics engineering technology from the University of Southern Colorado, a master's degree in electrical engineering from the University of New Mexico, and has completed additional graduate work in Management Science and Engineering at Stanford University.

Chairman LAMB. Thank you. Ms. Speakes-Backman?

**TESTIMONY OF KELLY SPEAKES-BACKMAN,
CHIEF EXECUTIVE OFFICER,
ENERGY STORAGE ASSOCIATION**

Ms. SPEAKES-BACKMAN. Chairman Lamb, Ranking Member Weber, and Members of the Subcommittee, on behalf of ESA, thank you for the invitation to speak today on the role that energy storage plays in modernizing and securing our electric power infrastructure. Energy storage technologies are transforming the way we generate, deliver, and use electricity because it essentially decouples the element of time from when we make it, move it, and sell it. That simple concept enables enormous amounts of capabilities for the grid: Supplying backup power, reducing peak system demands, relieving stressed infrastructure, firming variable generation sources, like solar and wind, and optimizing inflexible generation sources, like nuclear.

Most people think of a battery when they hear energy storage, but there are a variety of technologies, not only different kinds of batteries, like flow batteries, but also mechanical storage technologies, like pumped hydro and flywheels, thermal storage technologies like ice storage and molten salt, and power-to-gas storage technologies like hydrogen and ammonia. Each has its own performance characteristics, and best suited applications, but all do the same job of storing energy for use when and where it's needed most. Storage is uniquely flexible among all resources. It's the only grid resource that operates as both supply and demand in a single asset. I've outlined a lot of reasons in my written testimony, of course, for our claim, quoting my fellow panelist, Katherine Hamilton, that storage is the bacon of the grid, just makes everything a little bit better.

ESA applauds the Subcommittee for incorporating energy storage into its *Grid Modernization Research and Development Act of 2019* to modernize and secure the electric grid. For the remainder of my testimony today, I'm going to outline the recommendations from my written testimony, which are intended to strengthen the effect of the proposed legislation. So in Section 3, Enhancing Grid Resilience and Emergency Response, the proposal to enhance grid resilience is really important, particularly in light of the terrible impact of the increasingly frequent and severe weather events limiting access to electricity. Grants for projects that increase the resilience of electric service with distributed energy resources will speed the ability of communities and local governments to prepare for the next disaster.

It's also important for the Federal Government to use that information that it gathers in this effort to prove the economic case for resilience investment more broadly so that State commissions can measure cost effectiveness, and the private sector can step in when the proposed grant money is spent. To that end, ESA asks the Subcommittee to consider directing DOE to work with stakeholders to develop a method for quantifying the economic value of resilience.

In Section 6, there are a number of commendable provisions within Section 6, Grid Scale Energy Storage, reflecting bipartisan ideas from H.R. 2909, the *Promoting Grid Storage Act*, and H.R.

2986, the *Better Energy Storage Technology Act*, or *BEST Act*. ESA endorses both these bills. The *Promoting Grid Storage Act* would create a competitive grant program at the Department of Energy for State and local governments, utilities, public power authorities, and rural co-ops seeking support for incorporating storage into long-term planning and grid operations. We respectfully request that the Subcommittee include the competitive grant program from Sections 4 and 6 of the *Promoting Grid Storage Act* to accelerate learning through experience, and share that investment responsibility. The *BEST Act* emphasizes DOE investments in demonstrations projects to provide flexibility on intra-day, inter-day, and seasonal basis. Those demonstrations are intended to establish cost and performance targets, which is critical to developing commercialization milestones, but also may pose a risk to innovation unintentionally limiting technology development pathways.

Section 7, in Hybrid—in the Hybrid Energy Systems, we commend the Subcommittee for efforts to drive research and development on storage systems paired with generation. Hybrid systems with storage are relatively new, and we ask in this section that the Subcommittee direct FERC (Federal Energy Regulatory Commission) to seek a report on the current rules on interconnection, market participation, and capacity accreditation of hybrid energy systems.

And finally, in Section 8, Grid Integration, in addition to the RD&D (research, development, and demonstration) programs for integrating the—an electrified transportation system. We recommend adding complimentary RD&D efforts on the re-use of ED batteries for second life applications in charging infrastructure and electric grid service. Re-use for grid applications could lower costs, and could divert still useful assets from recycling or disposal. And so, with that, I thank you for the opportunity to speak to these critical issues, and I welcome your questions.

[The prepared statement of Ms. Speakes-Backman follows:]

Testimony of
Kelly Speakes-Backman

on behalf of the
U.S. ENERGY STORAGE ASSOCIATION

before the
United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Energy

Hearing entitled
**“The Future of Electricity Delivery: Modernizing and Securing our
Nation’s Electricity Grid”**

July 17, 2019



Energy
Storage
Association

901 New York Avenue NW, Suite 510
Washington, DC 20001
energystorage.org

Chairman Lamb, Ranking Member Weber, and Members of the Subcommittee—

On behalf of the U.S. Energy Storage Association (ESA), thank you for the invitation to speak today on the role that energy storage plays in modernizing and securing our electric power infrastructure.

ESA is the national trade association working toward a more resilient, efficient, sustainable and affordable electricity grid enabled by energy storage technologies. With more than 180 member companies, ESA represents a diverse group of power sector stakeholders, including independent power producers, electric utilities, energy service companies, financiers, insurers, law firms, installers, manufacturers, component suppliers and integrators involved in deploying energy storage systems throughout the United States on the electric grid, in homes and businesses, integrated into critical infrastructure and in military installations. We represent a broad technology base that includes electrochemical, thermal, mechanical, process, and pumped hydro storage.

About Energy Storage

Our electric system is bound to a simple reality of physics—supply must precisely match demand at every moment, everywhere. Energy storage technologies are transformative for the electric system because they enable electricity supplied from any source to be saved for use at a later time, precisely when, where, and in whatever form it is most needed. That simple concept enables an enormous amount of capabilities for the electric grid—be it supplying back-up power, reducing peak system demands, relieving stressed grid infrastructure, firming the supply of variable generation sources such as solar and wind, or maintaining optimal function of inflexible generation sources such as nuclear. These capabilities more efficiently ensure that supply and demand reliably match, which in turn optimizes the use of all grid infrastructure and resources. Energy storage is a critical hub of a resilient, efficient, sustainable and affordable energy system.

Energy storage is central to integrating higher levels of variable wind and solar resources. Storage can take excess generation from renewables and store it for later use, avoiding waste and filling gaps in supply; this is increasingly important as renewable penetrations increase and constraints in transmission or distribution systems impede full delivery of wind and solar. Moreover, storage is increasingly being procured in portfolios with renewable power to backfill from power plant retirements. Utilities as diverse as Xcel Energy in Colorado, Nevada Energy, Arizona Public Service, and Hawaiian Electric Company have each planned to procure hundreds of megawatts (MW) of battery storage paired with solar power over the next several years, often to replace retiring fuel-based power plants. And it's not just battery storage—there are over 2,000 MW of pumped hydroelectric storage projects currently pending a license before

FERC, as well as utilities testing and procuring flywheels, thermal storage, and other storage technologies.

Moreover, storage is increasingly critical for reliability and resilience of customer supply, especially in rural areas, island systems and remote communities without a grid connection. Cooperative and public power utilities are deploying storage systems on their grids and microgrids, particularly in remote communities with fuel supply risks such as those served by Cordova Electric Cooperative in Alaska and Kawaii Island Utility Company in Hawaii.

Storage is also increasingly being deployed, often in more rural communities, to increase the capabilities and extend the life of existing grid infrastructure. In using storage this way, grid operators can avoid far more expensive transmission or distribution upgrades, thereby suppressing cost increases otherwise borne by their customers. Utilities like Duke Energy, Eversource, and National Grid are finding innovative ways to extend the life of their wires infrastructure by installing storage, with innovative projects in some cases that integrate both utility- and customer-sited storage assets into “non-wires alternative” investments. At the same time, installing storage at the distribution level increases their hosting capacity, allowing more rooftop solar and electric vehicles to be used on the existing wires.

Most people think of a battery when they hear “energy storage” —and for good reason. Batteries are everywhere—in our phones, computers, appliances, our cars, and increasingly throughout our electric grid. There are a variety of energy storage technologies—not only different kinds of batteries, such as flow batteries, but also mechanical storage technologies (like pumped hydro and flywheels), thermal storage technologies (like ice storage and molten salt), and power-to-gas storage technologies (like hydrogen and ammonia). Each has its own performance characteristics and best-suited applications, but all do the same job of storing energy for use when it is most needed, be that across seconds, hours, or days. In effect, it decouples the element of time from supply and demand.

For the purpose of today’s hearing, I will focus my remarks on the role of battery storage, the fastest growing grid storage technology. Today approximately 2,500 megawatts (MW) of battery storage are installed or under development nationwide, with megawatt-scale installations planned or operating in 29 states. Battery storage technologies—primarily lithium-ion batteries—are declining rapidly in cost, dropping by 50% every 3 to 4 years and projected to continue in the near- to medium-term at 10-15% year over year. Driven by these cost declines, U.S. deployments doubled in 2018, are on track to double again in 2019, and are forecast to triple in 2020, representing over \$3 billion in annual sales in the U.S. by 2021. That sharp cost decline is driving greater performance of battery storage more cost-effectively, increasing their range of applications. The largest battery in the world is currently under development in the

U.S. and will be capable of providing 100 MW of power for four hours—enough to power 50,000 homes through the peak demands of the day. At the same, aggregations of distributed storage installed in homes and businesses are being operated as virtual power plants, with the largest aggregations currently about 20 MW in size—effectively mimicking a small generator.

Storage is uniquely flexible among all grid resources. *First*, storage is the only resource promoting reliability in every part of the grid: co-located with generation, connected to the high-voltage transmission system, placed on the lower-voltage distribution grid, and located in buildings, as well as in microgrids. It is modular and can be scaled to any size, from a home system of a few kilowatts (kW) to a central facility 10,000 times larger. *Second*, storage provides value to all power sector participants: utilities, independent providers, and consumers can all own and operate storage for a variety of reliability services and other cost-saving applications. *Third*, storage is the only grid resource that operates as both supply and demand in a single resource: supply when discharging and demand when charging, giving it the unique flexibility to mitigate oversupply as well as undersupply conditions. *Fourth*, storage is capable of near-instantaneous response and precise control, able to ramp its output to charge or discharge at full power in milliseconds. It is that precise control that allows storage to efficiently provide essential reliability services of frequency response, voltage control and ramping, as well as enhance resilience during sudden disruptions. *Fifth*, storage can provide a diversity of functions for the bulk power system, the distribution grid, and end-users, even providing multiple services interchangeably over time to meet the greatest need in any given moment. *Sixth*, storage can be deployed quickly, with build times for MW-scale installations in less than 6 months. Importantly, storage is agnostic to the supply of electricity, and its flexibility can be used to optimize grid functions for any supply mix, as it changes over time. That's why we call storage the "bacon of the electric grid"—it makes everything a little bit better. Nuclear, coal, gas, wind, solar, hydro, demand response, wires infrastructure and system efficiency: you name it, storage enhances its utilization.

About the Grid Modernization Research and Development Act of 2019

ESA applauds the Subcommittee for incorporating energy storage into its proposed draft legislation to modernize and secure the electric grid. Indeed, storage is being used to enhance electric service reliability & resilience and to increase the capabilities of the existing electric infrastructure.

In Section 3, "Enhancing grid resilience and emergency response," the proposed program to enhance grid resilience is important, particularly in light of the terrible impact of increasingly frequent and severe weather events limiting access to electricity. Distributed energy resources (DERs), including storage, have been critical to the resilience of communities in Puerto Rico,

California, Massachusetts, Florida, and others hit by hurricanes, fires and ice storms. Grants for projects that increase the resilience of electric service with DERs will speed the ability of communities and local governments to prepare for the next disaster. It's also important that, in undertaking this effort, the federal government use the information it gathers to help prove the economic case for resilience investment so that State Commissions can measure the cost effectiveness value when considering rate requests by regulated utilities, and so that the private sector can step in when the proposed grant money is spent. To that end, ESA asks the subcommittee to consider directing the Department of Energy to work with relevant stakeholders in government and industry to develop a method for quantifying the value of resilience. Without a well-defined and broadly accepted valuation method, resilience will remain challenging to fit into the cost-benefit analyses and program designs that ultimately determine whether an energy storage project makes financial sense for a grid operator, a state or local government, a utility or a community.

In Section 6, "Grid-scale energy storage," there are a number of commendable provisions that appear to reflect bipartisan ideas from H.R. 2909, the Promoting Grid Storage Act, introduced by Representative Casten and Representative Bacon, and H.R. 2986, the Better Energy Storage Technology Act introduced by Representative Foster and Representative Herrera Beutler. ESA endorses both bills, and I will try to briefly summarize the key contributions that have garnered our association's and our members' support.

The Promoting Grid Storage Act, which was also endorsed by the American Public Power Association and the National Rural Electric Cooperative Association, would create a competitive grant program at the Department of Energy (DOE) for state & local governments, utilities, public power authorities, and rural co-ops seeking support for incorporating storage into long-term planning and grid operations. This approach is new in that, rather than wait for the federal government to identify desired projects, these local entities would be empowered to identify the kinds of modeling support and grid deployments that will best accelerate their learning through experience, share the investment responsibility and construct a competitive proposal to cost-share those activities.

ESA requests that the subcommittee include in Section 6 the competitive grant program envisioned in the Promoting Grid Storage Act. The current section 6(a)(8) describes a technical assistance program that we believe DOE already has the authority to pursue. To empower local stakeholders to bring projects forward that best overcome informational barriers and lower risks, ESA recommends the subcommittee to incorporate Sections 4 and 6 of the Promoting Grid Storage Act directly into the legislation under consideration.

The Better Energy Storage Technology (BEST) Act, which was also endorsed by the Bipartisan Policy Center, the U.S. Chamber of Commerce Global Energy Institute, ClearPath Action, Citizens for Responsible Energy Solutions, the National Audubon Society, the National Hydropower Association, the Union of Concerned Scientists, and the Information Technology and Innovation Foundation, would emphasize DOE investments in demonstration projects of storage technologies providing flexibility to the electric system on an intra-day, inter-day, and seasonal basis—all of which are increasingly needed in an electric system adapting to higher levels of renewable energy and the demands on the grid of an increasingly electrified economy. Moreover, those demonstrations are intended to put such technologies on a path toward cost and performance targets, which is critical to commercialization. However, it should be noted that legislating the parameters of technology goals can pose a risk to innovation, potentially limiting technology development pathways that will become clearer only after some years of research and development.

ESA requests that the subcommittee therefore give greater discretion to DOE to identify the specific performance targets associated with the energy storage systems in Section 6. In particular, ESA recommends that the legislation specify only a desired service life of storage projects, recognizing that the number of cycles needed will vary according to the duration and application for the storage. Particularly for longer-duration storage, which may cycle less over its total lifetime, prescribing the needed cycle life in statute could eliminate possible technology solutions.

Finally in Section 6, ESA asks that the committee strike the term “grid-scale,” storage, as it can be confusing. Some large commercial and industrial facilities utilize energy storage at multiple-megawatt scale on-site, and their customer-sited *location* does not make them any less important in *scale*. Moreover, energy storage can provide service to the electric grid as a larger, single system or as an aggregation of smaller, distributed systems. For example, New England’s wholesale electric market operator has recently awarded a forward-capacity contract to an aggregation of 20 MW of storage paired with solar power—effectively competing right alongside larger, single systems. To the extent that the subcommittee seeks to use a term of art, “grid energy storage” should suffice without inadvertently confusing the intent of the section.

In Section 7, “Hybrid energy systems,” we commend the subcommittee for efforts to drive research & development on storage systems paired with generation and identify barriers to their use. Many of those barriers remain at the level of the bulk power system, which is in many places under the governance of a Regional Transmission Organization (RTO) or Independent System Operator (ISO). As hybrid energy systems with storage are relatively new, RTOs and ISOs have not yet presented clear rules for how they would operate in the electric system.

Therefore, in addition to the objectives presently in the bill, ESA respectfully requests the subcommittee to consider directing the Federal Energy Regulatory Commission (FERC) to seek a report from RTOs and ISOs on the present rules and processes regarding the interconnection, market participation, and capacity accreditation of hybrid energy systems.

In Section 8, "Grid integration," there are a number of useful research, development, and demonstration (RD&D) programs on the next frontier particularly for integrating an electrified transportation system with the grid. To these ideas ESA recommends adding complementary RD&D efforts on the re-use of electric vehicle (EV) batteries for "second life" applications in charging infrastructure and electric grid service. EV battery capacity equivalent to 100 times that installed on the U.S. grid will be removed from vehicle service globally by the mid-2020s, and a great number of these batteries may still have a power storage capability that is useful for service to the grid—representing a potential low-cost grid integration resource and an environmentally responsible method to divert still-useful assets from recycling or disposal.

In Conclusion

We are at an historic moment where the U.S. can harness energy storage technologies to cost-effectively modernize and secure our electric system. I thank the subcommittee for the opportunity to speak to these critical issues, and I welcome your questions.

Kelly Speakes-Backman
June, 2019

Kelly Speakes-Backman is the first CEO of the Energy Storage Association. Kelly has spent over 20 years working in energy and environmental issues in the public, NGO and private sectors, including United Technologies, SunEdison and Alliance to Save Energy. She is a former Commissioner of the Maryland Public Service Commission where she also served as Chair of the Board of Directors of the Regional Greenhouse Gas Initiative, co-vice chair of the NARUC Committee on Energy Resources and the Environment, and member of the EPRI Energy Efficiency & Grid Modernization Public Advisory Group. She serves on the Board of Directors at the Northeast Energy Efficiency Partnerships and on the External Advisory Board of Georgia Institute of Technology's Strategic Energy Institute.

Chairman LAMB. Thank you. And Ms. Hamilton?

**TESTIMONY OF KATHERINE HAMILTON,
CHAIR, 38 NORTH SOLUTIONS,
AND EXECUTIVE DIRECTOR,
ADVANCED ENERGY MANAGEMENT ALLIANCE**

Ms. HAMILTON. Good afternoon. My name is Katherine Hamilton. I'm the Chair of the firm 38 North Solutions, and Executive Director of Advanced Energy Management Alliance, a coalition of distributed energy resource providers and consumers. Thank you to Chairman Lamb, Ranking Member Weber, and the entire Subcommittee for inviting me to testify before you today.

A lot has changed in the last 2 decades since I last appeared before this Committee. Renewable energy resources are now the cheapest source of electricity, and energy storage is able to cost-effectively replace old fossil fuel peaker plants. Innovation has been instrumental in allowing these resources to efficiently, effectively, and safely integrate into the electric grid. And while innovation continues in the private sector, Federal investment and leadership is crucial to solving many of our most complex puzzles around grid modernization. This Act would provide a great deal of that leadership.

It is appropriate that the first part of the bill focuses on resilience. The need for resilience continues to grow, given increasing storms, wildfires, and other climate-related incidents. Reliability is the percentage of availability over time, while resilience is the ability to recover quickly from a specific situation. Distributed resources, such as micro-grids that can recover quickly from an outage incident, and provide continued service to local communities, will be important to increasing their resilience. In addition to metrics on outage duration, data should be collected on recovery time, costs of downtime, and customer impact. I suggest that a section on risk be developed, mapping out areas at greatest risk from both a physical, as well as an economic standpoint.

Smart grid technology deployments have allowed the grid to operate more efficiently, and with greater visibility. The year of detective work necessary to determine that the Northeast Blackout of 2003 was caused by a branch in Cleveland would no longer be the case, thanks to these technologies. The focus on modeling is greatly needed. Modeling assumptions can determine long-term investment in generation resources that may or may not be necessary, and that are paid for through consumer rate increases. While planning models have improved, most are lacking in considering demand-side resources in the planning process, so customer sided resources, from demand response to solar, energy efficiency, combined heat and power, electric vehicles, all can contribute to the customer not just being a load on the system, but actually becoming part of the resource, allowing the supply and demand sides to become interchangeable.

Technology demonstrations are key to proof of concept, lowering risk and gathering data for innovative solutions. A concept that's been used in other sectors, and to some degree in the utility sector,

is a sandbox, where an area is set aside that is completely free of regulation, and where multiple systems, technologies, and approaches can be experimented with removed from penalty and risk to the utility. Additional experimentation can actually lead to more creative solutions.

Advanced energy storage has grown tremendously, and seen exponentially reduced costs. New technologies have been nurtured and funded at the Department of Energy, including in ARPA-E (Advanced Research Projects Agency-Energy), and continued R&D should test new chemistries and use cases. But instead of identifying this research as grid scale, or prescribing time durations for storage technology operations, I recommend stating the problems that should be solved, or the services delivered, and allow new chemistries and technologies to be developed that fit those needs.

Grid integration is key to understanding how all these systems can interact to multiply the benefits of these innovative technologies for the grid and consumers.

In addition to protecting sensitive grid information and utility security, any standards for consumer or third-party access to consumer data should be reasonable, while ensuring privacy of information. I would caution against being overly prescriptive, and inadvertently stifling innovation, including the very innovation that could mitigate security risk. While these programs are not necessarily designed to reduce carbon emissions, tracking greenhouse gas impact is still useful as we transition to a cleaner energy future, and explore technologies whose greenhouse gas impacts are still relatively unknown.

Finally, I would propose adding a new section to the bill, one focused more on social science. Given the speed of our energy transition, manufacturing and worker transition is lagging. The U.S. should not only be the leading source of entrepreneurship globally, but we should also lead the world in building and deploying new energy technologies. I suggest that research be conducted on how factories can be retooled, power plants repurposed with clean fuels, and workers trained to adjust to new technologies. The U.S. is the global leader on clean and smart energy technology innovation, but to continue on that trajectory, we must sustain our R&D programs in ways that can assist grid operators, utilities, entrepreneurs, our workforce, communities, and consumers.

Thank you again to the Subcommittee for allowing me to testify, and for showing leadership in grid modernization research and development.

[The prepared statement of Ms. Hamilton follows:]

52

Testimony

of

Katherine Hamilton

before the

U.S. House of Representatives

Committee on Science, Space, and Technology

Subcommittee on Energy

July 17, 2019

Good afternoon. My name is Katherine Hamilton. I am the Chair of the firm 38 North Solutions, focused on clean energy public policy, and Executive Director of Advanced Energy Management Alliance, a coalition of distributed energy resource providers and consumers. Thank you to Chairman Lamb, Ranking Member Weber, and the entire Subcommittee for inviting me to testify before you today regarding the Grid Modernization Research and Development Act of 2019.

A lot has changed in the nearly two decades since I last appeared before this Committee. Renewable energy resources are now the cheapest source of electricity¹ and

¹ See article linking to report: <https://www.forbes.com/sites/jamesellis-smoor/2019/06/15/renewable-energy-is-now-the-cheapest-option-even-without-subsidies/#5d4add3f5a6b>

energy storage is able to cost-effectively replace natural gas peaker plants.² Innovation has been instrumental in allowing these resources to efficiently, effectively, and safely integrate into the electric grid. While innovation continues in the private sector--with some utilities, and at our universities--federal investment and leadership in research and development is crucial to solving many of our most complex puzzles around grid modernization. The Grid Modernization Act would provide a great deal of that leadership. I will now go through each section of the draft legislation, offering recommendations for consideration in the final bill.

It is appropriate that the first part (Section 3) of the bill focuses on *resilience*. The need for resilience continues to grow given increasing storms, wildfires, droughts, and other climate-related incidents. While reliability is the percentage of availability over time, resilience is the ability to recover quickly from a specific situation; the definition of resilience will be important to set forth as separate and apart from reliability. Thus, as the bill notes, distributed resources, such as microgrids, that can recover quickly from an outage incident and provide continued service to local communities, will be important to increasing community resilience. I recommend that, in addition to metrics on outage duration, data be collected on recovery time, costs of downtime, and customer impact. I would also suggest that a section on risk be developed, mapping out areas at greatest risk both from a physical as well as an economic standpoint. Technical assistance for resilience should also be available to communities and third party providers, many of whom enter into partnerships to invest in and deploy innovative resilience solutions.

² See story of gas peaker plant replacement here: <https://www.greentechmedia.com/squared/storage-plus/the-puente-saga-changed-the-playing-field-for-energy-storage>

Smart grid (Section 4) deployments of phaser measurement units, dynamic line ratings, capacitor banks, and Volt/VAR Optimization have allowed the grid to operate more efficiently and with greater visibility. The year of detective work necessary to determine that the Northeast Blackout of 2003 was caused by a branch in Cleveland would no longer be the case thanks to these technologies.³ In the smart grid section of the bill, focus is given to modeling, which is greatly needed, based on my experience engaging in Integrated Resource Planning proceedings in states. Modeling assumptions can determine long-term investment in generation resources--that may or may not be necessary—and that are paid for through customer rate increases. While planning models have been improving, most are still sorely lacking in considering demand side resources in the planning process. When I was running GridWise Alliance a decade ago, our vision was a system where the supply and demand sides interacted seamlessly, allowing full participation by consumers of all types to balance more dynamic renewable energy resources on the supply side. Customer-sited resources include demand response, energy efficiency, smart inverters, batteries, thermal storage (from hot water heaters, for example), fuel cells, combined heat and power, microgrids, electric vehicles, and geothermal heat pumps—all of which can contribute to the customer not just being a load on the system, but actually becoming part of the resource, allowing the supply and demand sides to become interchangeable. More complete modeling of these distribution resources, would allow for more holistic planning for utilities and system operators, resulting in a more flexible, cost-effective and cleaner grid. As the grid becomes more dependent on renewable resources, it is important that system planning tools can model a

³ See article on progress over five years here: <https://www.scientificamerican.com/article/2003-blackout-five-years-later/>

complete year of grid operations, hour by hour, so that grid planners can identify the best ways to manage the seasonal impacts of new resources on the grid. In addition, attention should be paid to customer access and inclusion in the system, enabling customers to access their utility data and use it to control when and how they use their energy.

Technology demonstrations (Section 5) are key to proof of concept, lowering risk, and gathering data for innovative solutions. A concept that has been used in other sectors and to some degree in the utility sector, is a “sandbox”, where an area is set aside that is completely free of regulation and where multiple systems, technologies, and approaches can be experimented with removed from penalty and risk to the utility. These sandboxes have been tested in the U.K. and several other countries and to a limited degree in Illinois.⁴ Providing grants to states for additional experimentation could lead to more creative solutions.

Advanced *energy storage* (Section 6) has grown tremendously and reduced costs thanks to state policies, such as in California, requiring utility procurements.⁵ New technologies have been nurtured and funded at the Department of Energy, including in ARPA-E,⁶ although the lack of federal tax credit support has inhibited the industry from reaching full potential in all parts of the U.S. Continued research funding will be needed to test new chemistries and use cases (such as longer duration). Rather than identifying this research as “grid-scale” or prescribing time durations for storage technology operations, I recommend instead stating the problems that should be solved or the

⁴ See article on sandboxes here: <https://www.utilitydive.com/news/experiment-without-penalty-can-regulatory-sandboxes-foster-utility-innov/550950/>

⁵ Additional information on energy storage procurements can be found here: <https://www.utilitydive.com/news/california-looks-to-next-steps-as-utilities-near-energy-storage-targets/525441/>

⁶ ARPA-E runs several energy storage programs: <https://arpa-e.energy.gov/?q=project-tech-areas/storage>

services delivered, and allow new chemistries and technologies—individually or as a system—be developed that can fit those needs. For example, in addition to bulk power storage, I recommend attention be paid to customer-sited storage that can be aggregated into Virtual Power Plants (“VPP”),⁷ providing generation-equivalent resources to the grid. DOE could be helpful on analysis of this VPP potential, modeling of local benefits on the distribution system, and developing business models that include customer participation. The solar industry benefited from DOE R&D on reducing “soft costs”—such as interconnection and balance of system—and the energy storage sector could have similar benefits. Regarding the important topic of battery materials, it should be noted that, while the U.S. has no comprehensive policy on battery end of life reuse and recycling, the technology to recycle lithium-ion batteries exists and is being done today in refining facilities globally.

The *hybrid energy systems* (Section 7) component of the bill is important and is focused correctly. One suggestion would be to incorporate other energy and water nexus technologies in addition to desalination—perhaps to include atmospheric water generation using renewable resources. As with all of these research programs, including private sector entrepreneurs and partners in the equation will enhance development of solutions and results.

Grid integration (Section 8) is key to understanding how all of these systems can interact to multiply the benefits of these innovative technologies for the grid and consumers. Customer-sited resource aggregation (including with electric vehicles), Virtual Power Plants, and Non-Wires Alternatives should all be part of this integration

⁷ See DOE article on Virtual Power Plants:
https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/ABB_Attachment.pdf

portfolio. Non-Wires Alternatives to traditional generation, transmission and distribution resources can be installed to defer capital outlay of new lines and substations, saving utility investment and reducing cost to customers.⁸ One example is the Brooklyn-Queens Demand Management project, where the utility, ConEdison avoided a \$1.2 B substation upgrade by deploying demand response, energy efficiency, and distributed resources.⁹ Additional applications of NWA could be piloted through this DOE R&D program. Experimentation of customer engagement, including through demand response, smart thermostats, blockchain, and other transactive energy solutions, should also be considered. It might also be useful to consider electrification as well as more efficient end use of gas.

In addition to protecting *sensitive grid information* (Sections 9 and 10) and utility security, it will be important to consider consumer data access and privacy. Any standards for consumer or third party access to consumer data should be reasonable, while ensuring privacy of information. While I am not an expert on the cybersecurity portion of the legislation, it is important that all electric and gas utilities—including local distribution companies, transmission/pipeline companies, and generators/producing facilities--meet the North American Electric Reliability Corporation (“NERC”) Critical Infrastructure Protection (“CIP”) standards.¹⁰ I would also caution against being overly

⁸ A collection of case studies of Non-Wires Alternatives projects can be found here: https://e4thefuture.org/wp-content/uploads/2018/11/2018-Non-Wires-Alternatives-Report_FINAL.pdf

⁹ Article about BQDM program can be found here: <https://www.utilitydive.com/news/despite-failures-coned-targets-more-energy-savings-from-non-wires-pioneer/547725/>

¹⁰ Additional information can be found on the NERC website: <https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>

prescriptive and inadvertently stifling innovation, including the very innovation that could mitigate security risk.¹¹

In the section on *considerations* (Section 11), I would add third party solutions-providers, consumers and communities to the list of stakeholder entities for coordination. End users are critical to ensuring that the technologies and experiences resulting from federal research and development will actually work as designed and deliver their intended benefits. I would also recommend that greenhouse gas emission data be collected in all of these programs. While these programs are not necessarily designed to reduce carbon emissions, tracking their impact is still useful as we transition to a cleaner energy future and explore technologies whose greenhouse gas impacts are still relatively unknown.

Finally, I would propose adding a new section to this already substantive bill: one focused more on social science. Given the speed of our energy transition, manufacturing and worker transition is lagging; the U.S. should not only be the leading source of entrepreneurship globally, but should also lead the world in building and deploying new energy technologies. I suggest that research be conducted on how factories could be retooled, power plants repurposed with clean fuels, and workers trained to adjust to new technologies. These activities should be conducted intentionally with public-private partnerships so that the results are realistic and economically beneficial.

As I have witnessed during my co-chairmanship of the Advanced Energy Technology Council at the World Economic Forum, the United States is the global leader on clean and smart energy technology innovation. To continue on that trajectory, we must

¹¹ A potential model for regulation that is designed to evolve with technology is the National Highway Traffic Safety Administration's rules on Automated Vehicles: <https://www.nhtsa.gov/vehicle-manufacturers/automated-driving-systems>

sustain our research and development programs in ways that can assist grid operators, utilities, entrepreneurs, workforce, communities, and consumers. Thank you again to the Subcommittee for allowing me to testify, but, more importantly, for showing leadership in grid modernization research and development.

Katherine Hamilton, Chair, 38 North Solutions

Katherine Hamilton is Chair of 38 North Solutions, a public policy consultancy specializing in clean energy and innovation. Her firm also manages a non-profit organization, Project for Clean Energy and Innovation. Previously, she ran the GridWise Alliance, was policy director to the Energy Storage Association, and served as an advisor for Good Energies, a private equity company with a clean energy portfolio. Katherine directed American Bioenergy Association, developing renewable portfolio standards in states legislatures, including Maryland and New Jersey. At the National Renewable Energy Laboratory (NREL), Katherine worked in buildings research and government relations. Katherine spent a decade at an investor-owned utility, designing electrical systems for commercial and residential developments. Katherine holds degrees from Cornell University and the Sorbonne. Katherine is Co-Chair of the World Economic Forum's Global Future Council on Advanced Energy Technology and is part of The Energy Gang podcase.

Chairman LAMB. OK. At this point we will begin our first round of questions. I will recognize myself for 5 minutes.

Ms. Hamilton, I'd actually like to start where you left off, which is on the need to make sure that we're thinking ahead on the impact of jobs that this transition will have. It will have it whether we like it or not, so, as far as I'm concerned, the question is what are we going to do about it? The whole theme of today's hearing is how are we going to protect? How are we going to protect the grid, make sure that people's power is protected, that their data is protected? But we also have to make sure that their jobs are protected. And I believe we can do that.

There's going to be a lot of hands-on, physical work that needs to be done to adjust our infrastructure, to install new equipment. But I was just hoping you could say a little bit more about what that would look like as a research project. What are some ideas of the type of research we would have to authorize? Who would be doing it, what do we need to know, and when? If you could, is there anything more you can say on that, please.

Ms. HAMILTON. It's a great question, Mr. Chairman, and it's something I think about a lot, because since I was in the utility, the workforce has been aging. Now about 30 percent of the utility workforce consists of Millennials, about 40 percent of the engineers, and Millennials tend to change jobs faster than we used to in the utility workforce. You would start in the utility, and you would retire in the utility.

But people change jobs a lot faster, and there are more types of jobs, so we need to find out what trainings are needed. I think it's important for a research project to look at what are all the skills that we need, and where do we need to source those, and who can do that? What are some of the skills that transfer really easily? For example, a coal worker that is an engineer, or a certified electrician, might transfer really well into energy storage or solar, where an electrician might be needed. So I think there is some of that to be done.

Also in California right now, there are wildfires that are going to cause public safety outages of 30 days or more. I mean, substantial outages, and there are not enough trained tree trimmers to do the work needed on vegetation management. You can't send a kid out with a bushwhacker. This is really trained labor. So there are a lot of job needs and opportunities, and there are people who don't have jobs, and we need to somehow match those. So bringing the public sector and the private sector together on that seems to me to be a good way to think about that.

Chairman LAMB. I think that's correct. Anybody else from the panel want to jump in on that topic? Are you familiar with researchers, or people doing this kind of work who might be able to add to that? OK, we will be sure to look at it on our own. Thank you for raising it.

Ms. Evans, on a kind of similar theme, I noted at the beginning that I think we're short on the cybersecurity workforce, and the jobs that need to be done there. Can you talk a little bit about how our bill, or future efforts we might make, can help us incentivize people to not only go into the areas of cybersecurity, but really to

serve the public the way that you have, and help us protect these assets?

Hon. EVANS. Thank you, Mr. Chairman. There's a lot of work that's already going on in this area that I know you are aware of, under the National Institute of Standards, with the Department of Homeland Security, and with the executive order that just recently was released. So under the categories of cyber, it's always going to increase. It's never going to go away. And also, as my esteemed colleague just described the utility workforce, you're going to have to constantly look at what skillset you're going to need. Right now we're very focused on what I would call the first responders, and those types of skills that you want to have, if you think about it that way, but you also have to build out who are the specialists that are having—if you think about it on a 1 to 10, that is going to have to constantly be looked at as what is the right mix both for the government as well as for private industry.

Chairman LAMB. Thank you very much. And I think with both, you know, and you know this from hosting the Cybersecurity Challenge, or promoting it, I think with both sets of challenges we need to be willing to look deep into our educational pipeline and realize that starting younger people on these projects, and gaining those skills at an earlier age is going to be essential for us to ever get ahead of this. It's a lot harder to retrain someone at an older age—given them confidence that they need to make that transition then if we have people interested in it from the beginning.

So, with that, I will recognize Mr. Weber for 5 minutes.

Mr. WEBER. Thank you, sir. Assistant Secretary Evans, one of the things that makes Texas unique is our islanded grid, ERCOT, that I referred to, it's the Electric Reliability Council of Texas, I know you're aware of that. And it's my understanding that this allows Texas to respond more quickly to cyber and physical—cyberattacks, physical threats, physical events, since they actually operate under one set of regulations, State of Texas, and, of course, they're accountable not to FERC, but to the agency in Texas. In your opinion, are Texas utilities more or less vulnerable because they have that kind of operating system?

Hon. EVANS. I don't know that I want to actually say they're more or less vulnerable. I think that the way that Texas has approached this problem is that they're aware. And, as was mentioned in some of my colleagues' testimonies, where we were talking about shifting more toward risk, that they have the ability to constantly evaluate the risk, regardless of whether it's a physical risk, a cyber risk, or a weather risk. And so it depends on how the mix works, but because of the way they are organized, they can always constantly evaluate the risk.

Mr. WEBER. Right. And you're aware that they're accountable to the PUC of Texas, Public Utilities Commission, as opposed to FERC, and so the State as a whole gets to kind of have control of that grid, one out of nine or eight in the country, and there's kind of a little undetermined area there. So I think it helps them work actually quicker and faster.

And I do want to come back to you too. In your prepared testimony, you said that existing CESER projects and artificial intelligence, AI, and quantum technology also. So how is CESER using

AI to strengthen the electric grid against cyber threats? And I want to give a Part B to that question. The Chairman talked about training people, and we talked about young people going into these different jobs, and changing jobs more often. Is CESER and the Department findings that they can find young people, retain young people, and train people in AI, and hopefully quantum computing?

Hon. EVANS. So I'll take the second part of that question first. We have an education piece associated with what is happening in CESER. We have a competition, which is the CyberForce Competition, that reaches out to all the universities. Several of the labs participate. So that's our outreach, and we are attempting to also work with the labs, as well as us, to then hire directly from the winners. We have a challenge, just like the rest of the government, just like the sector as a whole in this area, so we are working on creative ways through our authorities to be able to do that.

On the other part of the question, as to how we are using artificial intelligence and quantum computing, we have several research and development efforts that are underway, but it is really to try to get it machine-to-machine so that we're elevating the skill level. So things that the machines can do based on how we know attack vectors will happen is built into the technology and into the solutions, and then have those learning capabilities go across our data storage as it relates. So that's the artificial intelligence piece, so that then we can then feed into the intelligence sector.

In visiting the labs, I can tell you that the folks there that are studying under the labs are very interested in how we're going about doing this, so I'm hoping that I can hire them or they hire them.

Mr. WEBER. OK. Well, I appreciate that. Mr. Torres, I want to follow up with you on that. What are you experiencing in that same vein of thought?

Mr. TORRES. OK. With regards to both questions I'll start with the artificial intelligence, and some of the advanced technology concepts. So what we're seeing is the grid is evolving to the point that humans just won't be able to respond quickly enough to all the information that's going to be available to them, so they're going to have to be aided through some sort of computing/artificial intelligence types of technologies. So we are looking into concepts like autonomous systems, where we can incorporate some of the intelligence there to make decisions to maintain reliability, but also we need to do this in a way where we incorporate security from the very beginning, where we assume these systems are going to be targeted. So we are doing research in that particular space.

With regards to the talent pipeline, on the research side, what we are seeing is the pipeline is just not going to be strong enough here long term. We're not seeing enough people continuing into graduate research, their graduate studies, so we see a shortfall in folks with backgrounds in computer science, computer engineering, in electrical engineering, in the power grid. I think I heard earlier from Ms. Hamilton the fact that, you know, most of the workforce in the utility sector, they used to work their entire careers. They don't do that anymore. How can we retain folks in those areas, but also how can we retain the researchers so that we, as a country,

can maintain leadership in these technologies that are going to shape the future grid?

Mr. WEBER. All right. I appreciate it. I'm over my time. Thank you, Mr. Chairman.

Chairman LAMB. Recognize Mr. Lipinski for 5 minutes.

Mr. LIPINSKI. Thank you, Mr. Chairman. Thank you for holding this hearing. Thank our witnesses for their testimony. I wanted to follow up on one of the things that we were just talking about here, is artificial intelligence. I have introduced the *Growing Artificial Intelligence Through Research*, or *GrAITR*, Act, which would provide necessary resources to advance the science of AI and multiple applications, and I know Mr. Torres was just speaking about this, Secretary Evans was just speaking about this. I wanted to ask Mr. Torres, what are some of the research directions that need to be addressed to pursue an autonomous grid, and do you think that the Department of Energy has the resources necessary to pursue the research right now?

Mr. TORRES. I don't think I've done a full assessment to be able to answer the—that full question, but I can tell you about some of the things where I think the Department of Energy can have some impact. There's some foundational aspects to artificial intelligence application to the grid that we really need to develop further.

We have some work going on right now where we're applying AI concepts to the grid, as I mentioned, focused around four—building out four foundational areas that we think are really important. One is complex systems, and understanding complex systems theory, and the second is Big Data analytics. The third is non-linear control. So what we're seeing is with highly distributed systems, some of the linear control concepts that are used now on the grid may not apply in a highly decentralized type of system. And then the fourth area is optimization. How do you really get all of these really complex, highly distributed, where intelligence may be distributed, to work together to achieve some sort of common goal, so that it works as a cohesive system. So there's opportunity to continue to advance some of the foundations to be able to apply AI for the grid specifically.

Mr. LIPINSKI. Secretary Evans, do you have anything you wanted to add there?

Hon. EVANS. Well, what I would like to offer you, sir, is that the Secretary is very committed to AI, and Undersecretary Dabbar I know has really been working on this, so I would like to take it back and get back to you specifically—

Mr. LIPINSKI. OK.

Hon. EVANS [continuing]. About what our AI functions are doing. I know what we're doing in our areas that relates to cyber, but the Department is vast, as you know, so I'd be—

Mr. LIPINSKI. I understand.

Hon. EVANS [continuing]. Happy to get it back to you.

Mr. LIPINSKI. I appreciate that. Well, in addition to AI, everyone, I think, on this Committee, hopefully, knows by now that my interest in always promoting social science research, and the importance of social science research, which sometimes gets short shrift and—with the great importance that it has to fit in with a lot of our other research, so very happy that Ms. Hamilton raised that. Is

there anything else that you wanted to add about what we need to do in integrating social science research into this area that we're talking about?

Ms. HAMILTON. Thank you for the comment. One thing I would just note is that, because I come from the—I come from working with entrepreneurial companies, and innovation has become much more democratized, so innovators are not limited to our labs, our universities, or our utilities. They are everywhere. They're kids in basements playing with their apps, right? So trying to make sure that our research programs are able to connect the dots so that we can bring entrepreneurs to test, and make sure that we have proof of concept, because no utility is going to purchase a piece of equipment that was designed in somebody's basement. They need to know that Department of Energy and the National Labs have given it the seal of approval, and have shown credibility, by testing it, and making sure that this all works.

So I feel like, you know, while part of that is about bringing new people into the industry, because there are so many new excited young people coming in, we also need to make sure that we then connect them to the programs that are existing, to enrich the programs too.

Mr. LIPINSKI. All right. Thank you. Appreciate that. For sake of time, I don't have much, I will yield back.

Chairman LAMB. Recognize Mr. Cloud.

Mr. CLOUD. Thank you, Chairman. Thank you all for being here. Assistant Secretary Evans, I wanted to touch on EMPs (electromagnetic pulse). The commission to assess the threat from electromagnetic pulse attacks warned that a high-altitude EMP would be, they quote, "an existential threat to the survival of the United States and its allies". That sounds pretty ominous. In your written testimony, you mentioned that CESER's working to address EMP risk by sharing knowledge with industry, and developing mitigation strategies. Could you explain to us a little bit of what you're doing to communicate with stakeholders, how the progress is going, what our readiness is at this point?

Hon. EVANS. Thank you for the opportunity to talk about that. The Administration did pass and send out an executive order dealing specifically with EMPs, and so we're leveraging the research that's already there. There's a group that we work with within the National Labs called CSMART, so I'm going to give you the acronym: Center for EMP/GMD Simulation Modeling Analysis Research and Testing. And it involves several of our labs. This—because of that research that was previously done. And so Sandia is at the center, and then we have Savannah River. Livermore is involved, Los Alamos, and Oak Ridge. And then we work with EPRI on this.

And a lot of this is how do we model it, how do we do the validations of some of the things that were in that study so that we can actually work with industry through our ESCC (Electricity Subsector Coordinating Council) work and our oil and natural gas subsector coordinating group and share that research back out with them? There's a debate of whether you need to harden it all the way up to military standards or whether you can take a phased approach and what the impact of that is based on the wavelengths.

And so that research is ongoing, the test beds are being developed. So to the point about being able to validate the technology, and validate the research, that's what we're doing. We intend to accelerate that, provided what happens in our Fiscal Year 2020 budget. And so I know the House passed it, so you guys included the ability for us to do that research, so we're looking forward to continuing that work.

Mr. CLOUD. Are you working or communicating with, like local entities, local governments, power providers, or is it more still in the research vein?

Hon. EVANS. The information that we have to date, and how we work with EPRI, and then how we work with State and local governments, and then through our industry partnerships, and then with the councils, we do convey that out. We also work with the National Governors Association. We work through the associations as well, so the information and the research to date is shared. And then they also know what our project plan is going forward, and then who we are working with in the National Labs as well.

Mr. CLOUD. Are you getting any feedback on what challenges are on the ground, or—

Hon. EVANS. The hardest part is, like, to what level—and I would like Mr. Torres to jump in here, if he feels so inclined—

Mr. CLOUD. Yes.

Hon. EVANS [continuing]. Is how the investment is going to go forward, and how you would harden the different pieces of this. And we have some things that are going on with some of the bigger utilities, and they are sharing that information so that those decisions can be made. And we also work with FERC on this as well, and then FERC also then reaches out and shares the information too, because this becomes an investment decision, and then it'll inform the standards decisions going forward with FERC.

Mr. CLOUD. OK. Any of you want to speak to that as well?

Mr. TORRES. So I totally agree with everything Assistant Secretary Evans said there. There is an element of the energy that's released during an EMP that's very similar to a GMD, geo-magnetic disturbance, event, so that's something that we need to take into account as well, that actually is probably more likely than an EMP event. It's maybe higher probability, but also some severe consequence.

I think it does need a little bit more study. EMP has been studied for quite some time by the commission that's formed, and reformed, and so on. But I believe the—I would suggest that we take maybe a forward-looking spin as we think about EMP. I think a lot of times we're looking at how do we harden the grid of today against EMP. The grid we have in 10 years will not look a lot like today. It will change. There are a lot of things going on right now and—where it's become more distributed, the generation mix, and so on. So we need to do some analysis, and project how would we harden the grid of the future?

Mr. CLOUD. Thank you.

Chairman LAMB. Recognize Ms. Horn for 5 minutes.

Ms. HORN. Thank you, Mr. Chairman, and thank you to our witnesses and Mr. Ranking Member for holding this important hearing today. As I'm sure, with many of us across this country, but

also on this Committee—I also sit on the House Armed Services Committee—and especially given, Mr. Torres, what you mentioned about the blackout, and where we’re talking about this, we are very concerned about our electrical grid and our infrastructure as a national security issue on a broader level, as well as looking forward as an infrastructure issue.

So I’d like to start, Secretary Evans, with you today, if we could. So we know we have significant work to do, but I’m glad that you’re doing this work. You mentioned in your testimony talking about the national imperative, and the *Cybersecurity Research Development Act*, cybersecurity being one of the major threats. I’m curious to hear how you would assess the current state of our grid cybersecurity efforts, and what additional things those of us on the Committee can do to help bolster those efforts?

Hon. EVANS. I want to echo some of the comments that my esteemed colleague just mentioned about looking for the grid of the future. So there is a robust mechanism that we have as a sector specific agency going forward, but also with the whole government approach that we take with our partners, like Department of Homeland Security, Transportation, depending on what we’re looking at. But when we talk about the cyber threat, and how it continues to evolve, what we really need to do is look at where we’re going to be in the future and how is that mix going to be.

And then, based on the risk modeling, which has already been talked about, I’d like to bring up again the North American Resiliency Model that takes into consideration, along with what DHS is doing from the National Risk Management Center, the ability for us to be able to take the work that’s coming from the National Labs, model it, and be able to give you a databased-type-of decision, data informed, based on where we are. How can we project this out into the future? What is the mix going to look like? How is the weather on that? So when we talk about that in the research that we’re doing, again, I applaud what the Committee is doing to be very forward leaning into what do you think, and how research should be 10 to 15 years from now on that grid of the future.

Ms. HORN. Thank you. And continuing on the resiliency model, I want to turn attention to Ms. Speakes-Backman, especially when we talk about storage and generation. I represent Oklahoma, which is well known, of course, as an oil and gas State, but we also have a robust collection of renewable energy that is growing. In fact, 39 percent of the energy we produce is through renewables, but we know that the challenge is storage.

So, looking at the technologies as they’re evolving, beyond batteries, and where we are for the resiliency factor, I know, speaking with our utilities providers, one of the challenges, as we diversify our energy sources, is ready access beyond just the cyber issues and the other security issues. So can you speak to where we are on developing some of these other technologies to make them accessible beyond batteries?

Ms. SPEAKES-BACKMAN. Thank you for the question. So Oklahoma specifically does not have battery storage necessarily installed, but there’s about 259 megawatts of pumped storage in the State, so we congratulate you on that. In terms of other technologies, of course, pumped storage is a very mature technology.

It's installed—it dwarfs the amount of capacity that's actually installed in the United States currently, when you think about pumped hydro storage as well.

Other mechanical storage technologies, like flywheels, are being used in shorter-run, high-power applications. There's compressed air, and liquid storage—liquid air storage, and other mechanical systems that are in some demonstration levels right now. There are thermal storage technologies. Even when you think about building being—buildings being a thermal storage opportunity, but—water heaters in your home, there are a number of State programs that encourage water heaters and demand response that help—that is also a level of storage. And those, of course, technically are very advanced, just not used as much in the grid applications as well as they could be.

There's other—also molten salt storage technologies, and other grid-side technologies that are promising, but are yet to commercialize, but the progress has been made on those as well.

Ms. HORN. Thank you very much. Mr. Chairman, I yield back.

Chairman LAMB. Mr. Biggs for 5 minutes.

Mr. BIGGS. Thank you, Chairman Lamb, and Ranking Member Weber, for holding this important hearing. Thanks to all of you panelists for being here with us today. The U.S. relies on a robust cybersecurity front to keep our critical infrastructure, including delivery systems, safe, and I'm pleased that the President and his Administration have made cybersecurity a priority. President Trump's national cybersecurity calls for the development of a superior cybersecurity workforce. This strategy states that, "a highly skilled cybersecurity workforce is a strategic national security advantage," and I agree with this assessment.

Nearly 2 years ago, I had the opportunity to moderate a panel at an Arizona State University (ASU) cybersecurity conference, and we focused on education and workforce in this area. The panel included cybersecurity professionals representing ASU, PayPal, McAfee, Network Command at Fort Huachuca, and the National Institute of Standards and Technology. And the main issue was raised on how some of you have addressed this, on the cybersecurity workforce shortage that this country's facing.

The Center for Strategic and International Studies reported that the U.S. was facing a shortfall of almost 314,000 cybersecurity professionals as of January 1 of this year. And I think it's important that we work to encourage a free market, non-intrusive solution to develop a cyber workforce capable of managing not just the threats of today, but anticipate the threats of tomorrow, particularly in the energy industry. So I'm going to start with a question that I want to give each of you a shot at answering, and then I do have a couple more questions, so if you can help me out by being as concise, yet as informative, as possible. How do you think government can become a better partner with higher education institutions and industry to form an education pipeline that will actually meet our cybersecurity workforce needs to keep our electric grid safe? So I guess we'll start with Ms. Hamilton on this side, and then go my right to left, your left to—

Ms. HAMILTON. OK.

Mr. BIGGS [continuing]. Your right.

Ms. HAMILTON. I'll be really quick, because I'm not a cyber expert, but just on education, I think you need to start much younger than that. We need to have it in our—in all of our elementary schools too to try to get people—kids interested in doing this too. So I think having public-private partnerships are important, making sure that you bring in—so maybe you'll bring in some teachers who are science teachers bringing in—whether it's from a university or middle school to try to—

Mr. BIGGS. And not to interrupt, but are you talking about specifically STEM (science, technology, engineering, and mathematics), or computer—

Ms. HAMILTON. Well, STEM—

Mr. BIGGS [continuing]. Coding—

Ms. HAMILTON [continuing]. And also just—if you're interested in specific—

Mr. BIGGS. OK.

Ms. HAMILTON [continuing]. Cyber, get kids interested in that too, really.

Mr. BIGGS. Great. Thank you.

Ms. SPEAKES-BACKMAN. I'm also not a cybersecurity expert, but I'm really thrilled that my 15-year-old twin girls are here in the audience hearing this, because their high school has a program that is partnered with the U.S. Naval Academy specifically on cybersecurity, and I really want them to take it, so—

Mr. BIGGS. OK. Are these your daughters, you say?

Ms. SPEAKES-BACKMAN. Yes.

Mr. BIGGS. Please raise your hands so we can put pressure on you publicly.

Mr. WEBER. No pressure.

Mr. BIGGS. Thank you. We're helping out. Mr. Torres?

Mr. TORRES. So I would concur with my colleagues here. It's important to really spark that interest in STEM fields early. The other thing is I think we need to provide mentoring, because it's not just getting the workforce out there, it's getting the future teachers, and getting the future professors. And this is back to a point I made earlier, which is the fact that we need to continue to get people to advance their education, and it's—and be the mentors, and mentor the future teachers, as well as the future applications.

Mr. BIGGS. Thank you, and, I'm sorry, I'm going to skip you, and maybe we can have a one on one dialog later, because I have to ask this other question, which intrigues me, because Mr. Torres has repeatedly talked about what several of you have talked about the future grid, or what the grid looks like in the future, and it's really tough to be clairvoyant, obviously, but I am wondering what your thoughts are on the role that microgrids might play in making the grid more resilient. And what does the microgrid of the future—what might that look like? And, Mr. Torres, since you've talked about future grids, we'll start with you.

Mr. TORRES. So, just to make sure everybody's on the same page, a microgrid, basically—the way—a simple way to define it, there are formal definitions, is essentially a grid that has its own generation, its own wires to move the electrons, and its own loads to use those electrons. It connect—can connect and disconnect from the

larger utility grid. So I believe they do have their role. They don't need to be used everywhere.

I foresee that the future grid will be some sort of a hybrid of a centralized grid base, with some decentralized microgrids, especially for critical loads. We've seen that they've been very applicable where you have military installations, highly critical loads like hospitals, some key industrial areas, and so on, that may have a lower reliability connection to the utility grid, and where you may have some very sensitive types of load, sensitive to perturbations and disturbances in the grid. So you really need to right fit it and right size it. It's not a ubiquitous solution.

Mr. BIGGS. OK. Unfortunately, my time's expired. Thank you.

Chairman LAMB. Thank you. Mr. McNerney.

Mr. MCNERNEY. Well, I thank the Chairman for holding the hearing, and I thank the panelists. Really a very interesting area, and very important. But I want to start with a shout out to the Grid Innovation Caucus that I co-Chair with my colleague Bob Latta from Ohio. The purpose is to discuss policy and technology, but also to help educate Members of Congress, and to get people excited about this issue here in Congress, because it's important, and we need to move forward on these things.

Assistant Secretary Evans, we've heard a lot about artificial intelligence and how important its benefits are, including in the context of grid modernization and security. What role do you think AI can play in improving the resilience of our Nation's electric system?

Hon. EVANS. I think it has a critical role. Mr. Torres already highlighted some of the specific things of what we're talking about going forward, and really looking at software-defined networks, autonomous solutions, really analyzing the data, taking the things that we know are going to happen, and try to remove some of what is happening at a human level now that could be done by artificial intelligence, by machine learning. And that is the area that we are really exploring so that we can then look at higher analysis of security. And then also the resilience, of being able to model the resilience in real time.

Mr. MCNERNEY. Well, is there a significant risk that adversaries could use AI to attack our system?

Hon. EVANS. For every great new innovation that we do, and I believe Mr. Torres also highlighted this, is that we also then have to evaluate what are the potential risks associated with that, and then engineer preventative solutions for problems that we know of could happen as we deploy those out. So that's the longer answer to yes, we could do that, but we don't want to stifle innovation. We want to take advantage of those things and be able to use them, but also then make sure we have the right mitigations in place.

Mr. MCNERNEY. Well, I mean, those sorts of attacks are going to happen whether we deploy AI or not, so—

Hon. EVANS. So we—yes.

Mr. MCNERNEY. Mr. Torres, do you want to comment on that?

Mr. TORRES. I would concur with Assistant Secretary Evans. I guess I would add to it the fact that, you know, just about any tool, any weapon, can be used for good or for bad, and so this is why it's very—it's an imperative for us to maintain that leadership in the advancements of these technologies, so we are the ones that are

using these for the right purpose, and can actually deter any negative use, or any attacks on these systems.

Mr. MCNERNEY. Well, Mr. Torres, I'm concerned about the attack on March 5 on the SCADA system. There wasn't much damage done, but what would be the potential damage if attackers had access to the system, real access?

Mr. TORRES. And the attack that you refer to was, I believe, a denial-of-service attack on the SCADA system of a utility out west. And my understanding is that it basically blinded, or the operators lost—may have lost control or visibility from some of the devices, so the attack was on the SCADA system, which—supervisory control and data acquisition system—is used to monitor and control elements of the power grid. So if somebody were to gain access, they could potentially disrupt operation of the grid, and maybe even cause the operator to make a mistake in operation.

Mr. MCNERNEY. Well, with all behind-the-meter devices and distributive resources, we're facing increasing risk here, right?

Mr. TORRES. There's a potential to increase the attack surface as we add more devices near the end user. So this is where we do—I believe through the CEDS (Cybersecurity for Energy Delivery Systems) program at DOE, under Assistant Secretary Evans, we do have a road map to essentially secure the connectivity down to the meter, essentially, so that we try to minimize the risk back upstream to the utility.

Mr. MCNERNEY. Thank you. Ms. Speakes-Backman, what site-specific geographic considerations are important to consider when deciding what type of energy storage system is the most appropriate for a particular location?

Ms. SPEAKES-BACKMAN. Well, certainly—thank you for the question. Certainly there are geographic considerations when it comes to pump storage, hydro storage especially. Underground—you need large expanses of underground. But when you're talking about battery storage specifically, that can be scaled to behind peoples' meters in the home, it can be—at grid scale, it can be in commercial industrial applications. The biggest considerations that are necessarily—that are not necessarily having to do with the technology itself, in terms of its capabilities, but the application that you're going to be using it for.

So when you need to be in rural communities, when co-ops are needing to use energy storage to offset the cost of transmission upgrades and distribution upgrades, then you'll want to use a specific type of battery, or other technology, that can be longer duration. When you're talking about being up in the northeast, you need a longer duration storage type application for weeks—hours, weeks, even months, when it comes to wintertime issues.

Mr. MCNERNEY. And the cost goes up pretty dramatically after a couple hours of—

Ms. SPEAKES-BACKMAN. Yes, it can.

Mr. MCNERNEY [continuing]. Usage of a storage system? I yield back. Thank you.

Chairman LAMB. Mr. Casten for 5 minutes.

Mr. CASTEN. Thank you, Chairman Lamb. Thank you so much to our witnesses for being here. As we consider how to get to a low, or hopefully zero, carbon future, we are increasingly constrained by

how to have a flexible enough grid that can accommodate these intermittent sources of power that fluctuate out of phase with where the load is. It is a really important, really critical issue, and I am delighted to see this Committee thinking seriously about those issues. We have a lot of ways we have to solve that. We can solve that through market mechanisms and transmission, but I believe that chief among those has to be grid scale energy storage. And that's why I was proud to introduce H.R. 2909, the *Promoting Grid Storage Act of 2019* (PGSA). And I want to thank Ms. Speakes-Backman, and the folks at ESA, for their support of H.R. 2909.

One of the most important aspects of that bill is the creation of a competitive grant program for energy storage at the DOE, funded at \$150 million over 5 years. The competitive program is unique in that it would empower local entities to identify specific demonstration projects and compete for funds at DOE, instead of waiting for the DOE to identify specific projects to fund. Ms. Speakes-Backman, are you aware of any competitive grant programs for energy storage specifically at DOE, or, for that matter, anywhere else across the Federal Government, that currently operate like the program put forth in Section 6 of the PGSA?

Ms. SPEAKES-BACKMAN. Not specifically of that type, and that's why we've been so strong in our support of the *Promoting Grid Storage Act*, because not only does it allow the market to participate in the selection of these types of projects, but it also puts skin in the game. So the market participants are also participating, and putting their own business risk at this, so we think it's going to accelerate the demonstration project success.

Mr. CASTEN. Well, you've thankfully answered my second question as well, of why that structure was helpful, so I appreciate that. In your opinion, does the *Grid Modernization Research and Development Act of 2019*, in its current form, do enough to empower local stakeholders to bring demonstration projects forward that best overcome these informational barriers and lower the risks?

Ms. SPEAKES-BACKMAN. It goes pretty far, and we're really excited about this potential, but there are a number of things, as outlined in my testimony, that can be done to further this. One of them I think is very important is—you had the conversation about resilience, and it is to support the—for DOE to support the investigation into how States can prove out cost effectiveness for resilience. This is an issue that I personally had after the Derecho in 2011, where States can—States—sorry, utilities can invest in reliability, and there are metrics for that, but they cannot invest in resilience, because there aren't the correct metrics to—of that to prove cost effectiveness. I think that's an important part of it. The other part is, really, Section 4 and Section 6 of the *Promoting Grid Storage Act*, I think, could be included in this particular draft legislation, to be so helpful.

Mr. CASTEN. Well, thank you. And again, I'm really excited by the Committee's work on the *Grid Modernization Act of 2019*, but I am concerned that the—in its current form, it doesn't do enough to facilitate demonstration of energy storage technologies. And don't get me wrong, R&D and technical assistance are really important, but without efforts to further de-risk those technologies, I'm

concerned that the rate at which they're adopted by utilities, by cops, municipalities, will be too slow for the scale needed to combat the climate crisis. I, you know, I live in Illinois, and you can see in the data—we started to see an increase in CO₂ emissions because we are deploying so much intermittent energy—

Ms. SPEAKES-BACKMAN. Um-hum.

Mr. CASTEN [continuing]. And now we're installing—because it's so hard to site transmission, we're installing really inefficient, but quick-ramping, gas generation. And we can solve that with storage, but we've got to get it out there.

Ms. SPEAKES-BACKMAN. Yes. I—just to add a comment, I completely agree with you, in the fact that energy storage is really going—the only—the major delay in having this deployed on a major scale is really about how it fits within the regulatory construct, and how it fits within the energy grid integration itself. It's really more of a commercial question that's happening more than a technology question. I think the technology's ready to go.

Mr. CASTEN. Well, thank you very much. I'm about out of my time, but I really appreciate your testimony, and I hope I can persuade the Chairman to work with me to help strengthen the bill as it pertains to the demonstration of energy storage technologies. And I yield back.

Chairman LAMB. Thank you. Mr. Foster.

Mr. FOSTER. Thank you. Actually, my colleague just mentioned the difficulty of citing, you know, power lines, and the two components of that. Well, there's a big NIMBY (not in my back yard) difficulty that's much worse as you approach cities, but bad probably everywhere. The obvious solution to that's to bury power lines, and that is hellishly expensive presently. How extensively have people looked into just robotic assembly, you know, of underground power lines? Is there really any hope to make a big dent in the cost? Are there technological approaches that might really lower the cost of buried power lines, or has that pretty well been mined out already? Anyone familiar with any big initiatives that have ever been tried along those lines?

Ms. HAMILTON. I think you're still going to have the issue of NIMBY-ism. You'll still have the issue of having to get either eminent domain or permission, and permitting from folks as you put them in, so you'd want to look for other kind of rights of ways, whatever the technology—

Mr. FOSTER. Right, but for buried power lines it's orders of magnitude easier if you don't have to look at them. You know, those that believe cancer is caused by electric power lines, you know, if you can't see the line, that seems to bother them less, and so on. So it's a, you know, so that, you know, it strikes me that that might actually, you know, if there is money to be squeezed out of the cost of buried power lines, that might be a good Federal R&D and demonstration initiative.

The other one is something that would be a legal mechanism. You know, there's a well-documented drop in the real estate prices near high voltage power lines, you know, for partly rational and partly irrational reasons. It's a documented fact. So the question is whether some sort of assessment on those nearby, you know, for example, if there's an existing right of way, and now it comes time

to actually build the power line, you know, there's typically a big outcry, even though it's an established, documented right of way that people said, I didn't realize this when I bought my house, and now they're going to look at, you know, the rational part of that, as their real estate values are going to drop if the power line's actually put in. And then, of course, there's an irrational thing, they don't—or maybe it's rational or not, that they don't like looking at the power line.

So if there was a legal framework that allowed those who are affected, in terms of real estate value and impact, to contribute to burying the power line, then there may be, you know, I'm not sure exactly what that would look like, whether we're going to build this power line, it's going to be expensive, but part of the real estate appreciation that you will see, if you take an existing power line, say, and bury it, that will cause everyone's real estate value to rise, and capturing a part of that rise to pay for burying it, that there may be a social contract that's a win all the way around, particularly as the power lines approach cities.

Anyway, but you're unaware of things like this? Because hardening the grid by, you know, putting things like a DC overlay are, you know, very good ideas in principle, and you have to get past the difficulty in citing power. So there may be some opportunities for probably Federal law to enable that sort of a deal to be struck with the surrounding communities. Anyway, I'd just make a couple of comments on the *BEST Act*, another piece of legislation that I've introduced as well, having to do with—just encouraging energy storage R&D and demonstration projects, and I guess that's probably been pretty well discussed, I presume, and my apologies for having to jump back and forth between this and the Facebook Libra hearings. But is there anything that has not yet been settled on those lines that might be worth mentioning?

Ms. SPEAKES-BACKMAN. Well, I'd just like to add that ESA, and a number of other associations, have strongly endorsed the *BEST Act* as an excellent opportunity.

Mr. FOSTER. Yes. And we have partners in the Senate. I think there's a good chance that it's actually the, you know, one of those rare combinations of things that is going to have a chance at getting through the legislative graveyard that we're trying to populate as best we can in the House these days, but that may be an exception to that.

Ms. SPEAKES-BACKMAN. We have hopes for a number of energy storage pieces of legislation, including the *BEST Act*, and including the—sorry, the storage—standalone storage ITC, and a number of other pieces that—

Mr. FOSTER. Yes.

Ms. SPEAKES-BACKMAN [continuing]. We think could get through.

Mr. FOSTER. Let's see, the last thing, in my last 3 seconds, when you look at advanced nuclear technologies, some of them have the ability to essentially add storage to, you know, for example, molten salt reactors have the ability to put a molten salt tank nearby, if that's used as the coolant, so that you could effectively have the ability to—if you have excess generation capacity, this traditional knock against nuclear is that it's only worth running at a flat level. You could actually spike it up if you had a big storage tank, and

excess generation capacity. And is that being factored into the modeling, and the cost incentives, when people look at advanced nuclear, that some techniques have this, and others don't? Again, there's, you know, been a lot of discussion in the Department of Energy about trying to incentivize techniques that had storage capacity of some kind.

Ms. SPEAKES-BACKMAN. Well, I can't speak to what's being counted in and—not for the nuclear side, but I can say for energy storage, and the various technologies, that this is one of the things that we're asking from DOE, and DOE has been actually doing some work on, is the evaluation of the various applications for energy storage, that it flattens out, and indeed increases the efficiency of the grid overall.

Mr. FOSTER. Yes. All right. Well, I guess I'm well over time now, so I'll yield back the—my negative balance of time.

Chairman LAMB. Thank you. Before we bring the hearing to a close, I want to thank our witnesses again for appearing before us today, and sharing such great information. The record will remain open for 2 weeks for additional statements from the Members, and for any additional questions that the Committee may have for the witnesses. The witnesses are now excused, and the hearing is adjourned. Thank you.

[Whereupon, at 3:24 p.m., the Subcommittee was adjourned.]

Appendix I

ANSWERS TO POST-HEARING QUESTIONS

ANSWERS TO POST-HEARING QUESTIONS

Responses by the Honorable Karen Evans

House Committee on Science, Space and Technology
“The Future of Electricity Delivery: Modernizing and Securing our Nation’s Electricity Grid”
Questions for the Record Submitted to the Honorable Karen Evans, Assistant Secretary,
Office of Cybersecurity, Energy Security, and Emergency Response

July 17, 2019

QUESTIONS FROM CHAIRWOMAN EDDIE BERNICE JOHNSON

Q1. To capitalize on the promise of a secure and modernized grid, voluntary, consensus-based standards, such as those on interoperability, could simplify new equipment selection and installation and enhance the overall security of the grid.

Q1a. What is the current role of DOE in developing voluntary, consensus-based standards in this space?

A1a. The Department of Energy (DOE) works with both the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation to understand threats to the energy sector, so they can make risk-informed decisions regarding standards. For example, on March 28, 2019, DOE hosted a joint technical conference with FERC 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.

DOE’s Office of Cybersecurity, Energy Security, and Emergency Response works closely with the Department of Commerce’s National Institute of Standards and Technologies (NIST) to support standards development. NIST is responsible for the development and maintenance of cybersecurity standards for the smart grid. NIST is fulfilling its responsibility, under the Energy Independence and Security Act of 2007 (Title XIII, Section 1305), to coordinate standards development for the smart grid. NIST solicits input and cooperation from private and public-sector stakeholders in developing cybersecurity standards. DOE also works closely with the three energy sector information sharing and analysis centers (ISACs)—the Electricity ISAC, downstream natural gas ISAC, and oil and natural gas ISAC—to share best practices, threat-related information, and training initiatives. These activities help DOE promulgate cybersecurity practices that go above and beyond the standards.

House Committee on Science, Space and Technology
"The Future of Electricity Delivery: Modernizing and Securing our Nation's Electricity Grid"
Questions for the Record Submitted to the Honorable Karen Evans, Assistant Secretary,
Office of Cybersecurity, Energy Security, and Emergency Response

July 17, 2019

- Q1b. Is there any funding available to help develop voluntary, consensus-based standards collaboratively between DOE and industry stakeholders?
- A1b. DOE is in the process of updating its Cybersecurity Capability Maturity Model (C2M2) tool that aligns to the NIST Cybersecurity Framework. DOE's C2M2 is another tool used by industry to review their own cybersecurity practices across multiple domains and then make informed decisions to improve policies, procedures, and technologies.

*Responses by Mr. Juan J. Torres***House Committee on Science, Space, and Technology****"The Future of Electricity Delivery: Modernizing and Securing our Nation's Electricity Grid"**Mr. Juan J. Torres, Associate Laboratory Director, Energy Systems Integration,
National Renewable Energy Laboratory

Response to questions submitted by Congresswoman Eddie Bernice Johnson, Chairwoman, Committee on Science, Space, and Technology

Q1: To capitalize on the promise of a secure and modernized grid, voluntary, consensus-based standards, such as those on interoperability, could simplify new equipment selection and installation and enhance the overall security of the grid.

- a. **Do you believe the government has a role to play in developing voluntary, consensus-based standards, or should that be left to industry?**

Response:

Open industry standards are critical to grid modernization because they incentivize and accelerate effective interconnection and interoperability of new devices as they are brought to market. Without standards, we would have a patchwork of unique technological solutions and devices that do not work together and are more expensive to deploy and maintain. One effective example is the growing family of Institute of Electrical and Electronics Engineers (IEEE) 1547 standards for integrating distributed energy resources.¹

IEEE 1547 has been referenced in federal legislation and rulemaking, state regulatory deliberations, and utility engineering practices and interconnection agreements. IEEE 1547 was cited in the U.S. Energy Policy Act of 2005² as the model for interconnection services. Eighty percent of state public utility commissions in the United States have leveraged IEEE 1547 in promulgating regulations for their own states. These standards have simplified the integration of high levels of distributed energy resources into the U.S. electric power grid. This U.S.-driven standard also has international market impact, which can accelerate technology deployment and benefit industry. For example, IEEE 1547 requirements have been adopted to varying degrees in Germany, Japan, and Korea.

One challenge with market-driven standards is that vendor participants may attempt to influence the direction of a standard to block competitors from a market or to gain competitive advantage for their respective products. Government can play a beneficial role in standards development by serving as a technical expert in new fields and as an objective, unbiased participant that can level the playing field, especially in development of new markets that could impact our economic or national security.

- b. **What is the current role of DOE in developing voluntary, consensus-based standards in the space?**

Response:

Standards and codes are perhaps the best leverage we have in advancing research into practice. We believe that as a final step, our research advancements should be institutionalized as standards.

While we defer to the U.S. Department of Energy (DOE) regarding their broader role in this area, we can describe how national laboratories, and the National Renewable Energy Laboratory (NREL) in particular,

¹ http://grouper.ieee.org/groups/scc21/1547/1547_index.html

² <https://www.congress.gov/bills/109th/congress/house-bill/6>

House Committee on Science, Space, and Technology
"The Future of Electricity Delivery: Modernizing and Securing our Nation's Electricity Grid"
Mr. Juan J. Torres, Associate Laboratory Director, Energy Systems Integration,
National Renewable Energy Laboratory

support industry standards with DOE support. NREL staff conduct technical research to support the development of standards and help coordinate between different projects related to data standards, but staff generally are not involved in certification or compliance of equipment. NREL works on many standards in the technology space—solar, wind, buildings, and so on. Some examples with the International Electrotechnical Commission include photovoltaic system availability and reliability (IEC 63019) and operations and maintenance (IEC 62446). NREL staff also support standards development as members of technical teams led by standards-making organizations, such as the American National Standards Institute and IEEE. Examples include IEEE 1547 standards on grid interconnection and IEEE 2030 on smart grids.

In partnership with Sandia National Laboratories, NREL has produced a set of documented testing procedures that will be used by Underwriters Laboratory (UL) to establish a standard and a certification program for the distributed energy resource market. Once established, this UL standard and certification will drive manufacturers/vendors of distributed energy resource devices to certify their products before selling to utilities and other stakeholders. NREL is working with utilities to establish an IEEE 1547.3 working group that will develop a cybersecurity guide for distributed energy resources interconnected with electric power systems. Utilities will use this guide to develop requests for proposals that will ensure procured devices have a reasonable cybersecurity posture based on the UL standard and certification.

Responses by Ms. Kelly Speakes-Backman

901 New York Avenue NW, Suite 810
 Washington, DC 20001
 p.202.293.0537

September 16, 2019

██████████
 Subcommittee on Energy
 U.S. House Committee on Science, Space and Technology
 Transmittal by email: ██████████

Dear Ms. Wright,

Thank you for the opportunity to speak to the Subcommittee on Energy at the July 17, 2019 hearing titled "The Future of Electricity Delivery: Modernizing and Securing Our Nation's Electricity Grid." Please find below my responses to the Subcommittee's questions in follow up to that hearing.

Q1. Effective public-private partnerships can help reduce costs for taxpayers by accelerating development of relevant technologies.

- a. How do you think stronger partnerships between the DOE program offices and industry would be helpful to your members?*

Public-private partnerships between the Department of Energy (DOE) and the energy storage industry are critical, for ensuring that business experiences inform technology R&D pathways and for enabling better dissemination of federal R&D outcomes among the business community. In particular, DOE can accelerate its commercialization functions by more directly funding and partnering with businesses focused on project implementation and grid integration. Additionally, DOE has essential expertise on storage technology performance validation, testing, and safety code compliance that can benefit industry members developing new storage technologies and integrated solutions.

- b. How should such partnerships be setup to most effectively foster communication and collaboration between DOE and the private sector?*

To be most effective, DOE's various program offices working on energy storage might enable a regular channel for discussion specifically with the storage industry, either with annual/semi-annual meetings, a series of web conferences, or other ongoing means to facilitate dialogue. Such an effort would be separate from DOE's Electric Advisory Committee, for which energy storage is one of many topics of interest and which limits discussion specifically to the storage portfolio in DOE's Office of Electricity (i.e., not including offices of Science, Energy Efficiency & Renewable Energy, or other program offices).

For public-private partnerships on technology development, DOE could also create a call for storage project proposals to be funded via a formal cross-cutting storage account. The Promoting Grid Storage



501 New York Avenue NW, Suite 510
Washington, DC 20001
p.202.293.0537

Act (H.R. 2909) would set up a competitive grant program along these lines, which the U.S. Energy Storage Association has endorsed. DOE could accelerate higher value learning by sharing the results of those projects among grantees and other industry members.

If you have additional questions, please do not hesitate to contact us.

Sincerely,



Kelly Speakes-Backman
Chief Executive Officer
U.S. Energy Storage Association

Responses by Ms. Katherine Hamilton

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

“The Future of Electricity Delivery: Modernizing and Securing our Nation’s Electricity Grid”

Ms. Katherine Hamilton, Chair, 38 North Solutions

Questions submitted by Representative Eddie Bernice Johnson, Chairwoman,
House Committee on Science, Space, and Technology

Q1: To capitalize on the promise of a secure and modernized grid, voluntary, consensus-based standards, such as those on interoperability, could simplify new equipment installation and enhance the overall security of the grid.

- a. Do you believe the government has a role to play in developing voluntary, consensus-based standards, or should that be left to industry?

Yes, I believe the federal government plays an important role in convening stakeholders and driving consensus around standards to ensure that they meet the guidelines developed by public policy goals set by Congress. Standards such as the Corporate Average Fuel Economy (CAFE) for vehicles, for example, have pushed auto companies to develop and manufacture more fuel-efficient vehicles that save consumers money and reduce environmental impact. The carmakers on their own would not have done this, but needed the leadership of the federal government to set those goals. In the same manner, utilities have been investing in grid modernization only where it fits into their bottom line and they can get rate recovery from their customers. Having the federal government take a leadership role could push utilities, as well as solutions providers and manufacturers, toward outcomes for the greater public benefit and good.

- b. What is the current role of DOE in developing voluntary, consensus-based standards in this space?

While my organization does not work directly with DOE in this arena, my understanding is that the Appliance Standards program involves stakeholder participation, as does the Solid-State Lighting Program (with an Industry Alliance). When I ran the GridWise Alliance, the National Institute of Standards and Technology was tasked with developing interoperability standards for smart grid technologies, which was managed in collaboration with private sector stakeholders.

Q2: Effective public-private partnerships can help reduce costs for taxpayers by accelerating development of relevant technologies.

- a. How do you think stronger partnerships between the DOE offices and industry would be helpful to your members?

In my testimony, I recommended adding third party solutions-providers, consumers, and communities to the list of stakeholder entities for coordination. Input from end users can ensure that the technologies and experiences resulting from federal research and development will actually work as designed and deliver their intended benefits. Allowing their participation will also safeguard that results from DOE R&D are well-spent taxpayer dollars. As my Advanced Energy Management Alliance members engage in states throughout the U.S., we find that by engaging in stakeholder processes from a consumer perspective, we see better outcomes for consumers of all types—commercial, industrial, and residential—that can work within the utility planning process.

- b. How should such partnerships be set up to most effectively foster communication and collaboration between DOE and the private sector?

A collaborative alliance that represents all entities mentioned above could be formally appointed by the Secretary of Energy to provide input on grid modernization technology needs, to propose and offer pilot sites to test efficacy of technologies, and to assess DOE programs in the real world.

Appendix II

ADDITIONAL MATERIAL FOR THE RECORD

LETTER SUBMITTED BY REPRESENTATIVE CONOR LAMB



The association of electrical equipment
and medical imaging manufacturers
www.nema.org

July 17, 2019

The Honorable Conor Lamb, Chairman
The Honorable Randy Weber, Ranking Member
House Science, Space, and Technology Committee
Subcommittee on Energy
394 Ford House Office Building
Washington, DC 20515

Chairman Lamb and Ranking Member Weber:

On behalf of its Members, the National Electrical Manufacturers Association (NEMA) submits this letter for the record for the Subcommittee hearing entitled "The Future of Electricity Delivery: Modernizing and Securing Our Nation's Electricity Grid."

NEMA is the national trade association representing nearly 350 electrical and medical imaging manufacturers that make the equipment used in enabling electricity to flow across the grid and the products that provide safe and reliable diagnostic imaging.

One of our top priorities is to enact or revise programs and policies that improve our nation's electricity delivery infrastructure. Consequently, we commend you and your colleagues for holding this hearing on modernizing and securing the nation's grid. NEMA believes Congress and the federal government could be stimulating significant improvements in this area. We also believe the Department of Energy can make significant headway with proper research and development activities to push our grid into the future. NEMA and its Members support research and development, and we recommend adding the following additional provisions that will further improve outcomes for our energy infrastructure.

First, to capitalize on the promise of a secure and modernized grid, national industry consensus Standards, such as those on interoperability, will simplify new equipment selection and installation and enhance the overall value of the new grid. Therefore, grant programs should be targeted at helping industry develop the necessary Standards.

Second, we believe any reforms to existing programs or the creation of new programs should include strong partnerships with manufacturers, Standards development organizations, and research institutions. This approach has been very successful in the area of solid-state lighting. Congress required in the Energy Policy Act of 2005 that DOE establish just such a partnership with the private sector, and the results have been exceptional. In fact, this partnership resulted in over 250 new patents and lower cost for a single LED lightbulb from \$60.00 in 2011 to about \$1.00 by 2019. Adopting a similar approach in the grid modernization area could be just as useful. We would encourage the Subcommittee to consider language along these lines:

Sec: Industry Alliance.

Not later than 90 days after the date of enactment of this Act, the Secretary shall competitively select an Industry Alliance to represent participants who are private, for-profit firms that, as a group, are broadly representative of the United States electrical grid research, development, infrastructure, and manufacturing expertise as a whole.

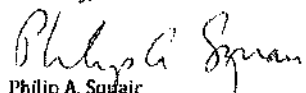
Industry Alliance. – The Secretary shall annually solicit from the industry Alliance –
(A) comments to identify grid modernization technology needs;
(B) an assessment of the progress of the research activities; and
(C) assistance in annually updating grid modernization technology planning documents (e.g. roadmaps, frameworks, etc.).

Availability to Public. – The information and documents shall be available to the public.

Third, protection from cybersecurity events—and the ability to recover from them—are essential to the modernization of the grid. Cybersecurity policies and research and development must provide a common risk-based approach that gives manufacturers, utilities, and grid operators the flexibility to detect, react and recover quickly and decisively. That is why we oppose efforts such as H.R. 680, the Securing Energy Infrastructure Act, which, by emphasizing outdated analog methodologies, would harm our ability to develop and deploy the next generation electric grid.

NEMA is supportive of your efforts to address many of the issues facing our nation's energy infrastructure, and we would welcome additional opportunities to discuss the ideas mentioned in this letter and any technical corrections that may arise as any legislation is being considered.

Sincerely,


Philip A. Squair
Vice President, Government Relations

