S. HRG. 114–505

S. 3018, THE SECURING ENERGY INFRASTRUCTURE ACT, AND TO EXAMINE PROTECTIONS DESIGNED TO GUARD AGAINST ENERGY DISRUPTIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON PUBLIC LANDS, FORESTS, AND MINING

OF THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JULY 12, 2016

Printed for the use of the
Committee on Energy and Natural Resources

Available via the World Wide Web: http://fdsys.gov

U.S. GOVERNMENT PUBLISHING OFFICE

21–995 WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND NATURAL RESOURCES

LISA MURKOWSKI, Alaska, *Chairman*

JOHN BARRASSO, Wyoming	MARIA CANTWELL, Washington
JAMES E. RISCH, Idaho	RON WYDEN, Oregon
MIKE LEE, Utah	BERNARD SANDERS, Vermont
JEFF FLAKE, Arizona	DEBBIE STABENOW, Michigan
STEVE DAINES, Montana	AL FRANKEN, Minnesota
BILL CASSIDY, Louisiana	JOE MANCHIN III, West Virginia
CORY GARDNER, Colorado	MARTIN HEINRICH, New Mexico
ROB PORTMAN, Ohio	MAZIE K. HIRONO, Hawaii
JOHN HOEVEN, North Dakota	ANGUS S. KING, JR., Maine
LAMAR ALEXANDER, Tennessee	ELIZABETH WARREN, Massachusetts
SHELLEY MOORE CAPITO, West Virginia	

SUBCOMMITTEE ON ENERGY

JAMES E. RISCH, *Chairman*

JEFF FLAKE	JOE MANCHIN III
STEVE DAINES	BERNARD SANDERS
BILL CASSIDY	DEBBIE STABENOW
CORY GARDNER	AL FRANKEN
JOHN HOEVEN	MARTIN HEINRICH
LAMAR ALEXANDER	MAZIE K. HIRONO
ROB PORTMAN	ANGUS S. KING, JR.
SHELLEY MOORE CAPITO	ELIZABETH WARREN

COLIN HAYES, *Staff Director*
PATRICK J. MCCORMICK III, *Chief Counsel*
BRIANNE MILLER, *Professional Staff Member*
ANGELA BECKER-DIPPMAN, *Democratic Staff Director*
SAM E. FOWLER, *Democratic Chief Counsel*
DAVID GILLERS, *Democratic Senior Counsel*

CONTENTS

OPENING STATEMENTS

WITNESS

ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

S. 3018, THE SECURING ENERGY INFRASTRUCTURE ACT, AND TO EXAMINE PROTECTIONS DESIGNED TO GUARD AGAINST ENERGY DISRUPTIONS

TUESDAY, JULY 12, 2016

U.S. SENATE,
SUBCOMMITTEE ON ENERGY,
COMMITTEE ON ENERGY AND NATURAL RESOURCES,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:30 p.m. in Room SD–366, Dirksen Senate Office Building, Hon. James E. Risch, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF HON. JAMES E. RISCH, U.S. SENATOR FROM IDAHO

Senator RISCH. We are going to bring this meeting to order, a couple of minutes early, as a matter of fact.

We do have a vote at 3:30 and, having looked at the agenda, the witnesses and the participants, I have every confidence that we can get done what we necessarily have to get done in order to finish by 3:30.

With that, the purpose of today's hearing is to receive testimony on Senate bill 3018, the Securing Energy Infrastructure Act, and to examine protections designed to guard against grid disruptions.

This is a result of, I think, what everybody acknowledges and what everybody knows and that is that the electric grid that we have in America is really, incredibly, dependable. That is true particularly if you have traveled in other parts of the world, you know how dependable our grid is.

Unfortunately, because of the development of the worldwide web and those new ways of handling operations of controls, it also now has vulnerabilities. These vulnerabilities, obviously, are targets by people who wish to do us harm. As a result of that, those of us who deal with this every day believe we should take a look at doing this better, perhaps even doing this differently.

One of the things that brought this to light, and only one of the things, was an event that happened on December 23rd, 2015 in the Ukraine where an attack shut down their electric grid system and caused immeasurable damage and difficulty for the people of the Ukraine.

The attack could have been substantially worse. And it was not because they operate differently than we do in that a lot of their

actions and operation of the grid is done with manual procedures as opposed to automated systems.

We, here in America and other first world countries, have really gone to automated systems for a lot of different reasons, not the least of which was/is convenience and reliability, but also those kinds of things do open us up to additional vulnerabilities.

This bill was originally introduced by Senator King and me, and our co-sponsors are Senators Collins and Heinrich. It is not by coincidence that all four of us are on the Intelligence Committee and we hear stories, not only stories, but expert opinions on what can happen not only to our grid but to other grids around the world, a good share of which we cannot share with you. But suffice it to say that the facts are sufficiently concerning that this is a subject that needs the attention of the U.S. Congress. So here we are today with this bill.

As everyone knows this is a two-year pilot project. It certainly isn't designed to be an absolute solution, but it is designed to explore possibilities of how the United States can handle one of these.

Speaking for myself, not the other co-sponsors but speaking for myself, I truly believe that the next significant event, and when I talk about a significant event, I mean a really significant event, will not be a kinetic event, but will indeed be an event that takes place in the cyber world that causes considerable grief and harm to Americans. As we all know, we face significant challenges in that arena.

We have asked four people to be with us today to testify.

We are going to start today with Ms. Pat Hoffman, who is Assistant Secretary in the Office of Electricity Delivery and Energy Reliability with the Department of Energy. She will start us off with an overview of the Department of Energy's work protecting our grid from energy disruptions.

We also have Mr. Duane Highley, President and CEO of the Arkansas Electric Cooperative Corporation. He is also co-chair of the Electric Subsector of the Coordinating Council.

We also have Mr. Rob Manning, Vice President of Transmission for the Electric Power Research Institute.

Finally, last but certainly not least from the great State of Idaho, we have Mr. Brent Stacey, who is Associate Lab Director at the Idaho National Laboratory. Right now, Idaho's National Laboratory is the world leader in critical infrastructure and control systems research, primarily because of the expenditures that we have made developing the systems and the facilities to do that research. I am sure Mr. Stacey will describe that for us.

With that, I certainly welcome everyone here today. I think this is a good opportunity. This is not a complicated bill. It is a bill that is intended to move us forward in a cautious way but a way that will help underscore some of the vulnerabilities that those of us on the Intelligence Committee have heard about over time.

Senator Manchin.

STATEMENT OF HON. JOE MANCHIN III, U.S. SENATOR FROM WEST VIRGINIA

Senator MANCHIN. Mr. Chairman, thank you, and thank all of you for being here today. I want to thank you for scheduling this

hearing, Mr. Chairman, and for your work on this important bill that we are working on. I also want to thank Senators King and Heinrich for their leadership on this issue. I appreciate our witnesses joining us today for this very special discussion.

The electric grid is essential to our lives and is also the lifeblood of the economy. The grid moves power hundreds, if not thousands, of miles to our houses, office buildings and factories every day. People and business in the Northeast and the Mid-Atlantic states are heavily dependent on a well-functioning grid to access power generated in my home State of West Virginia.

The Energy Information Administration, EIA, reports that in 2014 West Virginia produced approximately over 80,000 kilowatt hours of electricity. The EIA consistently reports that West Virginia typically exports more electricity than it consumes, so we are a net exporter of electricity.

West Virginia's neighbors, Maryland, Virginia, Washington, DC and others, depend on us for reliable electric generation, not to mention coal and natural gas production. Whether because of a cyber or physical attack or some other energy disruption, imagine what it would be like if West Virginia stopped producing and delivering energy. Incidents like the polar vortex quickly become even more dangerous and likely tragic.

The secure and reliable transportation of energy is vitally important to our state's economy and to the safety and health of our citizens and those in neighboring states, so I believe today's hearing is an important start to a longer conversation about the security of our grid.

As the electric industry has increased its reliance on digital technologies to better serve consumers, the grid has grown more vulnerable to cyber-attack. Just last December the first successful cyber-attack took place against part of Ukraine's electric grid demonstrating that shutting down the grid is a real possibility.

Many cyber experts have come to the conclusion that it is not a question of "if", but a question of "when" a massive attack on our grid will occur. We must do everything we can to protect and prepare, including hardening our networks to protect the grid and ensure the continued reliable delivery of electricity. But we also need to focus on emergency preparedness and incident response to minimize the effects of a potential attack. That is why the King/Risch/Collins/Heinrich bill is a step in the right direction.

Senate bill 3018 would establish a two-year pilot program within the national labs to research and test technology that could be used to isolate and protect the most critical systems of the electric grid. It would also establish a working group to evaluate the proposals of the pilot program and develop a national cyber informed engineering strategy.

Mr. Chairman, the 2013 attack on the Pacific Gas and Electric substation in Metcalf, California reminds us that the threats to our grid are not limited to cyberspace. According to press reports, the Federal Energy Regulatory Commission has identified a smaller number of critical grid-related facilities that, if physically attacked, could significantly impair the ability of utilities to keep the lights on.

Keeping America's energy network secure from cyber and physical intrusions is critical as new technologies and threats continue to emerge from transnational organized crime, terrorists' groups and hostile foreign governments. The argument goes that the smarter and more connected the power grid becomes, the more vulnerable it becomes. I am sure you are familiar with the scale we are talking about.

The Department of Homeland Security reported that 56 percent of cyber incidents against critical infrastructure in 2013 were directed at energy infrastructure, mostly in the electric grid. While the number has shrunk to 16 percent in 2015, there is much more to be done. That is why I support the Energy Policy Modernization Act of 2016 that Chairman Murkowski and Ranking Member Cantwell worked so hard to get passed out of Committee and finally out of the Senate by a vote of 85 to 12. Believe me, that does not happen here that often.

The bill includes a cyber energy section that includes the research and development program to develop advanced cyber security technologies, doubles the Department's current investment in cyber-related research and development, supply chain security and public/private partnerships.

It encourages the Department of Energy to work hand in hand with the private sector. This recognizes the importance of aligning government capabilities with the needs of industry actors that are dealing with potential threats to our grid every day.

The ability to deliver energy quickly, securely and without interruption is something that West Virginia prides itself on. So that is also why I am particularly appreciative of Senator King's passion for this issue, and I commend him and all of the co-sponsors of this bill.

Chairman Risch and Senator Heinrich's ongoing efforts for this bill is muchly appreciated.

I want to thank the Chair for holding this hearing, and I look forward to the testimony of our witnesses. At this time, I would like to turn it over to Senator King.

Senator RISCH. Senator King.

STATEMENT OF HON. ANGUS S. KING, JR., U.S. SENATOR FROM MAINE

Senator KING. Thank you.

I first want to commend the Chair. This is first in my experience of a hearing that actually started early rather than late. That bodes well.

Senator RISCH. If it ends or that could be it.

Senator KING. That is another challenge.

When I used to appear before the main legislature, the first question always asked was, why are you here? I think the answer in this case is pretty clear.

As Senator Risch mentioned he and I serve together on the Intelligence Committee. I am also on the Armed Services Committee. I would say in virtually every hearing that we have had over the past four years that I have been to, somehow the cyber vulnerability comes into the conversation.

In fact we had a classified Armed Services Committee hearing just this morning on this very issue, and I characterize this as the longest windup for a punch in the history of the world.

We know that it is coming, and we know that there are people who are actively working to do us harm right now. And we have had warning shots—OPM, SONY, and others.

As Senator Manchin mentioned, we are asymmetrically wired, so we are asymmetrically vulnerable. This is a very straightforward bill, and it does grow out, to some extent, of the experience in the Ukraine where when they found that they had analog and human intervention at certain key points. We are not talking about rewriting all the software or dumbing down the grid. We are talking about inserting some elements of analog and human intervention at certain critical points in order to protect us.

Interestingly enough, just this year, just in the last few weeks, there has been an analogous policy recognition in the United States Navy. For the first time in 20 years Annapolis is now going back to the teaching of celestial navigation, and the reason is that you can't hack a sextant.

This is a recognition that with all of our sophistication comes additional vulnerability and that what we are attempting to do today is to talk about and work on, on a pilot basis, and on a voluntary basis for the utilities, some unconventional solutions to this vulnerability challenge. I do not want to go home to Maine after a disastrous attack somewhere in the United States on our critical infrastructure and explain that we did not try some various options.

That is the reason I brought forth the bill. It grew out of conversations with Senator Risch and the work that we have done in the Intelligence Committee, and I am delighted that we are here today.

I appreciate the opportunity to present this bill.

Thank you.

Senator RISCH. Thank you, Senator.

Do you have an opening statement you want to make, Senator Heinrich?

STATEMENT OF HON. MARTIN HEINRICH, U.S. SENATOR FROM NEW MEXICO

Senator HEINRICH. I do, Mr. Chairman, and I will make it very quick.

I want to thank you for your work and Senator King as well. I think this is a very important piece of legislation, and I am pleased to be an original co-sponsor.

I want to reiterate Senator King and I both had a closed-door hearing in Armed Services this morning that really drives home what a real issue this is and how we need to take it very seriously.

I do think it is important to make the point that this is not about dumbing down the grid. I think Senator King, myself, and others on this Committee have been very staunch advocates of smart grid technology, of microgrids, and of all of the developments that are making our grid much more responsive today. But it is about having those backups in place and those fail safes in place.

I think it is important to state that our bill is not prescriptive in that the working group has the flexibility to consider a full range of options.

So, once again, I want to thank Chairman Risch and I want to thank Senator Manchin for holding this hearing today, and I very much look forward to the testimony from our witnesses who are here.

Senator RISCH. We will now turn to our witnesses. Ms. Hoffman, would you care to start us off, please?

STATEMENT OF PATRICIA HOFFMAN, ASSISTANT SECRETARY, OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY, U.S. DEPARTMENT OF ENERGY

Ms. HOFFMAN. Thank you, Chairman Risch, Ranking Member Manchin and members of the Subcommittee. Thank you for continuing to highlight the importance of a resilient electric grid.

The Department also appreciates the opportunity to provide initial views on Senate bill 3018, the Securing Energy Infrastructure Act.

The Department supports the goals of Senate bill 3018 which are consistent with the Department's ongoing role to helping ensure resilient, reliable and flexible electricity system in an increasingly challenging environment.

The Department would like to work with the sponsor and this Committee to offer continued additional input on the bill, and I will discuss this later on in my testimony.

Our economy, national security and even health and safety of citizens depend on a reliable delivery of electricity. The mission of the Office of Electricity Delivery and Energy Reliability is to strengthen, transform and improve the energy infrastructure to ensure access to reliable, secure and clean sources of energy. We are committed to working with our public and private sector partners to protect that the nation's critical energy infrastructure, including the electric power grid, from disruptions caused by natural and manmade events, physical security events and cyber security events.

A crucial factor in meeting these challenges will be to be proactive and cultivate, what I call an ecosystem of resilience, a network of owners and operators, regulators, vendors, Federal partners and consumers, working together to strengthen our ability to prepare, respond and recover.

Our organization works on in-depth strategies, products and tools which inform and educate industry as well as state and local officials in their energy emergency preparedness activities. As part of the Administration's effort to improve the electric sector, cyber security capabilities, the Department and industry partners are developing and have developed a maturity model. This evaluation tool helps an organization prioritize and advance its security posture in the areas such as information sharing, supply chain management and access control, just to name a few.

The Department of Energy has provided strategic leadership by requesting and facilitating the development of an electricity information sharing and analysis center and the development of the Electric Sector Coordinating Council. The Electric Sector Coordi-

nating Council is a group of leaders from the electric sector that meet regularly with government to coordinate and share information.

When the power goes out the local utility is a first responder. Should any threat or emergency exceed local or private resources or require a full blown response, the Electric Sector Coordinating Council will engage with the Federal Government for a coordinated response to a crisis activity.

The keys to strengthening resilience are not only from better threat insight and response but also through innovation. Advanced technology and innovation in cyber security, storage, and microgrids will help the industry get ahead of these risks. All of the Department's cyber security research initiatives are based on industry involvement, joint funding with matching funds and the development of an end goal to get industry deployment.

There are several examples of DOE, our organization's, activities that support cyber security technologies developed for the power grid and use physics and the capabilities of the electric grid to its advantage. One example is an industry-led research project that helps the protection and control equipment check the commands it receives to ensure these commands support this ability of grid operations. Another example is a national laboratory-led research that is designing cyber security awareness and to power system applications themselves so that malicious actors should not be able to manipulate power system devices.

Thank you for the opportunity to provide technical assistance on Senate bill 3018. We agree with the goals of the bill to strengthen the cyber security posture by allowing the DOE national laboratories to study the systems most critical to national security.

With respect to assessments, many electric sector entities already conduct vulnerability assessments of part of the standards set by the North American Electric Reliability Corporation. Yet, there still may be a gap where the DOE national laboratories should partner with industry.

But even assessments aren't enough. Research is required to conduct cyber engineering to mitigate these risks.

In conclusion, threats will continue to evolve. The Department is working diligently to stay ahead of the curve. To accomplish this, we must invest in resilience, encourage innovation and use the best practices to raise the energy sector's cyber security, physical security maturity level as well as strengthen incident response and recovery capabilities.

Thank you. This concludes my remarks, and I look forward to any questions that you may have.

[The prepared statement of Ms. Hoffman follows:]

Testimony of Assistant Secretary Patricia Hoffman

Office of Electricity Delivery and Energy Reliability

U.S. Department of Energy

Before the

Subcommittee on Energy

Committee on Energy and Natural Resources

United States Senate

July 12, 2016

Chairman Risch and Ranking Member Manchin, and Members of the Subcommittee, thank you for continuing to highlight the importance of a resilient electric power grid and for the opportunity to provide the initial views of the Department of Energy (DOE) on S. 3018, the Securing Energy Infrastructure Act. DOE supports the goals of S. 3018, which are consistent with the Department's ongoing role in helping to ensure a resilient, reliable, and flexible electricity system in an increasingly challenging environment. DOE would like to work with the sponsor and this Committee to offer additional input on the bill as discussed later in this testimony.

Our economy, national security, and even the health and safety of our citizens depend on the reliable delivery of electricity. The mission of the Office of Electricity Delivery and Energy Reliability (DOE-OE) is to strengthen, transform, and improve energy infrastructure to ensure access to reliable, secure, and clean sources of energy. We are committed to working with our public and private sector partners to protect the Nation's critical energy infrastructure, including the electric power grid, from

There are plenty of risks beyond cyber, including physical, severe weather, natural disasters, electromagnetic pulses (EMPs), aging infrastructure, and infrastructure interdependencies. In the face of these diverse threats, we can help ensure that the grid is poised to recover quickly following an incident. Fostering partnerships with public and private stakeholders plays a critical and necessary role in this work.

THE ECOSYSTEM OF RESILIENCE

A crucial factor to meeting these challenges is to be proactive and cultivate what I call an ecosystem of resilience: a network of producers, distributors, regulators, vendors, and public partners, acting together to strengthen our ability to prepare, respond, and recover. We continue to partner with industry, other Federal agencies, local governments, and other stakeholders to quickly identify threats, develop in-depth strategies to mitigate those threats, and rapidly respond to any disruptions.

Our resilience efforts are further bolstered by our broader grid modernization activities, including our support of the research, development, and demonstration of advanced technologies and our work with state, local, tribal, and territorial stakeholders to help them improve their local

resilience and energy emergency response capabilities. Of the $4.5 billion that we invested in grid modernization through the American Recovery and Reinvestment Act (ARRA), $3.4 billion was used to help industry accelerate the deployment of advanced technologies that are now reducing costs and keeping the lights on more reliably and efficiently. This smarter grid is helping to prevent outages, reduce storm impacts, and restore service faster when outages occur.

Our model is partnerships first. We are all in this together. It is through working together that we continue to strengthen our ability to bounce back following an event.

PARTNERSHIPS FOR READINESS

DOE-OE has been working with utility owners and operators, regulators, and state and local officials across the country concerning threats to cybersecurity and other risks. Through these partnerships, we are providing tools, best practices, new technologies, and funds to support their many ongoing efforts.

We directly support preparedness efforts at the community level, in part through products and tools produced by our Infrastructure Security and Energy Restoration (ISER) division, to inform and educate state and local officials in their energy emergency preparedness activities. This is done through forums, training, and tabletop exercises for Federal, state, and local energy officials.

Cybersecurity and Resilience

Intentional, malicious challenges to our energy systems are on the rise. We are seeing threats continually increase in numbers and sophistication. This evolution has profound impacts on this sector, which is why we've made cybersecurity one of our highest priorities at DOE.

As there has been an increase in malicious cyber activity, we work closely with the energy sector to share cyber threat information. Since 2010, DOE-OE has invested more than $210 million in cybersecurity research, development and demonstration projects that are led by industry, universities and National Labs. Since then, more than 20 new technologies that our investments helped support are now being used to further advance the resilience of the Nation's energy delivery systems. For example, SecureSmart helps keep Smart Grid networks secure, and Hyperion helps keep power system applications secure.

All of OE's cybersecurity research initiatives are based upon industry involvement, joint funding through matching funds, and development with an end goal of practical use.

There are several examples of DOE-OE supported cybersecurity technologies tailored to respect the stringent operational requirements of the power grid, and to advantageously use the physics of energy delivery. One example is an industry-led research project that helps protection and control equipment check received commands to ensure these commands support the stability of grid operations and do not jeopardize grid stability[i]. Another example is DOE National Laboratory-led research that is designing cybersecurity awareness into the power system applications so malicious, adversarial manipulation of power system devices and applications can be identified and mitigated automatically.[ii]

The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership, co-funded by DOE-OE and industry that also focuses on building sector resilience. The purpose of CRISP is to collaborate with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information and to develop situational awareness tools that enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources. CRISP leverages advanced sensors and threat analysis techniques developed by DOE along with DOE's expertise as part of the National Intelligence Community to better inform the energy sector of the high-level cyber risks. Current CRISP participants provide power to over 75 percent of the total number of continental U.S. electricity subsector customers.

Cybersecurity preparedness was part of the Smart Grid Investment Grants (SGIG) awarded by OE through American Recovery and Reinvestment Act. Each of the 99 projects that received funding was required to develop a cybersecurity plan. Participants included investor owned utilities, public power utilities, and cooperatives. This process truly raised the bar of awareness of cybersecurity risks and jumpstarted progress in cybersecurity protection actions and best practices.

Further, as part of the Administration's efforts to improve electricity subsector cybersecurity capabilities, DOE-OE and industry partners developed the Electricity Subsector Cybersecurity Capability Maturity Model (C2M2) to help private sector owners and operators better evaluate their cybersecurity capabilities. The C2M2 evaluation helps organizations prioritize and improve cybersecurity activities.

Since the C2M2 program's inception in June 2012, more than 900 C2M2 toolkits have been distributed, and industry adoption of the C2M2 is growing steadily. This is a comprehensive and credible approach that all energy sector companies can use to improve their cybersecurity posture. DOE-OE also released versions of the C2M2 for the oil and natural gas sector and for industry at large.

PARTNERSHIPS FOR RESPONSE

Our partnerships with private and public stakeholders also focus on quickly identifying threats, developing in-depth strategies to mitigate them and rapidly responding to any disruptions. With 90 percent of the Nation's power infrastructure privately held, coordinating and aligning efforts between the government and the private sector is the only viable path to success.

Under Presidential Policy Directive-21: Critical Infrastructure Security and Resilience and the Fixing America's Surface Transportation (FAST) Act (P.L. No. 114-94), DOE is the Sector-Specific Agency (SSA) for electrical infrastructure. The SSA plays the pivotal role of ensuring unity of effort and message across government partners, including the Department of Homeland Security, the Department of Defense, and DOE offices.

As the Energy SSA we also serve as the day-to-day Federal interface for the prioritization and coordination of activities to strengthen the security and resilience of critical infrastructure in the electricity subsector. This involves building, maintaining, and advancing our relationships and collaborative efforts with the energy sector. We have invested in public/private partnership

programs and initiatives that involve sharing real time information, assessing vulnerabilities, clarifying responsibilities, and engaging in training and exercises.

In addition, the Department of Energy serves as the lead agency for Emergency Support Function 12 (ESF-12) under the National Response Framework. As the lead for ESF-12, the DOE is responsible for facilitating the restoration of damaged energy infrastructure. During a response operation, the Department works with industry and Federal/state/local partners to:

- Assess disaster impacts on local and regional energy infrastructure;
- Coordinate asset delivery to repair damaged infrastructure;
- Monitor and report on restoration efforts; and
- Provide regular situational awareness updates to key decision makers in the Administration and our interagency partners.

To achieve these operational priorities, the Department deploys responders who work directly with the affected utilities and local officials on the ground during a disaster. The responders provide expertise on a variety of energy issues, and have direct access to our subject matter experts in Washington, DC who work with our interagency partners to coordinate the appropriate waivers, when needed, to further speed restoration efforts. In extreme cases, the Department can use its legal authorities under the Federal Power Act, Defense Production Act, and other statutes to assist in response and recovery operations.

Threats ranging from a fallen tree to a dedicated hacker from overseas can threaten the broader transmission system and the distribution system. When the power goes out, the local utility is the first responder. Should any threat or emergency exceed local public or private resources or require a full-blown national response, a utility CEO, a representative trade association member of the Electricity Subsector Coordinating Council (ESCC), the Electricity Information Sharing and Analysis Center (E-ISAC), or the Federal Government can request what is called a Crisis State Activity. Crisis State Activities are coordinated through the ESCC because, as with preparedness, we respond through partnerships. The ESCC is a group of leaders from across the electricity subsector that meet regularly with government to coordinate and share information. Together, we work toward collective actions to address the threat or risk.

Congress enacted several important new energy security measures in the FAST Act. The Secretary of Energy was provided a new authority, upon declaration of a Grid Security Emergency by the President, to issue emergency orders to protect or restore critical electric infrastructure or defense critical electric infrastructure. This authority allows DOE to respond as needed to the threat of cyber and physical attacks on the grid. DOE is working to issue rules of procedure regarding this new authority.

PARTNERSHIPS FOR INNOVATION

Innovation and preparedness are vital to grid resilience. In January 2016, the DOE built upon its Grid Modernization Initiative – an ongoing effort that reflects the Obama Administration's commitment to improving the resiliency, reliability, and security of the Nation's electricity delivery system – by releasing a comprehensive new Grid Modernization Multi-Year Program Plan (MYPP). The MYPP, developed in close collaboration with a wide range of key external partners, lays out a blueprint for DOE's research, development, and demonstration agenda to

enable a modernized grid, building on concepts and recommendations from the first installment of the Quadrennial Energy Review (QER) and Quadrennial Technology Review (QTR).

For example, large power transformers are critical to grid resilience, and are ripe for innovation. These important grid assets can weigh hundreds of tons, are expensive, and are typically custom made with procurement lead times of a year or more. A significant number of damaged transformers from any type of hazard could result in a long-term impact on the overall resilience of the grid. The QER recognized the risks associated with the loss of large power transformers. The QER recommended that DOE work with other Federal agencies, states, and industry on an initiative to mitigate these risks. Approaches envisioned in the QER include the development of one or more strategic transformer reserves through a staged process, beginning with an assessment of technical specifications and whether new Federal regulatory authorities or cost-share are necessary and appropriate.

Secretary Moniz also announced last January an award of up to $220 million over three years, subject to congressional appropriations, to DOE's National Laboratories and partners to support critical research and development in advanced storage systems, clean energy integration, standards and test procedures, and a number of other key grid modernization areas. This Grid Modernization Laboratory Consortium effort recognizes regional differences and will strengthen regional strategies while defining a diverse and balanced national strategy. In addition to projects that address the needs of incorporating individual grid technologies like solar or energy storage, DOE is also developing crosscutting projects that have impact across multiple technologies. As Secretary Moniz said at the announcement, "Modernizing the U.S. electrical grid is essential to reducing carbon emissions, creating safeguards against attacks on our infrastructure, and keeping the lights on."

Energy storage is another key technology for whole-grid resilience. Energy storage fundamentally changes the relationship between when energy is produced and when it is consumed. The President's FY 2017 Budget Request supports OE's work on materials research, device development, demonstrations, and grid analysis to help transition selected energy storage technologies from R&D to industrially relevant scales with improved safety, industry acceptance, and reduced cost. Improved energy storage technologies will enable the stability, resiliency, and reliability of the future electric utility grid, as well as increased deployment of variable renewable energy resources.

We have been proactive in advancing technologies to modernize and make our grids smarter and more adaptive to the challenges posed by threats to the grid. For example, DOE-OE has made key investments in the area of synchrophasor technology, which reduces grid vulnerabilities by providing timely and accurate power outage information and better self-healing capabilities, and has also invested in microgrids, which keep local communities up and running during regional and other outages and help supply power to affected areas.

Many of these projects are working in local jurisdictions throughout the United States. Supporting the research, development, and deployment of next-generation technologies enhances the grid's ability to recover quickly from disruptions.

S. 3018

Thank you for the opportunity to provide technical assistance on S. 3018. It appears that the intent of S. 3018 is to strengthen the cybersecurity posture by allowing DOE National Laboratories to study the systems most critical to national security to the grid.. Yet, many energy sector entities already conduct such assessments to comply with mandatory Critical Infrastructure Protection (CIP) standards set by the North American Electric Reliability Corporation (NERC) or as part of their due diligence in ensuring their system is reliable and capable of providing uninterrupted service in the face of today's evolving cyber threat landscape.

There may still be a gap where the DOE National Laboratories could be of value to the Nation. Given that the National Laboratories are able to address complex system vulnerabilities, S. 3018 could provide an opportunity for the National Laboratories to not only identify complex system vulnerabilities, but do the research and development to mitigate these risks.

CONCLUSION

Threats continue to evolve, and DOE is working diligently to stay ahead of the curve. The solution is an ecosystem of resilience that works in partnership with local, state, and industry stakeholders to help provide the methods, strategies, and tools needed to help protect local communities through increased resilience and flexibility. To accomplish this, we must accelerate information sharing to inform better local investment decisions, encourage innovation and the use of best practices to help raise the energy sector's security maturity, and strengthen local incident response and recovery capabilities, especially through participation in training programs and disaster and threat exercises.

Building an ecosystem of resilience is—by definition— a shared endeavor, and keeping a focus on local communities remains an imperative. Because DOE has spent decades building—and continues to build—local partnerships and investing in technologies to enhance resilience, the grid is better able to withstand and recover quickly from disasters and attacks.

---

[i] Led by ABB, with partners University of Illinois at Urbana Champaign and Bonneville Power Administration.
[ii] Led by Argonne National Laboratory, with partners Idaho National Laboratory, State University of New York-Buffalo, Illinois Institute of Technology, Commonwealth Edison, and PJM.

Senator RISCH. Thank you, Ms. Hoffman.

You mentioned that, I thought I picked up in there, you had some suggestions for the bill. Do you have any specifics at this point?

Ms. HOFFMAN. With respect to specific suggestions, one suggestion that we have is to make sure to coordinate with the Electric Sector Coordinating Council, which Duane is a co-chair of the Council, as part of the working group.

We would like to make sure that we have leverage the continued capabilities within——

Senator RISCH. I hope you will put some language together for us, and we will be happy to have a look at that. As I think everybody has picked up here, this is not a partisan issue, by any stretch of the imagination. We are all pulling the wagon together here, and I think that the Administration's view on this, particularly DOE's, will be very helpful for us as we go forward.

If you will get that for us, we would sure appreciate it.

Thank you.

Ms. HOFFMAN. Thank you.

Senator RISCH. Thank you.

Mr. Highley.

STATEMENT OF DUANE HIGHLEY, PRESIDENT AND CEO, ARKANSAS ELECTRIC COOPERATIVE CORPORATION (AECC)

Mr. HIGHLEY. Yes, sir.

Chairman Risch, Ranking Member Manchin and all members of the Committee, thank you for the invitation to testify today. It's an honor to sit on this panel with these colleagues that I respect so much.

I serve as President and CEO of the Arkansas Electric Cooperative Corporation. We serve a million Arkansans with reliable and affordable, non-profit electricity.

Electric co-ops in the United States serve—900 coops serve 42 million people in 47 states covering 75 percent of the nation's land mass. That's 2,500 of the 3,100 counties in this country. You can imagine the challenge protecting that much infrastructure from intentional attack, let alone just normal weather events. But the challenge of protecting that is actually impossible, but we're working on it all the time.

I serve as co-chair of the Electric Subsector Coordinating Council which is a public/private partnership of critical infrastructure operators which coordinate with our government counterparts on a regular basis on policy-level security issues. So this council is comprised of 30 utility and trade association CEOs. We represent all segments of the electric industry. We work regularly with the White House, Department of Energy, DHS, Federal Energy Regulatory Commission (FERC), the FBI, National Security, all those agencies, to make sure that electric policy is complementary to reliability for our members.

Now through the ESCC, the Electric Subsector Coordinating Council, we have this thing called the Information Sharing and Analysis Center that provides real time information on threats to utilities.

It's working well, but it could work even better. We would like to see stronger communications and more timely information flowing from government. We understand there's confidentiality that has to be preserved, and yet when we get that information we can send it on to our utility partners, who can take action. So in the instance of the Ukraine event, the sooner we know about what's going on there, the quicker we can develop a way to respond.

Now as we develop standards for reliability on the grid, we don't do that haphazardly. The grid has developed over 100 plus, and we have to be very deliberate about the way we make changes to the grid. The way we do that is through a standard setting process through NERC.

So if FERC passes a regulation, they pass it off to NERC, the North American Reliability Corporation. Subject matter experts vet that. The NERC Board approves it. FERC then approves that, and those standards then become mandatory and enforceable on this industry. We can face fines of up to $1 million a day for violations of cyber security regulations or physical security regulations, and NERC has established standards for physical security and GMD.

Now the standards are based on criticalities. So the most critical assets get the largest amount of standards. Less critical don't have as much. Just for example in our little co-op we have 90 million log entries a day that we have to preserve of what computer talked to what computer so we can ensure that that is not, nothing bad is happening.

Now our main answer to all threats is defense in depth. We didn't design the grid to protect against intentional acts of war, but when we designed it with the redundancy to cover weather events and equipment failure we end up having high reliability. And if you imagine the very worst threats possible, a bad event like a tornado or an earthquake, we've seen the grid out for, maybe, days. A really terrible event like a hurricane or a massive regional ice storm, you might see it out for a week or two.

But the reason those events don't cause greater outages is because of the reliability that's already built into the grid, and that's also going to protect us from intentional attack.

And we talk about EMP (electromagnetic pulse), which is a doomsday scenario and would constitute an act of war against the United States. It would impact more than just the electric sector. If we fried all the microprocessors, obviously, it would affect gas pumps, ATMs, cash registers, automobile engines. We're concerned about the impact of EMP but we want to act based on facts, not speculation, which is why we want to hear from EPRI about the good work they're doing on a voluntary basis to try and figure out the threat, characterize it, so we can design appropriate mitigation.

We have to remember that we could gold plate every substation, but there's transmission lines coming in and out so we have to balance the amount of effort we put on protecting. We can't overprotect one area and leave the rest vulnerable.

How can Congress help? We thank you for the FAST Act and for the Consolidation Appropriation Act which is already helping us improve government and industry coordination.

The insider threat is one of the largest factors we face now. We'd like to see you consider legislation giving the FBI authority to as-

sist the industry with fingerprint-based, criminal and terrorist background checks so the people that operate our control systems we know don't have a bad background.

And we find Senate 3018, Securing Energy Infrastructure Act, to be very complementary to the industry efforts.

Please avoid a one-size-fits-all legislation. The grid has been custom-designed based on geography and the characteristics of the grid. And if we can work that through the NERC standard setting process, I think we'll end up with the best result.

Thank you.

[The prepared statement of Mr. Highley follows:]

Testimony of Mr. Duane D. Highley

President and CEO of the Arkansas Electric Cooperative Corporation (AECC)

to the Committee on Energy and Natural Resources

Subcommittee on Energy

U.S. Senate

July 12, 2016

Duane Highley, President and CEO
Arkansas Electric Cooperative Corporation
July 12, 2016 Testimony

Introduction

Chairman Risch, Ranking Member Manchin, and all members of the Committee, thank you for inviting me to testify before your committee on this very important topic, it is an honor. I am here today to testify about security in one of the 16 critical infrastructures within the United States, the electric portion of the energy sector, on behalf of the Arkansas Electric Cooperatives Corporation (AECC) and the National Rural Electric Cooperative Association (NRECA). After I give you a little back ground about myself and those I am representing today I will discuss our current practices which help guard against and recover from energy disruptions including private-public partnerships, processes, and regulations.

As an engineer with 34 years' experience in a sector that many call the most critical of the critical, I continuously strive along with other owners and operators in the sector to ensure reliable, resilient and affordable power so that our communities and neighbors can depend on the light switch in their homes and businesses.

I serve as President and CEO of AECC, a not-for-profit power supply system serving 17 distribution systems, who in turn serve about 1 million Arkansans. I report to a democratically-elected board representing the customers we serve. Arkansas Electric Cooperative Corporation (AECC) was created in 1949 and provides power for more than 500,000 farms, homes and businesses served by our 17 electric distribution cooperative owners. AECC relies on a diverse generation mix to serve its members, including hydropower, natural gas, coal, biomass, wind and solar.

In addition, I also serve as President and CEO of Arkansas Electric Cooperatives Inc. (AECI), which provides construction, right-of-way, and electrical products to utilities across the U.S. A new AECI subsidiary, Today's Power Inc. (TPI) develops utility scale community solar projects and other products to enable household distributed generation.

The electric cooperatives of Arkansas are members of the National Rural Electric Cooperative Association (NRECA), a service organization for over 900 not-for-profit consumer-owned electric utilities serving over 42 million people in 47 states. Electric cooperative service territory makes up 75 percent of the nation's land mass and includes over 19 million businesses, homes, schools, churches, farms, irrigation systems, and other establishments in 2,500 of 3,141 counties in the U.S. NRECA's membership includes 65 generation and transmission (G&T) cooperatives, which provide wholesale power to distribution co-ops through their own generation or by purchasing power on behalf of the distribution members. Kilowatt-hour sales by rural electric cooperatives account for approximately 11 percent of all electric energy sold in the United States. NRECA members generate approximately 50 percent of the electric energy they sell and purchase the remaining 50 percent.

As member owned not-for-profit utilities, distribution cooperatives and G&Ts reflect the values of our membership, and are uniquely focused on providing reliable energy at the lowest reasonable cost. We have to answer to our owners and justify every expense to them. There is never any debate as to whether a proposed project will benefit our shareholders or our customers, because they are one and the same.

I also serve as a co-chair of the Electricity Subsector Coordinating Council (ESCC), a public/private partnership outlined in the National Infrastructure Protection Plan (NIPP) for critical infrastructure owners and operators to serve as the sectors' principal entity with the government on policy-level security issues. Though membership of these councils do vary dramatically across the critical infrastructure sectors, in the electric sector the council is composed of 30 utility and trade association CEOs, representing all segments of the electricity industry, and it engages regularly with its government counterparts, including, senior Administration officials from the White House, Department of Energy (DOE), Department of Homeland Security (DHS), the Federal Energy Regulatory Commission (FERC), the Federal Bureau of Investigation (FBI) and others as needed.

Electric Sector Security

Often news headlines about cyber or physical threats to the electric grid focus on far-fetched scenarios and sensational claims. However, though there are real threats to the grid, the scenarios put forth for public consumption are rarely reflective of the real threat environment but rather disproportionally put forth the highest consequence scenarios that are less likely to occur. Many of these scenarios would constitute acts of war on the United States that would directly impact more than just the electric sector.

Protecting the nation's complex, interconnected network of generating plants, transmission lines, and distribution facilities which make up the electric power grid to ensure a supply of safe, reliable, secure and affordable electricity, is a top priority for the electric power industry.

Defense in Depth

We didn't intentionally design the electric grid to defend against intentional attack and acts of war, but fortunately our normal preparations against severe weather and equipment failure serve us well in limiting the potential impact of intentional actions. This approach to protecting critical assets is known as defense-in-depth. To protect against extreme weather events, vandalism and major equipment failure a high level of redundancy is built into the power supply system. The grid is designed to reliably deliver the highest possible summer or winter peak load demand with the most critical facilities out of service – that is our standard. Because of this we have withstood intentional attacks such as the 2013 California and Arkansas substation attacks with no loss of customer service, despite severe damage to our infrastructure.

The grid is incredibly resilient – imagine the worst ice storm – thousands of poles and wires down – and even in these severe cases service is usually restored in days or at most a couple of weeks – longer outages are extremely unlikely. From drafting plans, to coordinating with our partners, private sector and government alike, to assessing and mitigating risks including building in a multitude of redundancies, we are continuously working to ensure outage times are minimal if and when they do occur.

The electric power industry continuously monitors the bulk electric system and responds to events large and small. Consumers are rarely aware of these events primarily because of the

sector's routinely planning, coordinating, and responding to take care of them. In the cases where an event impacts the consumer, these same activities, in addition to the decades of lessons learned from supplying power, have helped ensure there are hazard recovery plans in place for working within the sector and with government counterparts to get the power back on.

It is critical that one threat doesn't get prioritized over any other simply due to media sensationalism or fear mongering. The concept of an act of war on the United States via a nuclear device detonated above the earth causing an electromagnetic pulse (EMP) wiping out all microprocessors within the impact radius – not just ones utilized by those who own or operate the grid – is a great example. There is often a focus in discussion in the media on only the grid in these scenarios and the concept of a magic bullet that can protect the whole infrastructure from a nuclear attack. The grid relies on other critical infrastructures for fuel, water for generator cooling and telecommunications to support quick recovery from a storm or other event. As those infrastructures would also be impacted by an EMP event, the focus on only one infrastructure could result in a misappropriation of critical resources.

In order for the electric sector to better understand the true potential of the EMP threat and potential mitigation options, a number of electric utilities, including electric cooperatives, are funding research through Electric Power Research Institute (EPRI). It is possible that the shielding built into the current generation of electronic equipment, which allows it to function amidst continual gigahertz interference from cell phones and microwave ovens, may also provide some protection for EMP. We need to work based on facts, not speculation.

Again, defense in depth and system redundancies are helping electric utilities to keep the grid reliable and secure. This will continue to be our first and best defense to any event.

Value in Partnerships & Information Sharing

The industry has decades of experience working together to protect our shared infrastructure and is constantly reevaluating threats and taking steps to protect the system as well as plan for its recovery. Electric cooperatives make protection and security of their consumer-members' assets a high priority. NRECA, their member cooperatives, industry partners and government agencies work closely to develop effective approaches to protecting the electric system. One example is the Cybersecurity Capability Maturity Model (C2M2) a public-private partnership effort that supports the adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework by assisting organizations – regardless of size, type or industry – to evaluate, prioritize, and improve their own cybersecurity capabilities. This tool was then customized for electric utilities through the creation of the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).

To further bolster the efforts of C2M2 for electric cooperatives specifically, NRECA's Business and Technology Strategies (BTS) developed a "Guide to Developing a Cyber Security and Risk Mitigation Plan" which includes tools and processes cooperatives (and other utilities) can use today to strengthen their security posture and chart a path of continuous improvement. All co-ops participating in NRECA's Regional Smart Grid Demonstration are using these tools to develop a smart grid cyber security plan. The continued engagement on development and

improvement to cybersecurity programs and tools – combined with access to actionable relevant information, both classified and unclassified – is vital when it comes to security postures in critical infrastructures.

As mentioned earlier, the ESCC serves a role in these efforts as a place for the sector to work with government to coordinate policy-level efforts to prevent, prepare for, and respond to, national-level incidents affecting critical infrastructure. The major trade associations and industry work together with government to improve cyber security through the ESCC. These efforts include: planning and exercising coordinated responses; ensuring that information about threats is communicated quickly among government and industry stakeholders; and deploying government technologies on utility systems that improve situational awareness of threats. At the most recent meeting of the ESCC, the government and private sector worked on a number of issues including identifying R&D needs, developing a cyber mutual assistance program, and gaining a better understanding of the Fixing America's Surface Transportation (FAST) Act provisions.

We stand ready to continue our work with our government counterparts and begin the transition into the next administration.

In addition to pulling industry leadership together with government leadership throughout the year, the ESCC also serves an advisory role with the Electricity Information Sharing and Analysis Center (E-ISAC). The E-ISAC collects and promptly disseminates threat indicators, analyses and warnings from a variety of private sector and government resources to assist electric sector participants in taking protective action. The information is handled confidentially and distributed through NERC's secure portal directly to industry asset owners and operators.

Mandatory and Enforceable Standards

To maintain and improve upon the high level of reliability consumers expect, electric cooperatives work closely with the rest of the electric industry, the North American Electric Reliability Corporation (NERC), the Department of Homeland Security (DHS), the Department of Energy (DOE), and the Federal Energy Regulatory Commission (FERC) on matters of critical infrastructure protection – including sharing needed information about potential threats and vulnerabilities related to the bulk electric system.

Approximately 60 generation and transmission and 60 distribution cooperatives must comply with some portion of NERC's reliability standards based on the criticality of the bulk electric system assets they own and operate. Since 2007, when NERC standards (reliability and cyber security) become mandatory, electric cooperative representatives have participated in numerous NERC standard development activities and those cooperatives with compliance responsibilities have been working to both comply and to demonstrate compliance through scheduled NERC audits. When covered entities are found to have violated cyber security and/or other NERC standards, they can be subjected to fines as high as one million dollars per day per violation. Sizable fines have been levied when entities have been found in violation and as a utility CEO I can tell you that we take compliance with the NERC standards very seriously.

The NERC standards development process begins with input from industry experts. After approval by industry, the NERC Board of Trustees is asked to approve the standards, which, if approved, are then submitted to FERC for their approval. Upon FERC approval, the standards become mandatory and enforceable. The electric utility Industry recently developed standards on physical security and geomagnetic disturbances (GMDs) and continues to revise and develop additional cyber security and GMD standards. NERC also has an "alert system" that provides the electric sector with timely and actionable information when a standard may not be the best method to address a particular event or topic.

How Congress Has Helped

In the first half of the 114th Congress, legislation was passed that will assist efforts in securing the grid – thank you.

As mentioned previously, the Fixing America's Surface Transportation (FAST) Act was enacted last year, P.L. 114-94, with a number of helpful provisions including:

- A plan for the Department of Energy to create a plan for a strategic transformer reserve program which assists in all-hazard recovery planning for large scale events;
- Clarification of roles and authorities when there is an imminent threat to the bulk power system as well as identifying DOE as the official lead Sector-Specific Agency (SSA) for cybersecurity for the energy sector – it was already the SSA for the sector but this was clarified to include cyber;
- FOIA exemptions for "critical electric infrastructure information" (CEII) submitted by industry to the Federal Energy Regulatory Commission (FERC) and other federal agencies.

Also enacted into law in the first half of the 114th Congress was the Consolidated Appropriations Act of 2016, P.L. 114-113, which included long-sought legislation to promote robust, multidirectional voluntary information-sharing about cybersecurity threats between and among federal agencies and critical infrastructures, including the utility industry. The implementation of this new law is still in its infancy, and the first milestones with final guidance on how to share is still in process.

How Congress Can Help

An example of where government can improve information sharing with industry is the December 2015 Ukraine event. While the content of the classified and unclassified information from the government was very helpful, the timeliness of getting specific, actionable information to industry must be improved so that we can respond as quickly as possible.

Critical infrastructure owners and operators are aware the biggest threats tend to be those that are hardest to identify – the insider threat. We urge Congress to consider legislation giving the FBI the statutory authority to assist industry with fingerprint-based, criminal and terrorist database background checks for industry-determined personnel that perform critical functions.

This would assist industry in further mitigating risks in a way we cannot accomplish at the local and state levels.

S. 3018, the Securing Energy Infrastructure Act

When I was invited to testify today I was asked to not only discuss ways the sector already protects and guards against threats to the electric grid but to also specifically speak to S. 3018, the Securing Energy Infrastructure Act. This legislation creates a pilot program to study vulnerabilities and consider new and old solutions for isolating and defending industrial control systems (ICS) which would likely be applicable to many outside of the electric sector. Participation in the study would be voluntary and includes an appropriately diverse working group. These are good goals and intentions – not all that different from those of the owners and operators who regularly consider and look at these issues nor their regulators who are tasked with overseeing a sector which utilizes ICS. However, it is important to avoid a one size fits all strategy. For example, security issues relevant for an entity on the bulk electric system may be very different from another entity due to geography, engineering architecture and redundancies among other differences, just as security issues relevant for the bulk electric system are not necessarily equivalent to issues facing the local distribution system.

Cooperatives believe building and investing in partnerships will be vital as the industry navigates this dynamic environment. We are implementing a coordinated and collaborative effort across the electricity sector to respond to threats and to vigilantly modify our tactics as needed to keep pace with these threats. For instance, NRECA's research arm mentioned earlier in my testimony, the Business and Technology Strategies (BTS) unit, leads a highly regarded $5 million cyber security research program. BTS develops products to improve the cyber security capabilities of our members, including a cutting edge early warning system, called Essence, which detects unusual changes in the behavior of a system resulting from a cyber-attack.

Conclusion

Thank you for holding today's hearing on this very important issue. I am proud of the efforts of our sector and hope that my testimony helps the Committee to better understand a few of the many activities and collaborative efforts of our industry and our federal government partners.

In closing, I thank you again for inviting me to testify today and I look forward to your questions.

Senator RISCH. Thank you very much.
Mr. Manning.

STATEMENT OF ROBIN MANNING, VICE PRESIDENT, TRANSMISSION, ELECTRIC POWER RESEARCH INSTITUTE (EPRI)

Mr. MANNING. Thank you, Mr. Chairman. Thank you, Senators and staff.

I appreciate the opportunity this afternoon to talk about the electric grid. It is a passion of mine, and anytime I talk about the grid I get excited. So I'm excited to talk about that this afternoon.

I've spent 38 years of my life dedicated to grid operations in one way or another. I've taken apart an analog relay and reassembled the analog relay. I've taken apart a digital relay. Well, I'll stop there. Perhaps I didn't reassemble that one.

But I will say that it's always exciting to talk about the electric grid. And I have watched, over the last 38 years, the transformation of our nation's electric grid from what it was to a true technological marvel that we see in operations today. After all, it's a tremendously integrated system. It's a tremendously complex engine, in fact. And in short, we deal with a unique commodity.

Electricity is a unique commodity. We make it, we move it at the speed of light, and we use it all at exactly the same time. And there's no doubt that there's such a complex system out there to manage that. And to operate that grid requires huge volumes of information. It requires constant attention. It requires constant tremendous diligence by operators like Mr. Highley here.

This is particularly true as we begin to see greater concentrations of intermittent resources such as renewable energy resources as they enter the equation. These are important resources. They are clean resources. They are a part of our future, but integrating those resources creates a greater reliability on technology.

The U.S. grid is a collaborative engine. Utilities across our country work carefully together, day in, day out, to ensure a safe, reliable supply of electricity flows from home to home. Even so, from time to time, we face threats that challenge the reliability that for which we become known. And many of these threats are predictable and become very manageable, like evening thunderstorms.

Yet, we're also seeing an emerging class of threats which we have dubbed high impact, low frequency events that are less predictable. They're more problematic when it comes to preparation and recovery. And certainly much of the discussion this afternoon centers around cyber security threat, but utilities are evaluating risk and threats from many potential hazards and each of these potential hazards have to be evaluated and understood so that determination can be made regarding strategies to address the entire array of potential threats.

And we can learn from the threat analysis that is taking place and from the approach taken with other high impact, low frequency events, such as the threat, for example, of electromagnetic pulse, or EMP, on the grid. EPRI is initializing a broad collaborative effort with the assistance of the Department of Energy and the ESCC, as Mr. Highley spoke. And in doing so, we are adopting a consistent methodology used to develop a deeper understanding of threats and mitigation options.

This mitigation, this methodology, highlights a scientific approach to adopting change within the complex U.S. grid. The methodology is a tried and true method of threat mitigation. It requires systematic research and development, and it provides a scientific basis underpinning to any significant change initiative.

Essentially, the methodology requires a clear characterization of the threat and identification of potential vulnerabilities, evaluation of the impacts and risk and identification of mitigation, hardening and recovery practices and tools and a well-defined decisionmaking process that considers the balance of risk and reward.

Finally, we need to ensure that there are trials, that there are pilots, so that we understand the true implications of applying changes to a very complex system. We believe following an approach such as this one ensures there are no unanticipated impacts any time you introduce change into a complex system like the U.S. grid, even a change that is designed to simplify.

The MP initiative provides a solid technical approach that it considers all impacts, mitigation, recoveries, even the cost to implement, allowing utilities to take these considerations and balance them against effective risk making decisions.

So, we at EPRI, we were created to serve the public good. We do that by providing a scientific basis for safe, reliable, affordable and environmentally responsible energy. And it is this consistent supply of energy that fuels our nation. But it is the well-rounded, thoroughly understood science that is the underpinning of this energy supply and its carefully constructed research and development that is the pathway to lighting our future and negotiating all manner of threats, even ones so ominous as cyber security.

I couldn't help but be struck, Mr. Chairman, by your comment. It is science that answers the question, can we do it better? Should we do it differently?

Thank you very much. I look forward to your questions.

[The prepared statement of Mr. Manning follows:]

Written Testimony

Hearing of the Senate Committee on Energy and Natural Resources
Subcommittee on Energy

United States Senate

Mr. Robin Manning
Vice President, Transmission
Electric Power Research Institute

"Hearing to receive testimony on S. 3018, the Securing Energy Infrastructure Act, and to examine protections designed to guard against energy disruptions"

July 12, 2016

The Electric Power Research Institute (EPRI) conducts research and development relating to the generation, delivery, and use of electricity for the benefit of the public. An independent, non-profit organization, EPRI brings together its scientists and engineers, as well as experts from academia and industry, to help address challenges in electricity, including reliability, efficiency, affordability, health, safety, and the environment. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries.

The subject of today's testimony is the impact on the power industry of potential cyber and physical security activities, including high-impact, low-frequency (HILF) events. Although EPRI recognizes the introduction of S. 3018, today's testimony addresses the technical aspects of these events, rather than any proposed legislation. HILF events include severe weather and other natural events; cyber, physical, or coordinated attacks; pandemics; unanticipated severe shortages of fuel or water for power generation; and electromagnetic pulse (EMP) and intentional EM interference (IEMI) attacks. There are inherent vulnerabilities in the transmission grid system to these threats because the severity is generally greater than the design basis for the system. To eliminate these vulnerabilities would be cost prohibitive and would thwart the objective to provide reliable, safe, environmentally responsible, *and* affordable power.

A prudent approach is to assess the vulnerabilities, understand the impacts should these types of events occur, and develop cost-effective countermeasures to reduce the risk by increasing system resiliency. In the context of the transmission system, resiliency is the ability to harden the system against—and quickly recover from—HILF events, which include both severe weather (including space weather), and man-made attacks. HILF events can disrupt generation, transmission, and distribution systems, as well as interdependent systems such as natural gas pipelines, other fuel transport channels, and telecommunications. There are a large number of possible mitigating technologies from which to choose to enhance transmission resiliency in the face of potential HILF events.

My testimony today focuses on the security considerations of HILF events, specifically: 1) the threat of HILF events to the grid including EMP, geomagnetic disturbance, and IEMI; 2) risk management approaches to address EMP threats; 3) EPRI's recently-launched EMP research program; 4) the threat of cyber security to the grid; and 5) risk management approaches to address cyber security. Physical

security can also be considered a HILF threat; however, the topic of physical security is quite broad and as such will be considered outside the scope of today's brief remarks. All remarks are based upon EPRI research as well as industry knowledge and documents available in the public domain.

Electromagnetic Pulse

Electromagnetic pulse (EMP) and geomagnetic disturbance (GMD) are often discussed together when evaluating potential impacts on the power system and approaches for improving system resiliency. While these events are both considered HILF events (along with physical attacks, severe storms, earthquakes, and other events), there are very important differences between EMP and GMD events that should be understood when evaluating resiliency improvement priorities and investment decisions.

- EMP refers to a very intense pulse of electromagnetic energy, typically caused by detonation of a nuclear or other high-energy explosive device. High-altitude EMP (HEMP) is a nuclear warhead detonated hundreds of kilometers above the Earth's surface to produce more widespread effects (areas affected can be hundreds of kilometers in diameter). It is generally accepted that a HEMP will require a high-altitude delivery device (e.g., a missile) which will require a high level of sophistication and logistics. As a result, the HEMP threat is most often associated with potential attacks from nation-states.
- EMP events are intentional, man-made attacks of electromagnetic energy specifically for the purpose of disrupting and/or damaging electrical/electronic systems. The three categories of EMP may have different impacts on transmission systems (see figure 1).
    - E1—Very fast rise time, may result in damage to electronic components either directly, or indirectly by coupling into the attached wires. GMD events do not have this characteristic.
    - E2—Characteristics are similar to lightning and consequently can result in damage to electronics and potential flashover of distribution class insulation. Neither GMD nor IEMI have this characteristic.
    - E3—Characterized by a longer duration and low-frequency content similar to GMD but much shorter in duration. EMP has two potential grid impacts resulting from the flow of geomagnetically-induced currents (GICs): 1) voltage collapse due to increased reactive power consumption and misoperation of protection systems due to harmonics, and 2) additional hotspot heating in transformers.
- EMPs can occur with little or no warning. With the possible exception of enhanced visibility tools, most operational strategies are inapplicable. Therefore, response to the EMP threat generally comes in the form of hardening assets ahead of time to reduce initial damage, reducing the duration of the interruption, and providing workable routes to recovery.

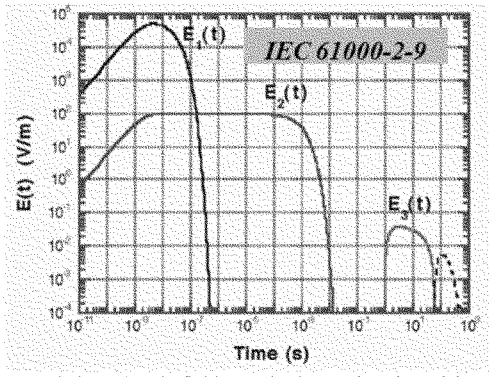


Figure 1. EMP Characteristics: Electric field magnitude as a function of time for an EMP pulse.

Geomagnetic Disturbance

- Geomagnetic disturbances (GMDs) are natural phenomena which induce slowly changing, quasi-direct currents onto the power grid. These currents are similar to those created in an E3 EMP event; however, the duration of the E3 pulse is much shorter than a GMD.

- Locations that are closer to the Earth's poles are more susceptible to GMDs than lower latitudes. Space weather warning systems provide estimates of GMD activity as much as four days before the storm reaches Earth. These systems use direct observations of the sun. Accuracy of the forecast improves when the storm reaches NOAA's DSCOVR satellite, about one hour before the storm reaches the Earth. DSCOVR is an Earth observation and space weather satellite launched on February 11, 2015. It is positioned at the Sun-Earth L_1 Lagrangian point, 930,000 miles from Earth, to monitor solar wind conditions; provide early warning of approaching corona mass ejections; and observe phenomena on Earth including changes in ozone, aerosols, dust and volcanic ash, cloud height, vegetation cover, and climate.

- Monitoring systems have been installed in multiple locations which measure the GIC currents in transformers across the grid.

- GMD events, many of which are low magnitude, occur on a regular basis, which enable grid operators to improve their understanding of the phenomena, determine the impacts on the grid, and evaluate trial countermeasures. These storms can provide an indication of the grid's response to severe storms, and support development of prudent operational strategies.

- The inherent nature of GMD phenomena do not threaten ground-based grid electrical components. Large equipment heating and voltage stability are the primary challenges.

- Although severe storms can occur any time during the approximately eleven-year solar cycle, more storms occur during the peak of the solar cycle.

- GMD storm duration can be in the order of hours or days, while the duration of EMP is considered to be in the order of minutes.

- Utilities have established operational strategies to mitigate risk during GMD events. NERC has two compliance requirements in place or in approval; EOP-010-1 and TPL-007-1. EOP-010-1 is in place and requires utilities to have operational procedures to mitigate the effects of GMD events, while TPL-007-1, is waiting FERC approval and would require utilities to: 1) perform vulnerability assessments of their systems to determine the potential impacts of a 1-in-100-year GMD event, and 2) develop mitigation measures if performance criteria are not met.

Intentional Electromagnetic Interference

Like EMP, intentional electromagnetic interference (IEMI) generates and delivers electromagnetic energy. IEMI is generated and delivered locally, and employs no nuclear material. IEMI devices have the potential to impact electronic assets in nearby locations such as control centers. Critical electronic equipment in these locations include relays, supervisory communications and data acquisition (SCADA) systems, communication networks, and energy management systems (EMS).

Individual grid components are inherently vulnerable to these threats because the severity is generally greater than the design basis for the system. Today's power systems are operating in an increasingly complex electromagnetic environment in which large current and voltage components, sensitive electronics, digital signals, and analog waveforms coexist and interact. The widespread proliferation of smart grid systems, including substation automation and syncrophasor systems, are part of this increasing complexity. However, extensive grid-wide damage by IEMI would require a tremendous coordinated effort as the loss of individual components do not, in and of themselves, cause cascading loss of the grid. NERC CIP-014 would require utilities to protect their system against that risk and develop mitigation strategies if they do not meet the specified performance criteria.

Risk Management Approaches to Address EMP Threats

EPRI is working with industry stakeholders to characterize EMP threats, including HEMP attack, EMP, and local IEMI attack. This work is providing the design basis for assessing vulnerability and developing mitigation strategies. EPRI is gathering available data on component vulnerabilities to the benchmark threats. The results, when complete for all critical components, will support calculation of the system impact. EPRI is gathering leading practices by electricity providers who have applied trial implementation of countermeasures to reduce vulnerability.

A number of risk-management approaches can be considered to reduce the impact of EMP on the transmission system. Some of these methods are being considered by various utilities for implementation:

Risk Assessment
Prudent application of scarce resources requires careful countermeasure and site selection procedures. While it may be difficult to identify regions of the grid that are more likely to be attacked by an EMP, it may be possible and prudent to identify and focus resources on the most critical components necessary for the reliable operation of the transmission system.

Hardening of Assets
Hardening for new and existing systems generally focuses on reducing the impact of electromagnetic waves on electronic equipment. Some hardening options include:

- New control rooms with EM shielding in the form of a Faraday cage are being implemented at some locations. External cable entrances must be considered, including the number and location of penetrations as well as the implementation of surge protection, filtering, and grounding strategies. Other challenges include staff entrances/exits and ventilation ducts.

- New relay houses that are EMP-hardened are being developed and tested by some utilities. These relay houses use metal buildings with special consideration given to ensure bonding of metal members, improved grounding, and cable entrances.

- The use of power supply and communication cables with integrated shields, as well as consideration for the grounding strategies for these shields, is being implemented (e.g., individually-shielded, twisted pair cables with an overall shield that is grounded).

- Surge protection and grounding of cables entering and exiting the facilities is routine practice due to everyday lightning activity that could affect the electronic equipment.

- Interference filtering can be applied at cable entry points to reduce high-frequency conducted energy that can impact the attached electronic activity.

- Relocation of unprotected, sensitive control equipment to inside the shielded enclosures.

- Relocation of control cables to a lower EM environment, such as conductive conduit, to reduce induced voltage.

- Increase the use of fiber-optic cables rather than metallic cables for communications. Fiber-optic cables have much lower susceptibility to EM impacts.

- Utilities are engaging original equipment manufacturers (OEMs) to incorporate EM resiliency into new components, such as relays and communications systems.

- Neutral blockers for transformers to reduce the impact of GMD are being evaluated. These blockers may aid in the reduction of induced E3 currents. The impact of neutral blockers on system operation requires consideration.

Recovery Options

- Consider spare parts. Because a severe EMP attack can damage key electronic system components, strategic stockpiling is prudent. Sparing can be considered for relays, which are susceptible to the E1 and E2 component of an EMP. Storing critical spares in shielded EM enclosures is a consideration.

- Other equipment that supports restoration could also be protected from EMP. This includes equipment associated with black start, backup communications systems, transportation, and

diagnostics components.

- Asset owners may consider adding the EMP threat to their transformer spare parts strategy. Lower voltage transformers below 69 kV can be affected by the E1 and possible E2 portions of an EMP if they are not protected with surge arresters. Larger power transformers are unlikely to be impacted directly by E1 or E2.

- In addition to spares, mobile systems to support recovery can be considered, such as mobile transmission capacitor banks, mobile substations (typically for distribution), and mobile substation control houses.

- Redundant systems that are not susceptible to EMP, such as electromechanical relays, can be applied.

- Utilities may consider disconnecting, and possibly grounding, redundant relays and communication systems, so that they are available after an EMP. However, caution is warranted for this approach because system resiliency to traditional threats may be compromised.

- Restoration plans and training can be embellished to incorporate recovery from EMP. Relay technicians will be especially important to EMP recovery.

EPRI's EMP Research Project

Electromagnetic pulse events are a growing concern in the energy business. While the industry has worked to develop effective responses to GMD, little definitive work has centered on the effects of an EMP attack.

Numerous constituencies are pressing to ensure the electric power system is more resilient to a large EMP event, but technical information is inconsistent and options to increase resilience through hardening and recovery are not well-defined. Some proposed approaches are high-cost and lack the technical basis to substantiate their viability.

EPRI is collaborating with the U.S. Department of Energy to develop objective options to respond to the EMP threat. EPRI's EMP research project intends to provide a sound, technical basis by which utilities can effectively evaluate potential impacts, mitigation, and recovery plans.

EPRI's three-year, collaborative research effort aims to characterize specific EMP threats, assess substation component vulnerability, assess methodologies for determining system impact, and assess or develop mitigation strategies—including hardening and recovery—to enable utilities to make important decisions about system resiliency.

Cyber Security

With the increased use of digital devices and more advanced communications and other information technology (IT), the overall attack surface has increased. For example, substations are modernized with new equipment that is digital, rather than analog. These new devices include commercially available operating systems, protocols, and applications as an alternative to proprietary solutions that are specific

to the electric sector. Many of the commercially available solutions have known vulnerabilities that could be exploited when the solutions are installed in operational technology (OT) system components. Potential impacts from a cyber event include: billing errors, brownouts/blackouts, personal injury or loss of life, operational strain during a disaster recovery situation, or physical damage to power equipment.

The nation's power system consists of both legacy and next generation technologies. New grid technologies are introducing millions of novel, intelligent components to the electric grid that communicate in much more advanced ways (e.g., two-way communications and wired and wireless communications) than in the past. These new components will operate in conjunction with legacy equipment that may be several decades old, and which provide no cyber security controls. Traditional IT devices typically have a life span of three to five years. In contrast, OT devices can have a life span of up to 40 years or longer. With the constantly changing IT and threat environments, addressing potential cyber security events is a challenge.

Another change is the convergence of IT and OT. Historically IT has included computer systems, applications, communications technology, and software to store, retrieve, transmit, and process data typically for a business or enterprise. OT has historically focused on physical equipment-oriented technology that is commonly used to operate the energy sector. Multiple groups and operators often independently gather and analyze information from isolated and "stove-piped" systems that have been developed to provide security monitoring for physical, enterprise, and control system environments. As the threat landscape has evolved, there is a greater need to have a coordinated view of all aspects of an organization's security posture (i.e., situational awareness) and events (both unintentional, such as a component failure, and malicious) that may impact an organization's security posture, and responses to those events.

Cyber Security Risk Management

Cyber security is a priority for critical infrastructures, especially electric utilities. To adequately address cyber security risks, utilities must identify basic differences between the security requirements for IT systems and the security requirements for OT systems. In general, the focus for IT systems is confidentiality of information; for example, customer energy use and privacy information. The focus for OT systems is availability and integrity, to ensure that the reliability of the grid is maintained even in the event of a cyber security incident. The OT systems also have performance requirements, and any significant delay in sending and/or receiving data and commands could adversely impact the reliability of the grid. Typical IT security controls, such as cryptography and vulnerability scanning, that have been implemented in OT systems could cause systems to fail. Because of these differences, utilities need to take care so that implemented security controls do not adversely impact the reliability of the grid.

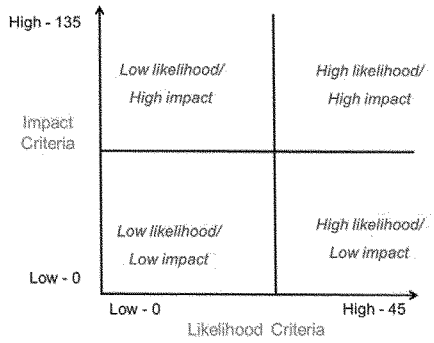
- To adequately address potential threat agents and vulnerabilities, cyber security should be included in all phases of the system development life cycle—from the design phase through implementation, operations and maintenance, and sunset. Cyber security should address deliberate attacks launched by disgruntled employees and nation-states, as well as non-malicious cyber security events (e.g., user errors, incorrect documentation, etc.). Currently, the majority of cyber security events are non-malicious.

- Cyber security must be prioritized with the other components of enterprise risk because organizations, including utilities, do not have unlimited resources, personnel, and funds. *Risk* is the potential for an unwanted impact resulting from an event. *Enterprise risk* addresses many types of risk such as investment, budgetary, program management, legal liability, safety, and inventory risk, in addition to cyber security. A cyber security risk management strategy should be a component within an organization's enterprise risk management strategy.

- Risk assessment is a key planning tool for implementation of an effective cyber security program and involves identifying threats, vulnerabilities, and the potential impact and risk associated with the exploitation of those vulnerabilities. Risk assessments are performed on systems. Once the risk is determined, the organization needs to determine a course of action: accept, avoid, mitigate, share, or transfer.

- Organizations should perform risk assessments on an ongoing basis throughout the system life cycle. The two criteria used in a risk assessment are impact and likelihood. EPRI, in conjunction with utilities, academia, researchers, and vendors, developed a risk assessment methodology that is based on a typical IT methodology with impact and likelihood criteria that are specific to the electric sector. This work was performed as part of the National Electric Sector Cybersecurity Organization Resource (NESCOR) project—a U.S. DOE funded public-private partnership.

    - Some of the NESCOR impact criteria include: system scale, safety concern, ecological concern, restoration cost, negative impact on generation capacity, and negative impact on the bulk transmission system.
    - Some of the NESCOR likelihood criteria include: skill required, accessibility (physical), accessibility (logical), and attack vector. A score of 0, 1, 3, or 9 is determined for each criterion, then a sum is calculated for impact and likelihood.
    - The resulting score can be displayed on a graph, as shown below. The systems that fall in the upper right quadrant, high likelihood/high impact, are the highest priority for the organization as are the mitigation strategies for these systems.



Cyber Security Mitigation Strategies

Utilities, government agencies, academia, research organizations, and vendors are collaborating on many projects to develop tools and techniques to address cyber security threats and vulnerabilities. This collaboration is important to ensure that the unique cyber security requirements of the electric sector are addressed.

Several requirements documents that specifically address the electric sector provide mitigation strategies. Three of these documents are highlighted below.

- The first document is the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, initially published in 2010. The development was led by NIST with a team of volunteers from the private sector, academia, research organizations, and government. Roughly 150 individuals volunteered their time to author this document. This is the first document that focused on the electric sector, and it has been distributed and used worldwide.

- A second document is the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), which guides electric utilities and grid operators in assessing their cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity. The maturity model was developed as part of a White House initiative led by DOE in partnership with the Department of Homeland Security (DHS) and involved close collaboration with industry, other federal agencies, and other stakeholders. This document is also used worldwide.

- The third document is a joint publication of DOE and EPRI, "Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology." The purpose of the report is to specify a risk assessment process that may be used by utilities. Included are high-level diagrams that illustrate the risk assessment process at the security requirements and security-control-selection stages, as well as for ongoing assessment and for assessing emerging changes. A second objective is to illustrate how to use the content of the NESCOR cyber security failure scenarios and impact analyses document in the risk assessment process.

DOE has been the designated Sector-Specific Agency (SSA) for the energy sector since 2003, and research and development has been identified in the Sector-Specific Plan (SSP) as a key source of innovation and productivity for the energy sector. Since more than 80 percent of the country's energy infrastructure is owned by the private sector, DOE has initiated several collaborative research efforts. Two are highlighted below:

- A key mission of DOE's Office of Electricity Delivery and Energy Reliability (OE) is to enhance the reliability and resilience of the nation's energy infrastructure. Cyber security of energy delivery systems is critical for protecting the energy infrastructure and the integral function that it serves in our lives. OE designed the Cybersecurity for Energy Delivery Systems (CEDS) program to assist the energy sector asset owners (electric, oil, and gas) by developing cyber security solutions for energy delivery systems through integrated planning and a focused research and development effort. CEDS co-funds projects with industry partners to make advances in cyber security capabilities for energy delivery systems.

- DOE published a *Roadmap to Achieve Energy Delivery Systems Cybersecurity* in 2011 that provides a plan to improve the cyber security of the energy sector. The strategic framework within presents the vision of industry, vendors, academia, and government stakeholders for

energy delivery systems security, supported by goals and time-based milestones to achieve that vision over the next decade.

The vision within the roadmap states: *By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.* The roadmap is an update to the 2006 *Roadmap to Secure Control Systems in the Energy Sector*. The 2011 roadmap addresses gaps created by the changing energy sector landscape and advancing threat capabilities, and emphasizes a culture of security.

Many utilities and EPRI map their R&D programs to the strategies defined in the *Roadmap* and to the domains specified in the ES-C2M2. These common categories are used by utilities, academia, and research organizations in the public and private sectors as they define and prioritize their research agendas. This is particularly important with the constantly changing threat environment.

Another NESCOR project focused on the development of *failure scenarios* for the electric sector. A *cyber security failure scenario* is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. Each scenario includes a title, short description, relevant vulnerabilities, impact, and potential mitigations. Failure scenarios include malicious and non-malicious cyber security events such as:

- Failures due to compromising equipment functionality
- Failures due to data integrity attacks
- Communications failures
- Human error
- Interference with the equipment lifecycle
- Natural disasters that impact cyber security posture

Impacts identified in the failure scenarios include loss of power, equipment damage, human casualties, revenue loss, violations of customer privacy, and loss of public confidence.

Included below is a sample failure scenario.

AMI.26 Advanced Metering Infrastructure (AMI) Prepaid Billing Cards are Compromised Resulting in Loss of Revenue

Description: The prepaid billing cards for AMI are compromised. Example compromises include tampering with cards to change the credit amount, erasing the logic that decrements the credit amount remaining, or forging cards.

Relevant Vulnerabilities:

- *System assumes data inputs and resulting calculations are accurate* on prepaid billing cards inserted into a meter.
- *System permits unauthorized changes* to AMI billing information on prepaid billing cards.

Impact:
Loss of revenue

Potential Mitigations:

- *Design for security* in the payment system.
- *Check software file integrity* (digital signatures or keyed hashes) on the prepaid billing card contents.
- *Authenticate data source* (i.e., prepaid billing cards) for AMI billing.
- *Perform security testing* as a part of system acceptance testing.

For utilities that do not have readily available cyber security staff, the failure scenarios may be used as part of the overall risk management process to begin addressing potential cyber security events. For all utilities, the failure scenarios may be used to train new personnel and for refresher training for all staff. Finally, the failure scenarios may be used as input to tabletop exercises. Tabletop exercises are discussion-based sessions where team members meet in an informal classroom setting to discuss their roles during an emergency and their responses to a particular situation. Many tabletop exercises can be conducted in a few hours.

The NESCOR failure scenarios have been used by researchers and utilities around the world.

Conclusion

Potential impacts of cyber security, EMP, GMD, and IEMIs on existing and new power grid infrastructure requires concrete, scientific evaluation and analysis. Threats must be quantified and addressed to allow for common sense and robust mitigation strategies. While we've identified several strategies in today's testimony, much more research and information is needed, especially as technology advances and as new cyber security threats enter into the equation.

EPRI will continue to offer technical leadership and support to the electricity sector, public policy-makers, and other stakeholders to enable safe, reliable, affordable, and environmentally responsible electricity.

Senator RISCH. Thank you.
Mr. Stacey.

STATEMENT OF BRENT STACEY, ASSOCIATE LABORATORY DIRECTOR, NATIONAL & HOMELAND SECURITY, IDAHO NATIONAL LABORATORY

Mr. STACEY. Chairman Risch, Ranking Member Manchin and distinguished members of the Subcommittee, I want to thank you for holding this hearing and inviting testimony from Idaho National Laboratory, also known as INL.

As a fellow citizen of Chairman Risch's home State of Idaho and the Associate Laboratory Director of INL's National and Homeland Security directorate, I'm honored to participate and request that my written testimony be made a part of the record.

INL extends its gratitude to Senators King, Risch, Collins, Heinrich, Crapo, and Murkowski for the leadership and dedication demonstrated in sponsoring Senate bill 3018 with the goal of establishing a pilot program to develop a cyber informed, engineering strategy that defends our energy infrastructure from the most serious security threats.

INL views this bill as an opportunity to perform the research and development and testing that are necessary to explore, innovate and validate with science-based data the ground truth on credible, high consequence, vulnerabilities and their mitigation.

We understand that the solutions will include advanced technologies and engineering alternatives that can be proven and practically implemented.

We believe that our understanding is consistent with the intentions and perspectives of many peers in government and in industry. My colleague, Mike Assante, the SANS Lead for Industrial Control System and Supervisory Control and Data Acquisition Securities, said it this way, and I quote, "Beyond enhancing our cyber defenses our goal is to unlock the greatest benefits that technology offers but not go so far as to ignore the select need to establish responsible limits and alternatives." This is a role appropriate for national labs.

INL, as well as other laboratories, partner today on a breadth of solutions. This research is sponsored by and coordinated with Assistant Secretary Hoffman, leading DOE's Office of Electricity Delivery and Energy Reliability, DOE's Office of Nuclear Energy, the National Nuclear Security Agency's Office of Defense Nuclear Non-Proliferation and DOE's Office of Intelligence and Counter Intelligence.

Our utilities have been efficient and effective in positioning the electric sector's infrastructure for functionality, reliability and safety and in raising their cyber security awareness and posture. Yet, with the advent of sophisticated and adaptive cyber adversaries, we are now faced with the need to enhance our infrastructure security that it can better detect, resist, absorb and respond to the most sophisticated cyber attackers.

INL's vision for control system cyber security research is grounded on the following principles and trends. First, the speed of technological innovation is outpacing traditional approaches. Second, determine sophisticated and patient adversaries will be successful

in penetrating an infrastructure's digital systems. Third, a disciplined adversary likely will know the dynamics of digital technology better than the asset owner and the asset owner will know their engineering and processes better than the adversary. We need to leverage our knowledge advantage and strengths. And fourth, technology for automation and digital control are inherently embedded into our infrastructure. It's simply not feasible to go back and implement large scale manual control.

At INL, we believe that unexplored options exist for taking consequences off the table. To this end, INL is piloting a transformative approach. We call it consequence driven, cyber informed, engineering, or CCE for short.

CCE reprioritizes the way we look at high consequence risk within control system environment. This process starts with identifying the highest impact, most severe consequence and then discovers the best process design and protection approaches for engineering out the cyber risk. Further reducing risk will require government research and industry toward a common goal complemented by investment in over the horizon research and development addressing these holistic solutions.

An example of a significant step forward in partnering within national laboratories to address this national challenge, INL, Pacific Northwest National Laboratory and Sandia National Laboratories are teaming to lead a research initiative that holistically addresses control system, cyber security across multiple sectors of the infrastructure and government.

I thank the Committee's members and fellow panelists for their dedication to this complex challenge. Protection of the energy sector deserves our full commitment to assure economic prosperity and energy security, and INL welcomes its role in serving the nation.

Your commitment to this hearing, the high quality of peers as my fellow witnesses, your proposed legislative actions and appropriations for research demonstrate that the nation is actively engaged in addressing this challenge.

Thank you for inviting me today to testify, and I look forward to your questions.

[The prepared statement of Mr. Stacey follows:]

STATEMENT OF
MR. BRENT J. STACEY, ASSOCIATE LABORATORY DIRECTOR
NATIONAL & HOMELAND SECURITY

IDAHO NATIONAL LABORATORY

BEFORE THE

UNITED STATES SENATE
SUBCOMMITTEE ON ENERGY
COMMITTEE ON ENERGY AND NATURAL RESOURCES

JULY 12, 2016

Mr. Brent J. Stacey, Associate Laboratory Director, Idaho National Laboratory National and Homeland Security Division

U.S. Senate Hearing to receive testimony on S.3018, the Securing Energy Infrastructure Act, and to examine protections designed to guard against energy disruptions

Introduction

Chairman Risch, Ranking Member Manchin, and distinguished members of the Subcommittee; I want to thank you for holding this hearing and inviting testimony from the Department of Energy's Idaho National Laboratory, also known as INL. As a fellow citizen of Chairman Risch's home state of Idaho and the Associate Laboratory Director of INL's National & Homeland Security Directorate, I am honored to participate with this most distinguished panel in the national discussion on the role of technology and research in assuring the security of the energy sector, one of the lifeline sectors within the 16 sectors of our critical infrastructure. I request that my written testimony be made part of the record.

S.3018 "Securing Energy Infrastructure Act"

INL extends its gratitude to Senator King, Senator Risch, Senator Collins, Senator Heinrich, Senator Crapo and Senator Mikulski for the leadership and dedication demonstrated in sponsoring S.3018 – with the goal of establishing a pilot program to develop a cyber-informed engineering strategy that defends our energy infrastructure from the most serious of security vulnerabilities. Electricity and the grid are essential in all sectors of our infrastructure, including transportation, communications and water.

The grid plays a central and unique role in our national security and public safety. Components within S.3018 support the objectives of ongoing and proposed research, development and testing within the Department of Energy (DOE) laboratories. Additionally, this bill has elevated the public discourse on a number of factors, including: 1) the benefits of how digital control systems and communications improve safety, reliability and efficiency; and 2) the security risks of cyberattack on individual components, systems and interdependent infrastructure.

This public discourse also has included discussions regarding slowing or stopping the implementation of advanced technology within certain, highly selective elements of the energy sector to eliminate the risks of cyberattacks that could result in high-consequence events from sophisticated adversaries who are focused and capable of conducting targeted attacks on power systems.

Outside of the policy debate, INL views this bill not as taking a step to limit the implementation of advanced technologies, but rather an opportunity to perform the research, development and testing necessary to explore, innovate and validate, with science-based data, the ground truth on credible, high-consequence vulnerabilities and the best way to mitigate these vulnerabilities.

We understand that the solutions resulting from this science-based ground truth on vulnerabilities and mitigation will include advanced technologies and all other practical solutions that can be proven and practically implemented to protect our national energy sector. We believe that our understanding also is consistent with the intentions and

perspectives of many peers in government and industry. My colleague, Mike Assante, the SANS lead for Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) Security, said this: "*Beyond enhancing our cyber defenses, our goal is to unlock the greatest benefits that technology offers, but not go so far as to ignore the select need to establish responsible limits and alternatives.*"

Consistent with the language in the legislation, this is a role that is most appropriate for national labs. INL, as well as many other laboratories, partner on the research and implementation of a breadth of solutions with public utilities and control system vendors. This research, detailed later in this testimony, is sponsored by and coordinated with DOE's Office of Electricity Delivery and Energy Reliability, DOE's Office of Nuclear Energy, the National Nuclear Security Agency's Office of Defense Nuclear Nonproliferation, and DOE's Office of Intelligence and Counterintelligence.

Based on the ubiquitous nature of industrial control systems, their protocols, and often their automated operational functions, there is an economy-of-scale benefit of this research across all 16 sectors of critical infrastructure, the Department of Defense, Department of Homeland Security and many other federal, state and local governments. The integration and coordination of this cross-sector work is becoming significantly more important as we seek to address the challenges of preventing catastrophic, cascading, high-consequence events from sophisticated, highly adaptive cyber adversaries.

Idaho National Laboratory's role in Infrastructure Security

INL has the mission to discover, demonstrate, and secure innovative nuclear energy and critical infrastructure solutions. To achieve our mission and vision for securing critical infrastructure, INL provides the nation with the scientific capabilities, world-class research expertise and unique experimental infrastructure to conduct the complex research, development, demonstration and testing that are needed to protect the energy sector's infrastructure. INL's national security R&D emphasizes physical protection against ballistics, explosives and natural phenomena, such as solar storms, as well as the cyber protection of advanced digital controls, embedded and wireless communication systems.

INL's leadership and partnership with other federal agencies and industry in the protection of the nation's infrastructure is grounded on an accumulated history of innovations in risk and vulnerability assessment; infrastructure interdependency modeling and simulation; technical threat analysis; scaled testing of physical and cyber threats; and the deployment of information and technology solutions that assist public and private stakeholders in preventing, mitigating and recovering from natural and man-made threats.
Examples include:

1) The "Aurora project test," which was performed for the Department of Homeland Security (DHS), during which an electrical generator was destroyed by exploiting a cyber-physical vulnerability.
2) The completion of more than 100 cybersecurity assessments on vendor and asset-owner control systems in support of the DOE Office of Electricity Distribution and Energy Reliability's National SCADA Test Bed.
3) First-of-a-kind, grid-scale, ground-induced current tests for the Department of Defense and DOE to establish a scientific baseline for understanding the threat to the power grid from geomagnetic disturbances (GMD).

4) Multitudes of industrial control system cyber threat reports and advisories, on-site cyber assessments, interdependency analyses, and training sessions with government and industry for the Department of Homeland Security Industrial Control System Cyber Emergency Response Team (ICS-CERT), DOE, and Department of Defense.

Our U.S. utilities have been efficient and effective in engineering and maintaining the electric sector's infrastructure for functionality, reliability and safety – and in raising their cybersecurity hygiene through the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) standards. Yet, with the advent of sophisticated and adaptive cyber adversaries, such as seen during the attack against the grid in Ukraine, we are now faced with the need to enhance our critical infrastructure's efficiency, reliability and safety by implementing effective security features that can detect, resist and respond to the most sophisticated cyberattacks.

Principles and Trends

INL is committed to perform our national laboratory's role to advance scientific knowledge and to help transform the security of our national infrastructure. Our vision for control systems cybersecurity research is grounded upon the following principles and threat trends:

1) Cyber risks to critical industrial control systems and networks are serious and are taken seriously by industry and government.
2) The U.S. and our allies are playing catch-up in research investments and validation of assessment results given the complex co-dependencies of technology, engineering, and process.
3) The speed of technological innovation is outpacing our traditional approach to solve the problem by using standards and policies.
4) Determined, sophisticated and patient adversaries will be successful in penetrating an infrastructure's digital systems.
5) A disciplined adversary likely will know the dynamics of industrial control system (ICS) technology better than the asset-owner. Since the asset-owner will know their engineering and operational/business processes better than the adversary, we need to leverage our detailed engineering and process knowledge for a higher level of cyber protection.
6) While we are catching-up with incremental improvements to harden our defenses and better detect and respond to a cyberattack, we also can make progress if we identify and focus protections on the few areas where we have made engineering and business decisions that leave us exposed to high national security level risks. These areas of high risks are where we can re-design and develop engineered barriers or cyber-informed human responses as last lines of defense to remove the possibility of a significant consequence.
7) Cyber authorities, system defenders and research efforts are spread across multiple government, academic and industry organizations. Access to this dispersed advanced control systems security talent is limited and does not facilitate response in a coordinated and integrated manner to prioritize resources on high-consequence vulnerabilities. Additionally, robust and resilient security solutions to address threats to functional cyber-physical systems require access to multidisciplinary operational and engineering teams and realistic at-scale experimentation environments. We have observed that unique integrated staff and facilities for research and protection of our

infrastructure reside within the DOE laboratory complex and within a few select organizations across the federal government and industry.

8) Technology advances for automation and digital control are inherently embedded into our energy infrastructure. The opportunity to go back decades to implement large-scale manual control and response is unfeasible relative to the benefits from diversifying our energy supply with renewables, providing service and reliability into rural regions, and managing costs by balancing supply and loads.

Consequence-Driven Cyber-Informed Engineering

INL is piloting a transformative approach. Consequence-driven Cyber-informed Engineering (CCE) reprioritizes the way the nation looks at high-consequence risk within the control systems environment of the most essential infrastructure assets. Our goal is to provide both private and public organizations with the tangible steps and tools required to examine their environments for high-impact events/risks; identify implementation of the most likely digital devices and components that facilitate that risk; illuminate specific, plausible cyberattack paths for these digital devices; and develop concrete mitigations, protections and tripwires to address the high-consequence risk. The ultimate goal of the CCE effort is to help organizations take the steps necessary to thwart cyberattacks from even the most highly resourced, top-tier adversaries that would result in a catastrophic physical effect.

The CCE framework research is built upon three generally recognized realities of control systems cyber space:

1. Asset-owners must recognize the difference between targeted and indiscriminate attacks, and accept that if targeted by an advanced cyber adversary the asset-owner will be compromised.
2. Traditional IT security defenders primarily are focused on cyber hygiene which, while critical to an overall cybersecurity strategy, is only sufficient to repel non-targeted attacks, rather than the cyber-physical effects of a high-consequence event. Minimizing these effects, along with the potential impacts of an advanced persistent threat, depends upon the highly technical skills available through government assistance.
3. Control systems are most often designed to meet functional engineering and safety requirements, not security requirements. As such they are designed and programmed around failure mode analysis of the function rather than incorporating improved risk-based and synergistic security profile.

When INL pilots this CCE approach with utilities and government organizations, we work with them to tackle the challenge by advancing through four distinct phases:

1. Consequence Prioritization. The entity and government partner identify the highest-consequence event that would pose a risk to national security - for example, loss of electricity to a large segment of a utility's customers for eight days or longer.
2. System-of-Systems Breakdown. The entity evaluates its infrastructure and operational processes to identify critical functions and services that are linked to the highest-consequence event. This process can be thought of as an engineering analysis process.
3. Consequence-based Targeting. This phase builds on how an adversary achieves a specific impact against a target system. The entity and INL cooperatively share information to answer this question: "Is there anyway an adversary can achieve a negative impact through cyber to this function?" Using the ICS Cyber Kill Chain (a

high-level model that emulates the steps used by an adversary), the entity can identify steps necessary for an adversary to be successful against a specific system(s).

4. Mitigations and Protections. The goal of this phase is to intelligently improve the security posture based on development and implementation of physical, infrastructure, digital, engineering or operational change(s) that interrupts the attack vector against credible target systems.

INL is currently validating this approach in several sectors through pilot projects. Some lessons being learned as critical to the future success of this approach are:

1) We will benefit from more effective translation of classified threat information about the specifics of threat actors' technology readiness capabilities and intentions to do damage into "actionable intelligence," information that is specific, prioritized and implementable into changes in an asset-owner's systems and processes.
2) We can benefit by optimizing and coordinating research, expertise and information-sharing forums to gain economy-of-scale in solving high priority ICS cybersecurity challenges. There is much commonality among the control systems and their protocols that generally are ubiquitous across the sectors of critical infrastructure. Hence, much of the technical threat and technical solution information developed for a high priority vulnerability will be useful to many others.

Partnership is Critical

The challenge of protecting our energy infrastructure is vital and complex. By complex I mean that it is technologically complex, institutionally complex and politically complex. Our energy infrastructure is an integrated system that must be protected on multiple fronts. Our country needs short term tactical solutions, but it also needs foundational work that provides longer-term holistic system solutions. Reducing risk through the energy infrastructure will require the rallying of government organizations, national laboratories, industry and industry trade groups, other research organizations, and academia working together as a team towards a common outcome. This teaming will require commitment, trust, resources, and leveraging of each partner's unique roles and strengths. The nation needs increased investment in long-term over-the-horizon research and development addressing holistic solutions that fundamentally reduce the system risk to our energy infrastructure.

An example of a significant step forward in partnering within national laboratories to address the national control systems cybersecurity challenge, INL, Pacific Northwest National Laboratory, and Sandia National Laboratories are teaming to lead a research initiative that holistically addresses control system cybersecurity. This initiative will: 1) provide a forum to focus government and other research investments on solving the control systems cybersecurity research challenges found within the most common control systems that have great potential for high-consequence; 2) advance the fundamental science and engineering needed to develop and implement cybersecure control systems; and 3) integrate research, training and education to develop the national technical expertise and workforce capacity to support government and industry.

This initiative's success in enhancing the protection of critical infrastructure is dependent upon broad national support that enables the future priorities and resources for research programs; creates a current, anticipatory and actionable collaborative information-sharing environment; and implements adaptable, forward-leaning technologies, standards, policies and regulations.

Summary

I thank the Committee's members and fellow panel members for the honor of serving as a witness on this complex challenge, one that requires comprehensive action across technology, policy and regulation. Protection of the energy sector, as well as the other sectors of critical infrastructure, deserves our attention and commitment to assure our economic prosperity, national defense and public safety. INL welcomes its role in serving the nation as a unbiased technology 'broker' for protection of our critical infrastructure by developing and validating credible threats and their consequences; developing, testing and demonstrating the effectiveness of innovative security technologies; conducting experimentation that establishes the science- and engineering-based data to support policy; and performing the threat analyses and risk assessments that support industry's implementation of protective measures and regulatory actions.

The pace of the evolution of the threat balanced against the economic factors accelerating the implementation of advanced technologies calls for a unified team of stakeholders interested in addressing the challenge. This teaming includes government, researchers, vendors, asset-owners and regulators.

Your commitment to this hearing, the high quality of peers as my fellow witnesses, and your proposed legislative actions and appropriations for research, demonstrate that the nation is actively engaged in addressing this challenge.

Thank you for inviting me today to testify, and I look forward to your questions.

Senator RISCH. Thank you, Mr. Stacey.

Thank all of you for your well advised thoughts and we really appreciate that. Hopefully we will all be able to move this forward together.

We are going to go to a round of five minute questions. Since we do have the vote at 3:30, I would urge everybody to be as succinct as they can in their questions and answers. I want to have everybody have an opportunity, so I will pass. I will waive, at least at the outset, and proceed to Senator Manchin.

Senator MANCHIN. Thank you. Thank you, Mr. Chairman.

My one concern is the reliability of the grid and if you are concerned about that base load fuel being in jeopardy of giving you the necessary reliability. Do any of you have concerns about that with so much of our base load being diminished?

Very quickly, anybody? Do you want to start, Mr. Manning?

Mr. MANNING. So it does change. It changes the equation. So we have designed——

Senator MANCHIN. We are talking base load, mostly, the fossils have come offline. Okay, we understand that and we know there is a transition going on.

But are we in jeopardy of the system basically not being able to provide reliability?

Mr. MANNING. No, I don't believe we're in jeopardy.

Senator MANCHIN. Okay.

Mr. MANNING. But I do think we have to operate the system differently tomorrow than we operated the system.

We spent 80 to 100 years operating it a certain way. And the generation of today is very different from the traditional generation and is creating new operational protocols, is demanding new technologies and we're implementing those as we go. But I believe with Pat's help, with the help from FERC and from NERC, we're managing that effectively.

Senator MANCHIN. My main concern on that was with the polar vortex. PJM has about 61 million customers, and that is in all of our area. They came within a razor's thin of collapsing.

Have you all been able to shore that up so that won't happen again? Mr. Highley.

Mr. HIGHLEY. When we plan the grid we're always planning 10 to 15 years out. And so, we're definitely looking at the loss of those coal and fossil assets and making the mitigation plans now where transmission lines might be needed or gas pipeline infrastructure might have to be enhanced.

Senator MANCHIN. Were you all aware of how critically close that become?

Mr. HIGHLEY. Absolutely. It was also close in Arkansas that same winter.

Senator MANCHIN. Okay.

Now I will go to the shrinkage. We call it shrinkage or loss. Six percent of electricity is lost when it is transported from generation facilities across transmission with the current technology that we have and the current products we are using. That is enough I understand to power two million homes for one month. We are losing that much on the grid system.

Are there any changes, technology wise, that would give us more efficiency so we don't have that much loss?

Ms. Hoffman, do you know of any?

Ms. HOFFMAN. So yes there is technology opportunities to improve efficiency on the system.

With respect to the distribution system and some of the Recovery Act activities, we did look at conservation voltage reductions, really looked at better optimization and utilization of the distribution system.

But there's also composite conductors, more efficient conductors out there that can support capacity on the transmission system as well as information technology such as the dynamic line rating. But really to be able to maximize the use of the transmission system, those are all some of those technologies.

Senator MANCHIN. Are we changing the quality of products that we are using or the composition of the products such as ceramics? Are we using ceramics that I understand are much more efficient?

Mr. HIGHLEY. I just might add on the transformers we're buying power transformers.

We price in what the lifetime losses would be on that. So it's a cost benefit analysis. The losses that we incur are losses that are incurred because it's not cost effective to make them lower, and when we buy that transformer we price that in.

The ceramic technology comes at a price. There's limited applications where that works, but most of the time you can't afford it because the energy you're saving isn't worth it.

Senator MANCHIN. A final question, very quickly, to either Mr. Stacey or Mr. Manning.

Which country do you think poses the greatest threat for cyber security as far as the grid to the United States of America? What organization or country?

Mr. STACEY. I would offer the industrialized countries have the capability in many cases.

Senator MANCHIN. Which one has the desire and the interest?

Mr. STACEY. Well, there are probably a couple.

Senator MANCHIN. Do you want to name any names or do you just want me to name them for you?

Mr. STACEY. I'd prefer not, but I would say the industrial countries.

Senator MANCHIN. Mr. Manning?

Mr. MANNING. That was a fantastic answer. I should say——

Senator MANCHIN. Are we talking China or Russia or Russia and China?

Mr. MANNING. Yes, you are.

Senator MANCHIN. Which one first?

Mr. MANNING. So I'm not sure it matters which is first. I think we were vulnerable to all. My answer was going to be foreign countries.

Senator MANCHIN. Foreign. [Laughter.]

Mr. MANNING. But I thought that was a very good answer. Industrialized is a greater threat.

Senator MANCHIN. I got you. It was very nice.

Thank you very much. Thank you all.

Senator RISCH. Senator Cassidy.

Senator CASSIDY. Some folks from Bossier City, Louisiana, the site of our Innovation Center, had a conversation with a colleague of yours, Mr. Bachman. He differentiated between, let's see if I have this correct, traditional IT systems security personnel and the industrial control systems, supervisory control and data acquisition systems security personnel. I am learning that distinction, but is that a fair distinction? I see everybody nodding their head yes.

The reason I bring that up is that he made the point that whereas we have the number of ICS security professionals is really limited, maybe 500 to 1,000 worldwide and we need tens of thousands. Would you all agree with that statement?

Mr. MANNING. Yes.

Senator CASSIDY. Now I guess that begs the question of what we are doing to address a shortage which is almost exponential.

Ms. Hoffman, I hate to put the—but you are the guy, you are the gal from the government, if you will. To what extent are we planning for that in attempting to address that critical shortfall?

Ms. HOFFMAN. So what we're trying to do is we're working with two universities to look at control system engineering. We have the University of Illinois and the University of Arkansas where we're trying to develop the next generation engineers that have both a cyber security background and a power engineering background.

But likewise not only are we trying to develop through the research program engineers in this area, but we are also trying to help the industry as their key need is to develop cyber mutual assistance capabilities so if an event occurs they're able to respond, the industry has the capacity to respond. And so that's also a critical need that needs to be addressed.

Senator CASSIDY. Now it seems though as if you are doing not that much on man power or woman power training. I say that because if you have two universities with an engineering program, even if they are big engineering programs, they are still relatively small. Again, if I am told we have 500 to 1,000 but we need tens of thousands, it seems, just if you are, I mean, does anyone else see a problem with manpower there, so to speak?

Mr. Highley.

Mr. HIGHLEY. Certainly the demand for technically-skilled folks, a lot of times we have to go out of the country to get those people. So it's just we don't produce enough in house to make it happen.

Senator CASSIDY. To what degree would you characterize the shortage? Severe or OMG. [Laughter.]

Mr. HIGHLEY. If severe is the less strident of those statements, I'll go with severe. I think it's something we want to watch. We don't believe it's insurmountable.

And again, the Cyber Mutual Assistance that Pat mentioned allows us to rely on our neighbors to help us in the event of some kind of disaster.

Senator CASSIDY. Gotcha.

Well, I will put a plug in for our Bossier City Cyber Innovation Center which I think is trying to meet this need.

Let me ask as well. I was speaking to someone recently about the attack at San Jose. I had read about that but I don't know the whole thing about that. But obviously in one sense very low tech.

They just shot out a cooling system for a transformer and almost brought it down.

At the time I read that this may have just been people hoping to rip off copper but then subsequently I was told that no, it was actually more sophisticated and folks had attempted to infiltrate a communications system and cut lines. They did not succeed. That is the only reason it was detected. Again, I see people nodding in agreement with this assessment. So it appeared a more coordinated thing. That is low tech.

I am also told that if you hit key, maybe as few as nine, sub centers in the nation you could bring everything crashing down. What are we doing to protect ourselves against the low tech, if you will, not the EMP, but the guy with the rifle?

Mr. HIGHLEY. The first protection is that redundancy in defense and depth so that we have lots of duplicate facilities. The grid is planned so that any critical facility can be out of the time of the greatest peak demand and yet the grid can change to deliver power.

That's why in the Metcalf incident that you mentioned, there was no loss of service to any customers, even though nine transformers were destroyed. So that the grid continued to deliver and that's our first base line is to design for that and cover that.

So beyond that the most critical facilities have been identified. They're not for public knowledge, but those critical facilities are being hardened from that kind of attack.

Senator CASSIDY. Gotcha.

I am out of time. I appreciate it.

Thank you.

Senator RISCH. Thank you.

Senator King.

Senator KING. One of the genesis, what is the plural of genesis, I wonder? Genoese, of this I knew my college Latin would come in handy.

Of this legislation was an important paper written by Andy Bachman and others, and the point they made was that the very complexity of the grid adds vulnerability. Could you elaborate on that, Mr. Stacey, that I think the term was the new layers are petri dishes for the growth of new attack surfaces and new interdependencies?

Mr. STACEY. I believe that as we ask the grid to do things it wasn't necessarily originally designed to do, integrating distributed resources and others, that takes computer technology, software and other intelligent devices to be able to manage that.

And when you do, there's an inherent side effect of complexity associated with that kind of automation to manage the efficiency and effectiveness and reliability of the grid. That complexity, or the addition of automation, does include some additional complexities and vulnerabilities.

Senator KING. So what we are talking about is, I think, there is a term I had never heard, attack surface interruption zone, and that is really what we are talking about is a place where an attack would be particularly devastating. It is not the whole grid. We are not talking about re-engineering the whole grid, but we are talking

about picking out these particular areas of vulnerability. Is that accurate?

Mr. STACEY. That's accurate.

These attack surface interruption zones are intended to impact the sequence that a cyber attacker goes through to have a well-planned and predictable event. And so these disruption zones are intended to cause the attacker to have physical access and not be able to access remotely.

Senator KING. And that is the key term is physical access.

The Ukraine hack was done remotely, and the problem is once they get through whatever the defenses are, if the whole system can be run from the computer, then we are sunk.

Mr. STACEY. That's correct.

One of the biggest lessons learned, I believe, from the Ukraine incident is being able to protect that remote access both from others having access and also so that we can, the asset owner, can have secure remote access.

Senator KING. Well as I understand the history of the Ukraine hack, one of the first things they did was change all the passwords so the operators couldn't get back into their own systems, and then they put malware in. I think it showed that they had a sense of humor because the last thing they did was turn out the lights in the control room. [Laughter.]

Well, I hope this legislation will be helpful to you in focusing on this particular aspect. This is not intended to be the be all and end all for cyber security. Clearly, that is a massive issue.

We are trying to focus on this one area that the Ukraine hack and the aftermath suggested, like the important one possibility is simply air gapping some of these data systems. But I understand there are vulnerabilities and limits to that. This is another option.

Mr. Manning, your thoughts?

Mr. MANNING. Well I could not help but think about your reference to air gap.

During my time at TVA our system was air gapped. But you're still vulnerable if there's physical access because you may not be vulnerable as much to the intrusion from outside cyber, but you're vulnerable from an inside actor who may give access to someone, to an even an air gap system, via some other means.

Senator KING. I was interested in your comments that we need to also be talking about security of operators.

Mr. MANNING. Exactly.

Senator KING. Internal people rather than——

Mr. MANNING. It's physical and cyber. And it strikes me that all of these things, we have to understand and balance all of these factors together because there are many threats and we have to manage and balance all of those.

The complexity of the grid is by design. We added that complexity intentionally because we were lacking in areas that required that complexity. So the grid is inherently more reliable now because of that complexity.

It is the technology that overlays it that has increased that reliability. So it's becoming more and more reliable, but the tradeoff is you have that greater threat factor out there associated.

Senator KING. You have more points of attack?

Mr. MANNING. Yes.

Senator KING. Not to depress us, but another whole area that we have not discussed is risks in the supply chain.

I have a nightmare of all the bolts in all the transmissions in all the vehicles dropping out on the same day given that we are not sure where everything is coming from. There may be vulnerabilities built into some of the physical gaps or whatever it is that we are using. I presume that is another, again, echoing the Senator from Louisiana. You all are nodding. The record doesn't show nodding. [Laughter.]

So if you could say yes that would be helpful.

Thank you all very much for being here today and for your good thinking on this very important issue, I appreciate it.

Senator RISCH. Thank you, Senator King.

Senator Gardner.

Senator GARDNER. Thank you, Mr. Chairman, and thank you to the witnesses. This is an incredibly important topic and something that is only going to grow as the latency of the Internet evolves around us and becomes more and more prevalent in everything we do, touch and work with.

Ms. Hoffman, I just want to start with you. In 2013 there was a hack by Iranians of a New York hydropower facility. When that occurred where do you fall? Where does Department of Energy fall into the notification of that hack? Were you the first to notify, the first to find out? How did that process work?

Ms. HOFFMAN. So with respect to the Dam Sector, the Dam Sector actually falls under the Department of Homeland Security. So they would notify the entity would coordinate with the local FBI as well as the Department of Homeland Security on the notification of that.

That would go through the National Cyber Integration and Communication Center. That information would then go out to all the sectors with respect to it and be provided to the electric sector information sharing organization which would provide it to the entities involved.

Senator GARDNER. Okay. So hydro power is not within the Electricity Delivery and Energy Reliability Office?

Ms. HOFFMAN. No.

Senator GARDNER. Okay.

Ms. HOFFMAN. It is not, sir.

Senator GARDNER. And then so, at which point though—it is important though that you know about this.

Ms. HOFFMAN. Yes.

Senator GARDNER. When are you notified about it and how does that notification occur?

Ms. HOFFMAN. So we get notified in a coordination call with the Department of Homeland Security. We also participate on the floor at the end kick. The Department of Energy is an active participant there as well as the industry sector.

And so that ends up being the coordination point in which notification comes out regardless of what sector would have an incident or a breach.

We would also have, as part of the government, a unified coordination group, a call across the Federal agencies, to make sure everybody is on the same page.

The one thing that's really important with your question. It's a valuable question because we want to make sure that we have accurate information and get information out to the industry as soon as possible so we may have a very early on call, early on with respect to the knowledge and details of the event to at least give some situational awareness but recognize that more information will be coming out over time.

Like other events or unlike other events, physical events, you can generally know that somebody shot a bullet at a transformer. But with cyber security, the details tend to have to—there has to be more investigation to get some of those details.

Senator GARDNER. Would an agency or a department like the Department of State Cyber Bureau, would they reach out and contact your agency or Department of Energy over a concern, perhaps, that North Korea may be pursuing some kind of an attack? How does that ever occur?

Ms. HOFFMAN. So with respect to any sort of outside influences or interests, usually that comes from the intelligence community into the Federal Government and then an assessment is performed from that point of view. And so, that would be the angle that we would get that information.

Senator GARDNER. One of the things I am trying to understand from the Department of Defense, to DHS, to Department of State, Department of Energy, is how the communication process works. I know you mentioned just one that, you know, a dam's hydropower go through one system and nuclear goes through another system and coal and nuclear go through the same or electricity generation through fossil fuels go through the same system, but not hydropower. That all goes to grid reliability. Is that the best way to do it?

Ms. HOFFMAN. So we do have the existing sector specific agencies where DHS is in charge of all the critical coordination across all the critical infrastructures. The Department of Energy is the sector specific agency for the energy sector which includes electricity, oil and gas and those are the sectors.

It's predefined how these sectors were developed under the National Infrastructure Protection Plan, but the important thing is that there is coordination and communication if there is something that is going on in the electric sector.

For example, DHS co-chairs the Electric Sector Coordinating Council meetings with the Department of Energy when we bring the CEOs in and have these strategy discussions. So there is very close coordination. And that is the only way, regardless of the structure, the only way we're going to advance information sharing communication and get ahead of the discussions.

Senator GARDNER. And if you were to have a cyber issue that you wanted to address Congress with when it comes to a cyber issue and electricity, who do you think the Committee responsible for that jurisdiction is?

Ms. HOFFMAN. I would actually reach out to multiple committees.

Senator GARDNER. Any guess of how many? [Laughter.]

Ms. HOFFMAN. No guess, sorry, but thank you for the question.

Senator GARDNER. It is part of our problem and one of the things I am very concerned about is what you just stated is you would reach out to multiple committees because there seems to be a lot of heads of cyber and no one responsible body, something I am very concerned about.

Thanks.

Senator RISCH. There's a lot of concern about that, Senator. We appreciate that.

Let's see, Senator Heinrich.

Senator HEINRICH. Thank you, Mr. Chairman.

Mr. Stacey, I want to go back to the partnership that INL and some of our other labs, Sandia and Pacific Northwest have, the work that has been done to look at this so far and ask you specifically with regard to these data systems what that work has generated in terms of generalized vulnerabilities and what you are concerned about there and then what are some of the standards or things we should be putting in place to mitigate those vulnerabilities?

Mr. STACEY. Let me take the second part of the question first.

I think a lot of the research and work that's been done, not only with the national laboratories, but also with industry and within the Department of Energy, has driven the NERC CIP standards which has really driven more awareness and more systematic discipline to overall protection of that process.

To answer the second question, I would share with you that hygiene is an important element but it's not the only element. And as we work at the advanced persistent threat and other elements of the high consequence, low frequency event, there's additional research. And that's where the national laboratories come into play and working on things that others can't, won't or shouldn't do. Can't because they don't have access to the large infrastructure that Chairman Risch mentioned. They can't because they don't have the subject matter experts. Or they shouldn't for a variety of other reasons. So, we're focused on that research.

And I would tell you that that research is having a significant impact. We can't talk a lot about that here, but associated with other elements of the government in DOD, that research has significantly helped the U.S.'s national security posture.

Senator HEINRICH. Okay.

Mr. Manning, you talked a little bit about EMPs as one of these high consequence but low frequency or low probability events. Where would you put insider threats in that continuum of risk?

Mr. MANNING. That's a difficult question, I think, to answer with a distinctive, specific answer. So I don't know how to address it other than to say that I think Mr. Highley requested some assistance in that regard regarding ensuring that our employees are straightforward with us when we hire them.

Senator HEINRICH. Right.

Mr. MANNING. I think we don't know how serious this issue is because we haven't experienced a real serious issue yet in that regard. So it's difficult to handicap it.

So I couldn't speak——

Senator HEINRICH. It is one of the reasons why I asked the question, actually, is because——

Mr. MANNING. Yes, but I can't tell you what is the answer.

Senator HEINRICH. As you pointed out, we have to divvy up our resources and our efforts in this based on what we believe the risk to be and there are some areas where it is very hard to define what that risk is.

So, we need to figure out, at least, what low resource things we can do to mitigate that risk, even if we don't know what the gross risk is.

Mr. Highley, do you want to add anything to that?

Mr. HIGHLEY. It is important that we have access to this Federal database, so right now when we run background checks on potential employees we can only access the state level database, so we can't get that information.

Senator HEINRICH. Are you referring to, like, the tide state or the terrorist screening database?

Mr. HIGHLEY. Correct.

Senator HEINRICH. Those——

Mr. HIGHLEY. That the FBI would have access to, so we would like to know before we put someone in our critical control center.

Senator HEINRICH. Yes.

Mr. HIGHLEY. If they have that kind of background.

Senator HEINRICH. That is very helpful actually.

Mr. HIGHLEY. Yes.

Senator HEINRICH. I want to ask on another, sort of, broad scale issue, and it can be Ms. Hoffman or any of you who want to jump in on this one.

One of the things we are seeing change dramatically from when I was a kid and my dad was a lineman at the utility and we had a centralized system and all the electronics load one way. We are seeing generation and things like storage which, kind of, act like a lubricant in the grid, migrate to the grid edge and to individual customers, storage generation all moving to places on the grid that they did not reside originally.

What does that mean for our resilience? How do we take advantage of that when we can? And are we thinking through that in addition to just trying to protect the overall architecture of the utility and the transmission pieces of that grid?

Ms. HOFFMAN. So I'll start real quick, and then I'll pass it to my colleagues.

Thank you for the question because it's important because we are looking forward to opportunities where we can isolate parts of the grid, looking at microgrids. We can look at graceful degradation. We can look at additional support capabilities to the grid via energy storage and distributed generation, but also local generation.

Regardless of the type of generation, I think, having a good proportional—proportion of generation in each of the regions of the country is very valuable.

And so, from that perspective, those technologies can be quite advantageous. But like anything else, those technologies must be protected themselves with respect to cyber security measures, control systems, even from the generation point of view.

Mr. MANNING. Yeah, I would say the same thing.

Secure technology enabled is the answer to your question. Secure technology enables us to take advantage of that and turn it from a challenge to a resiliency plus.

Senator HEINRICH. Great. Thank you.

Senator RISCH. Thank you, Senator.

Senator Hirono, you would be next but we usually go back and forth. Do you object to Senator Capito?

Senator CAPITO. Thank you, Mr. Chairman, and thank all of you who are here.

Mr. Stacey, I would like to ask the crux of this bill deals with the research done by the National Energy Technology Labs. As you know, there are many across the country, one in our State of West Virginia in Morgantown. I am curious to know you are already pursuing this in the Idaho lab.

What other kind of interplay do you have now with the other national laboratories? Are they all involved? Is it just centered around certain of those laboratories? And what would you envision through this bill in terms of research capacity at these different facilities?

Mr. STACEY. So all of the national labs are working in one way or another on cyber security issues. The labs that I pointed out earlier, Pacific Northwest National Laboratory and Sandia National Laboratory, as well as Idaho National Laboratory, we believe, have unique capabilities and skills to bring to the industrial control system challenge that we're facing.

But in fact, we shouldn't be restricted. We should have access to any of the national laboratories or resources we need to address this challenge, this complex challenge that the nation——

Senator CAPITO. Do you have that now with the other laboratories, that kind of collaborative approach?

Mr. STACEY. You know, I believe we do.

Senator CAPITO. You do.

Mr. STACEY. The national laboratories, early on, were more and more competitive. As we get challenges and the budgets are reduced you're seeing a renewed interest across all the laboratories, more cooperation and collaboration and frankly, the national challenge mandates that we take advantage of that.

So I'm pretty optimistic about the approach and the teaming that we have right now across the national laboratory system.

Senator CAPITO. Well, good. Thank you.

Ms. Hoffman, well actually this is for Mr. Highley. My question is she did a good recitation as to what would happen and who she would, what other government agencies and committees would be involved if a breach were to occur and how quickly could be acted in a coordinated capacity. In your sector, as the electricity provider, do you feel that you are in the loop enough or as quick enough as you would want to be? Is that something that you are working on? What is that collaborative relationship like?

Mr. HIGHLEY. So under the Electric Subsector Coordinating Council there's something called the Information Sharing and Analysis Center (ISAC), and that's where we would go.

So we are a hydropower operator. We operate hydropower plants on the Arkansas River. And frankly if we had a cyber incident occur there we would immediately notify the ISAC. And then they

disseminate that to the other utilities across the country, so that we know about that threat.

Senator CAPITO. And they then disseminate to the Department of Energy and Homeland Security or is that how that works?

Mr. HIGHLEY. And coordinates with NCCIC and the other counterparts.

Senator CAPITO. And all that, okay.

In the description of the bill I thought, well let me find the description of the bill that I found interesting. "Establishes a two-year pilot program with the national labs to examine ways to replace automated systems with manual procedures controlled by human operators to remove vulnerabilities that allow cyber criminals to access the grid through holes in digital software systems."

I am thinking to myself, I think today I might have seen a driverless car. I am thinking at the end of the day you can't replace the eyes on, hands on, mental acuity of a person actually driving a car which I immediately got on the sidewalk on, or in terms of this.

So it is interesting to me just looking at it as we evolve with all this technology where we, kind of, come back to in the end, particularly in the terms of security.

So I imagine that with that comes a lot of technological expertise, maybe some forensic ability to be able to pick this up. Are there any institutions in the country that are particularly looking at this as a job path, job creation? And if they are, maybe you could highlight a few of those for us, if anybody knows?

Mr. HIGHLEY. I just would echo the comments of Pat about the University of Arkansas and that partnership. I'm very familiar with that one to develop that capability.

Senator CAPITO. Anybody else, Ms. Hoffman, that you know that is working in this direction?

Ms. HOFFMAN. Beyond the two universities I mentioned, University of Illinois has a strong partnership with power system engineers. I think what we're trying to do is really go after what capabilities do we need to enable in industry?

Senator CAPITO. Right.

Ms. HOFFMAN. And build in the educational institution as well as the emergency responders so that we actually can have an effective restoration process, but get the right information out in a timely manner.

Senator CAPITO. Right. It would have to come from a whole spectrum of educational aspects to be able to really hit that.

Thank you all very much.

Senator RISCH. Thank you, Senator Capito.

The vote has been called and Senator Hirono, you can wrap it up for us.

Senator HIRONO. I will be quick.

Ms. Hoffman, the covered entities as defined in S. 3018 comes from Executive Order 13636 which requires the Department of Homeland Security Secretary to consult with sector specific agencies which includes DOE in identifying critical infrastructure, "where a cyber security incident could reasonably result in catastrophic regional or national effects on public health or safety, eco-

nomic security or national security." The list of entities is then updated annually.

Are you confident in the process that the DOE uses to identify critical infrastructure under this Executive Order? And can you describe how the DOE engages with DHS in this annual process? And I might add that the list of critical infrastructure through this process is classified, isn't it?

Ms. HOFFMAN. The list, I think, as a complete set is classified. Individuals, there can be conversations with individuals on that list.

But first of all, thank you for the question.

Identification, prioritization of critical entities and critical infrastructure gets to the crux of what we need to do in making sure that we're focusing on the right points on the system to advance technology but advance cyber security measures.

With respect to the evaluation, we did a very transparent collaborative process with industry and the Federal Government looking at the criteria which was significant economic impact as well as potential impact to health and safety, were some of the criteria that was looked at in that evaluation. So with respect to the electric sector it was companies that would have a high economic impact in the United States and as well as associated critical infrastructures with those companies.

Senator HIRONO. So when you apply that kind of criteria there would be states, possibly such as Alaska or Hawaii, where we may not have what may be termed a national impact and therefore, how can we be assured that the proper analysis is done with regard to our grid to identify very specific, specifically, where the areas of vulnerability are either to physical attack or cyber-attack? Can we get help to—in this kind of analysis of our grid?

Ms. HOFFMAN. Absolutely, Senator. I would love to sit down and talk to you and understand more the critical assets and the things that you're concerned about. And we can make sure that we incorporate that in our discussions and our activities moving forward.

Senator HIRONO. That is always a concern of mine whenever we have national legislation that kicks off with some kind of a program or assistance and then there is a criteria that you have to show a national impact. Obviously for noncontiguous states that is a little hard to show, and I think it really disadvantages Alaska and Hawaii. I just wanted to make that point, Mr. Chairman.

Mr. Manning, the Department of Defense's recent Smart Power Infrastructure Demonstration for Energy Reliability and Security, better known as SPIDERS program, included projects to boost energy security at Joint Base Pearl Harbor Hickam and Camp Smith in Hawaii. I have worked to promote energy resiliency at military installations in the DOD Energy Security Act which I had introduced along with Senator Wyden.

Clearly this is a rhetorical question that if it is a good thing that if our installations could get off the grid so that they can be pretty much self-sufficient. My question is could you talk a little bit about how a functioning military installation could help recovery of the larger grid if something happens to the larger grid?

Mr. MANNING. So I think it's not just specific to military installations but to a trend of microgrids in general. And the ability of a

microgrid to integrate in and out of the existing grid, I think, is a function of technology in the ability to synchronize those grids together and to operate them either independently or dependently and to be free to move in and out of that continuum.

I think with a number of the military bases we were very focused on the ability to operate either separately isolated or operate in conjunction with the grid. And ultimately I think that provides you the best scenario going forward because you may always decide I want to operate in this mode or the other or you may change depending on current conditions.

Senator HIRONO. Well that makes a lot of sense. So as more and more, for example, military installations become energy self-sufficient that that thought that the synchronization is as something that gets built into the design of the——

Mr. MANNING. Absolutely. And it's another example of where technology is enabling greater resiliency and greater poise going forward.

Senator HIRONO. Thank you, Mr. Chairman.

Senator RISCH. Thank you.

Those interesting sounds you have heard indicate that we have got to get down to vote. So I never have figured out exactly how that works, but I know you have got to run to the floor when you hear the sound. So that is where we are.

With that, I am going to conclude the hearing.

I am going to leave the record open. Senator King and I, as sponsors of this bill, and for that matter, everyone on the Committee, sincerely appreciate all of you coming today to give us your input. But we want to get this right. Obviously it is not an area that is particularly controversial, but it is highly technical and it is important that we do get it right.

If we have overlooked something, if there is something that you want to get your two cents worth in on this, I would really urge you to do that. I am going to keep the record open until this week, Friday at five o'clock, so you can get anything in that you want to.

Senator RISCH. Senator King, anything else for the good of the order?

Senator KING. No, I think I was just going to tell Mr. Stacey if we get this bill through I will personally deliver a sextant to the Office of the Idaho National Lab. [Laughter.]

Senator RISCH. Senator King, you have been threatening to come the INL and have not made it yet.

Senator KING. This is going to be the occasion.

Senator RISCH. We are going to get you there someday.

Anyway, thank you so much, all of you. We will end the hearing, declare the hearing closed.

[Whereupon, at 3:42 p.m. the hearing was adjourned.]

APPENDIX MATERIAL SUBMITTED

II

114TH CONGRESS
2D SESSION

S. 3018

To provide for the establishment of a pilot program to identify security vulnerabilities of certain entities in the energy sector.

IN THE SENATE OF THE UNITED STATES

JUNE 6, 2016

Mr. KING (for himself, Mr. RISCH, Ms. COLLINS, and Mr. HEINRICH) introduced the following bill; which was read twice and referred to the Committee on Energy and Natural Resources

---

A BILL

To provide for the establishment of a pilot program to identify security vulnerabilities of certain entities in the energy sector.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Securing Energy Infrastructure Act".

SEC. 2. DEFINITIONS.

In this Act:

(1) COVERED ENTITY.—The term "covered entity" means an entity identified pursuant to section

9(a) of Executive Order 13636 of February 12, 2013 (78 Fed. Reg. 11742), relating to identification of critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

(2) EXPLOIT.—The term "exploit" means a software tool designed to take advantage of a security vulnerability.

(3) INDUSTRIAL CONTROL SYSTEM.—

(A) IN GENERAL.—The term "industrial control system" means an operational technology used to measure, control, or manage industrial functions.

(B) INCLUSIONS.—The term "industrial control system" includes supervisory control and data acquisition systems, distributed control systems, and programmable logic or embedded controllers.

(4) NATIONAL LABORATORY.—The term "National Laboratory" has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(5) PROGRAM.—The term "Program" means the pilot program established under section 3.

(6) SECRETARY.—The term "Secretary" means the Secretary of Energy.

(7) SECURITY VULNERABILITY.—The term "security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

SEC. 3. PILOT PROGRAM FOR SECURING ENERGY INFRASTRUCTURE.

Not later than 60 days after the date of enactment of this Act, the Secretary shall establish a 2-year control systems implementation pilot program within the National Laboratories for the purposes of—

(1) studying the covered entities in the energy sector that voluntarily participate in the Program to identify new classes of security vulnerabilities of the covered entities; and

(2) researching, developing, testing, and implementing technology platforms and standards to isolate and defend industrial control systems of covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities, including—

(A) analog and nondigital control systems;

(B) purpose-built control systems; and

(C) physical controls.

SEC. 4. WORKING GROUP.

(a) ESTABLISHMENT.—The Secretary shall establish a working group—

(1) to evaluate the technology platforms and standards used in the Program under section 3(2); and

(2) to develop a national cyber-informed engineering strategy to isolate and defend covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities.

(b) MEMBERSHIP.—The working group established under subsection (a) shall be composed of not fewer than 10 members, to be appointed by the Secretary, at least 1 member of which shall represent each of the following:

(1) The Department of Energy.

(2) The energy industry, including electric utilities and manufacturers recommended by the Energy Sector coordinating councils.

(3)(A) The Department of Homeland Security; or

(B) the Industrial Control Systems Cyber Emergency Response Team.

(4) The North American Electric Reliability Corporation.

(5) The Nuclear Regulatory Commission.

(6)(A) The Office of the Director of National Intelligence; or

(B) the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

(7)(A) The Department of Defense; or

(B) the Assistant Secretary of Defense for Homeland Security and America's Security Affairs.

(8) A State or regional energy agency.

(9) A national research body or academic institution.

(10) The National Laboratories.

SEC. 5. REPORT.

Not later than 2 years after the date on which funds are first disbursed under the Program, the Secretary shall submit to the appropriate committees of Congress a final report that—

(1) describes the results of the Program;

(2) includes an analysis of the feasibility of each method studied under the Program; and

(3) describes the results of the evaluations conducted by the working group established under section 4(a).

SEC. 6. NO NEW REGULATORY AUTHORITY.

Nothing in this Act authorizes the Secretary or the head of any other Federal agency to issue new regulations.

SEC. 7. EXEMPTION FROM DISCLOSURE.

Information shared by or with the Federal Government or a State, tribal, or local government under this Act shall be—

(1) deemed to be voluntarily shared information; and

(2) exempt from disclosure under any provision of Federal, State, tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring the disclosure of information or records.

SEC. 8. PROTECTION FROM LIABILITY.

(a) IN GENERAL.—A cause of action against a covered entity for engaging in the voluntary activities authorized under section 3—

(1) shall not lie or be maintained in any court; and

(2) shall be promptly dismissed by the applicable court.

(b) VOLUNTARY ACTIVITIES.—Nothing in this Act subjects any covered entity to liability for not engaging in the voluntary activities authorized under section 3.

SEC. 9. AUTHORIZATION OF APPROPRIATIONS.

(a) PILOT PROGRAM.—There is authorized to be appropriated $10,000,000 to carry out section 3.

(b) WORKING GROUP AND REPORT.—There is authorized to be appropriated $1,500,000 to carry out sections 4 and 5.

(c) AVAILABILITY.—Amounts made available under subsections (a) and (b) shall remain available until expended.

○

Department of Energy
Washington, DC 20585

October 11, 2016

The Honorable James E. Risch
Chairman
Subcommittee on Energy
Committee on Energy and Natural Resources
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

On July 12, 2016, Patricia Hoffman, Assistant Secretary, Office of Electricity Delivery and Energy Reliability, testified regarding, S. 3018, the Security Energy Infrastructure Act, and to examine protections designed to guard against energy disruptions. To complete the hearing record, please find enclosed answers to the questions submitted by Ranking Member Joe Manchin, III, Senators Steve Daines, Elizabeth Warren, and you regarding this hearing.

If you need any additional information or further assistance, please contact me or Lillian Owen, Office of Congressional and Intergovernmental Affairs at (202) 586-5450.

Sincerely,

Jed D'Ercole
Deputy Assistant Secretary for Senate Affairs
Congressional and Intergovernmental Affairs

Enclosures

cc: The Honorable Joe Manchin, III
Ranking Member

QUESTION FROM CHAIRMAN JAMES E. RISCH

Q1. In the context of providing technical assistance, can you please provide specific suggestions for S. 3018?

A1. Thank you for the opportunity to provide technical assistance on S. 3018. It appears that the intent of S. 3018 is to strengthen the cybersecurity posture by allowing DOE national laboratories to identify, study, and defend energy infrastructure systems critical to national security. Note that the covered entities referred to in S. 3018, which are identified pursuant to section 9(a) of Executive Order 13636 (Improving Critical Infrastructure Cybersecurity), are confidentially notified about their status. A so-called "section 9" entity may opt to reveal its section 9 status to relevant industry groups or publicly. Participation in the S. 3018 pilot program may compel these entities to reveal their section 9 status to other program participants.

Many of these energy sector entities already conduct such assessments to comply with mandatory Critical Infrastructure Protection standards set by the North American Electric Reliability Corporation or as part of their due diligence in ensuring that their systems are reliable and capable of providing uninterrupted service in the face of today's evolving cyber threat landscape. We strongly recommend that the working group proposed in S. 3018 coordinate with the Electricity Subsector Coordinating Council (ESCC), which serves as the principal liaison between leadership in the Federal government and in the electric power sector, with the mission of coordinating efforts to prepare for and respond to national-level incidents or threats to critical infrastructure. Protecting the electric grid from threats that could impact national security and public safety is a responsibility shared by both the Government and the electric power sector. The ESCC is the vehicle for the industry and Government to have top-level policy and public affairs discussions and engagement on matters of national security to enhance the reliability and resilience of the electric grid. These activities include all hazards, steady-state preparation, and emergency preparedness, response, and recovery for the Nation's electricity sector.

QUESTION FROM SENATOR STEVE DAINES

Q1. Under the recently enacted FAST Act the Department of Energy became the Sector Specific Agency for all electrical infrastructure. This puts a large amount of responsibility on the DOE's shoulders. Keeping the grid up and functional should be one of your top priorities. From a National Security standpoint, cyber attacks are a real and serious threat and, as we have seen recently, they are being waged successfully on government agencies, the most well-known being the OPM breach in 2015. Luckily the grid is primarily owned by private entities that take a more serious look at cyber security threats. Can you confirm whether the DOE has ever been successfully breached, whether or not any of our major grid systems have ever been successfully breached, and if S. 3018 is enacted, how you will work with and learn from the private sector to make sure neither the DOE nor our grid system is breached by cyber attacks?

A1. The energy grid is a critical asset for the Nation and, therefore, is a significant target of interest to our adversaries. Cybersecurity remains a major area of focus for the Federal, public, and private partners that make up the U.S. energy grid. This also means that all involved parties, including the Department of Energy (DOE), remain targets as well. DOE takes cybersecurity threats very seriously, both within the energy grid and across the Department's mission areas. Under Department oversight, significant solutions have been developed and deployed to address cyber threats. The solutions include unique sensors for grid assets, improved information sharing with Federal and non-Federal partners, and improved safeguards within the Department.

Grid security is one of the highest priorities for the U.S. Government. DOE and the Department of Homeland Security (DHS) work closely with other Federal agencies, state/local/tribal governments, and our partners in the energy industry to manage cyber risk. As the Sector Specific Agency for the energy sector, DOE collaborates and coordinates with DHS, industry, and other partners to address energy sector cyber incidents. Through joint collaboration and coordination, DOE and DHS routinely and regularly share information with U.S. critical infrastructure companies, including utility owners and operators, to ensure that they have the information they need to protect their systems from malicious cyber activity.

The private sector owns and operates the majority of U.S. critical infrastructure. DOE and DHS have worked to build a strong partnership with owners and operators, recognizing that

secure infrastructure is vital to homeland security, community resilience, and our economy. Through information sharing, assessments of critical assets, and joint planning and exercises, DOE and DHS work with the electric sub-sector to address risks associated with malicious cyber activity, physical attacks, and other hazards.

Despite our best efforts, the complexity and frequency of attacks against the Department and the energy grid continues to escalate. DOE has experienced cyber events over the past three years resulting in adversary intrusion, data exfiltration, and website defacement. The most significant event occurred in the summer of 2013, when an intruder successfully exploited a vulnerability, resulting in the exfiltration of Personally Identifiable Information from a DOE-managed database. Also in 2013, a system administrator inadvertently introduced a malicious rootkit based on Hikit, malware combining capability with sophisticated persistence mechanisms.

In both instances, the Department worked closely with Federal partners, national laboratories, and the private sector to identify weaknesses, eliminate threats, and reconstitute the cyber environment.

In collaboration with Novetta and Microsoft, the Department's contributions helped eliminate Hikit deployments worldwide through a coalition of security vendors, security researchers, and major technology companies. The partnerships and collaboration forged from these experiences have strengthened the Department's capabilities to detect and respond to cyber threats. The Department's program offices, national laboratories, plants, power marketing administrations, and field offices utilize the latest technologies and industry best practices to protect the Department and energy grid.

QUESTIONS FROM RANKING MEMBER JOE MANCHIN, III

Q1. Assistant Secretary Hoffman, under your leadership, the Department of Energy released the "2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity". Developed as an update to the 2006 Roadmap to Secure Control Systems in the Energy Sector, the report outlines a strategic framework over the next decade among industry, vendors, academia and government stakeholders to design, install, operate, and maintain a resilient energy delivery system capable of surviving a cyber incident while sustaining critical functions.

Does your department plan on updating the roadmap and, if so, how will you address the fact that the "graying" of the electric sector workforce will lead to a larger need for specialized workers with an understanding of threats, vulnerabilities and solutions?

A1. The "2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity" established a vision that "resilient energy delivery control systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions," and set forth a five-part strategy and set of milestones to achieve this vision. To evaluate the progress that has been made in achieving the milestones over the last 5 years, the Department of Energy (DOE) is engaging ten national laboratories in a coordinated outreach activity to energy sector stakeholders to review and update the availability of tools, technologies, and guidance documents related to each Roadmap milestone. This coordinated outreach activity among the national laboratories will support highlighting energy delivery system cybersecurity progress, revealing areas that could benefit from increased emphasis, and informing various cybersecurity activities across the energy sector.

DOE has recognized that the electricity industry needs workforce development resources. Our Secure Power Systems Professionals effort has provided the industry with valuable products including recruitment and career development guides, job profile tables, individual and team guidelines, and behavioral interview guidelines.

DOE, in partnership with the Department of Homeland Security and the energy sector, supports university cybersecurity collaborations that engage 16 universities with the primary focus on research and development. Both undergraduate and graduate students participate in research to develop innovative cybersecurity technologies that will transition to the energy sector to reduce the risk of energy disruption resulting from a cyber incident. These academic collaboration projects engage extensively with the energy sector, providing

training opportunities that integrate the computer science of cybersecurity with power system engineering, and bringing together universities, energy asset owners and operators, and suppliers.

DOE will also consider actions from the joint U.S.-Canadian strategy and action plan for strengthening the security and resilience of the North American electricity grid, which includes addressing the growing threat from cyber-attacks, as a strategic component to future efforts.

Q2. Sixty percent of all the electricity consumed in the United States flow through high voltage electric transformers that enable power to be transported long distances. The simultaneous loss of a small number of these transformers could produce widespread long-term blackouts.

I understand that it is costly and difficult for utilities to keep spare high voltage transformers on hand. There are, however, several utility-run programs for the sharing of spare transformers. The Department's Quadrennial Energy Review recommended the development of one or more strategic transformer reserves.

Assistant Secretary Hoffman, last year's Fixing America's Surface Transportation (FAST) Act included a provision requiring the Department Energy to examine the feasibility of establishing transformer reserves.

When will the Department complete its determination whether strategic transformer reserves are feasible and have you made any preliminary determinations that you can share with us today?

A2. In January, we awarded this analysis project to a team led by the Oak Ridge National Laboratory. The project team includes researchers from the University of Tennessee-Knoxville, Sandia National Laboratories, Electric Power Research Institute, and Dominion Virginia Power. The strategic transformer reserve technical assessment is expected to be completed this fall. The Office of Electricity Delivery and Energy Reliability and the Office of Energy Policy and Systems Analysis will review the assessment and make recommendations to the Secretary for the report due to Congress.

QUESTIONS FROM SENATOR ELIZABETH WARREN

Q1. The Securing Energy Infrastructure Act focuses on researching, developing, and implementing technologies to protect critical infrastructure from cybersecurity threats by the means of analog and non-digital controls, purpose built controls, and physical controls. This Act is studying the potential to achieve increased security from cyber threats through reversion to older analog technology because of the inherent risks of newer digital and software based systems. However, to effectively study the security of energy grid and develop new cyber security technologies, the system should be studied completely and holistically.

Is the Department of Energy conducting any additional studies that focus on cybersecurity measures that address the digital components of the energy grid?

A1. The Office of Electricity Delivery and Energy Reliability is working with the private sector to develop advanced digital technologies to better secure the grid against cyber events. The Department of Energy (DOE) maintains a research and development portfolio that engages at least 30 asset owners and operators, 30 suppliers, 22 universities, and 10 national laboratories in research and development (R&D) of tools and technologies that strengthen the cybersecurity of energy grid digital components, working in partnership toward resilient energy delivery systems that can survive a cyber incident while sustaining critical functions.

Through this program, over 30 tools and technologies have been developed and transitioned to practice in the energy sector through R&D partnerships with the private sector, national laboratories, and academia. Many of these advanced technologies are being deployed in the energy delivery systems today to enhance security. For example, Schweitzer Engineering Laboratories partnered with the Tennessee Valley Authority and Sandia National Laboratories to develop a technology called Padlock—a security gateway that helps to prevent unexpected cyber-activity and to detect cyber and physical tampering on energy infrastructure field devices often found on pole tops and in cabinets throughout distribution systems. Also, Applied Communication Sciences partnered with DTE Energy, the Electric Power Research Institute, and the University of Illinois at Urbana–Champaign (UIUC) to develop intrusion detection technologies for mesh networks often used for distribution automation and advanced metering infrastructure. More recently, Schweitzer Engineering Laboratories partnered with Ameren and Sandia National Laboratories to develop the first field-hardened software-defined networking flow controller. The device provides enhanced

security and flexibility for substations and also helps reduce operational and maintenance costs.

Another example is an industry-led research partnership that helps energy infrastructure protection and control equipment to check received commands, ensuring these commands support stable grid operations, and blocking malicious commands intended to jeopardize grid stability. ABB leads this effort, partnering with Ameren, Bonneville Power Authority, and UIUC.

One final example is a national laboratory-led research partnership that is designing cybersecurity awareness features for energy management system applications, allowing these applications to recognize and reject a cyber-attack. Argonne National Laboratory leads this effort, partnering with Illinois Institute of Technology, Iowa State University, OPAL-RT Technologies, Pacific Northwest National Laboratory, and RTDS Technologies.

Q2. To what extent has encryption played a role in the cybersecurity of the critical infrastructure of the energy grid? Has the role of encryption in the cybersecurity of the energy grid been studied?

A2. Encryption plays an important role in the cybersecurity of the critical infrastructure of the energy grid for the protection and secure handling of information. Recognizing this importance, the purpose of the North American Electric Reliability Corporation Critical Infrastructure Protection Version 5, 011-2 enforceable reliability standard is "[t]o prevent unauthorized access to Bulk Electric System (BES) Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES."[a]

Various studies have examined the role of encryption in the cybersecurity of the energy grid. For example, the National Institute of Standards and Technology Interagency Report on Guidelines for Smart Grid Cybersecurity in Chapter 4, Cryptography and Key Management, identifies technical cryptographic and key management issues across the scope of systems and devices found in the smart grid along with potential alternatives.[b]

[a] http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-011-2&title=Cyber%20Security%20-%20Information%20Protection&jurisdiction=United%20States (last visited August 15, 2016)
[b] http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

Ongoing research in the cybersecurity for energy delivery systems community continues to advance technologies that will further enhance the effective use of encryption throughout critical energy infrastructure. The Trustworthy Cyber Infrastructure for the Power Grid university collaboration, supported by DOE in partnership with the Department of Homeland Security, performed research in this area, including developing innovative cybersecurity protections for legacy power system devices that predate today's interconnected systems and may have limited ability to support cybersecurity measures.[a]

[a] http://www.tcipg.org.

U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing: July 12, 2016
S. 3018, the Securing Energy Infrastructure Act, and
Protections Designed to Guard Against Energy Disruptions
Question for the Record Submitted to Mr. Duane Highley

Question from Senator Steve Daines

Question: In your testimony you mention how important it is to avoid a one-size-fits-all strategy to address our cyber-security needs. With a grid that is almost completely privately owned, and with each region and each company employing different infrastructure models and equipment to suit the specific area, how can we make sure that the pilot program proposed in S. 3018 doesn't fall into the DC directed one-size-fits all standard?

Highley Response: The best way to avoid the "one-size-fits-all" solution is to ensure that the pilot program carefully considers the differences that will exist among those entities that are eligible to participate. These differences will include not-for-profit and for-profit utilities, size differences as it relates to number of customers, amount of generation, miles of transmission, geography and climate. We can further avoid one size fits all by allowing for flexibility in implementation and utilizing an industry-driven model like the NERC standards-setting process which allows for subject matter experts to weigh in on proposals to insure that they can be implemented. If the pilot program is developed with these processes and differences in mind, the program will have a higher likelihood of providing benefits for government and industry.

U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing: July 12, 2016
S. 3018, the Securing Energy Infrastructure Act,
Protections Designed to Guard Against Energy Disruptions
Questions for the Record Submitted to Mr. Brent Stacey

Questions from Senator James E. Risch

Question 1: While working on the *Securing Energy Infrastructure Act*, some people mentioned that this legislation is duplicative of previous research efforts. Could you elaborate about how this work is unique and separate from previous efforts?

S. 3018 creates a pathway for the government to better serve in its leadership role by establishing the unique research programs and decision forums for government, national labs and industry to solve the cybersecurity challenges of highest consequence to the reliability and resilience of the grid. The majority of current cybersecurity research programs focus on information technology (IT) infrastructure, databases, and communications networks. Currently, there is limited research focused on the digital operational technologies (OT) within the engineered systems that are associated with the advanced, functional cyber-physical processes of complex infrastructures, including the electric grid. In addition to the emphasis on critical OT systems, this legislation promotes a holistic approach across physics, cyber, grid engineering, digital technology, alternative technologies, and operational response. The current model of addressing cyberattacks is simply not sustainable as the sophistication of our adversaries grows, the implementation of advanced digital technology accelerates, and our country's dependency on electricity increases. Protection of energy infrastructure from the most damaging, highest consequence events demands a fundamentally new research approach, an approach that must begin with different primary assumptions. At a high level these assumptions include:

- ✓ Cybersecurity research today focuses on tools and technologies to prevent adversaries from gaining access to our infrastructure. The new research assumption must be that adversaries are already in our systems.
- ✓ Cybersecurity research today attempts to rely on new or enhanced digital technologies as the source of solutions to cyber threats by providing barriers, detection and response. New research must address the fact that the majority of the long-term security and resilience solutions for OT must be based on cyber-informed innovations in engineering designs, processes, and operations – not solely dependent on defensive digital IT technologies.
- ✓ Cybersecurity solutions are reactively 'patched into' our infrastructure to provide intermediate relief from an unsustainable countermeasure treadmill. New research must assume that our approach to the overall security posture of the grid and our

U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing: July 12, 2016
S. 3018, the Securing Energy Infrastructure Act,
Protections Designed to Guard Against Energy Disruptions
Questions for the Record Submitted to Mr. Brent Stacey

ability to implement the grid-of-the-future is dependent upon 'stepping off' the treadmill by 'designing in versus bolting on' cybersecurity solutions.

With these assumptions as a basis, Idaho National Laboratory (INL) has developed and advocates a new direction for research that comprehensively addresses these assumptions, embraces the benefits of technology innovations, and develops a sustainable approach to protect the nation's energy infrastructure from the highest consequence cyberattacks. This different approach, consistent with the objectives of S. 3018, is based on the principle that identifying and engineering barriers to high consequence events will guide the best use of technology, instead of technology guiding which consequences can be responded to and mitigated. The science and engineering methodologies of this approach are:

- ✓ Define the Problem: Collaborate with knowledgeable stakeholders to identify the few most severe consequences we must defend the grid against to assure our economic and national security – rather than conventionally identifying technologies that mitigate our current cyber risks.
- ✓ Multi-disciplined Solution Teams: Integrate multidiscipline engineering teams of cyber, process, safety systems, and operations talent with deep knowledge of the engineering and operations of the grid, including the basic engineering design, equipment functionality, and controls for remote access – rather than constraining the pool of solutions options to the limited availability of cyber staff.
- ✓ Map the Cyber Kill Chain (the steps necessary for an attacker to have a predictable consequence): Determine each system's connection to attacker availability and capability, or lack of, to the highest consequence events – rather than developing individual technology solutions to detect and mitigate vulnerabilities as they are identified.
- ✓ Implement Robust and Resilient Designs: Prevent or disrupt high consequence events through engineering sustainable interruption barriers into the kill chain through a forward-leaning, integrated research plan for technologies or intuitively secure processes that optimize a long-term engineered infrastructure design – rather than cycling in digital 'assembly line' and 'best-of-breed' technologies to detect and block today's attacks.

U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing: July 12, 2016
S. 3018, the Securing Energy Infrastructure Act,
Protections Designed to Guard Against Energy Disruptions
Questions for the Record Submitted to Mr. Brent Stacey

Question 2: How is the Idaho National Lab collaborating with other National Laboratories, industry partners, and the Department of Energy to protect our grid against disruptions?

INL is a major center for national security technology development, demonstration and deployment. Our mission focuses our research and development programs on innovative, high impact products and solutions for the sustainable protection of our critical infrastructure, with an emphasis on the power grid and other lifeline infrastructure sectors. DOE routinely measures our success in fostering academic, industry, government, and international collaborations to assure that INL's mission is fulfilled in close alignment with the DOE strategic objectives for energy and national security. In the original written testimony, INL highlighted an emerging partnership with Pacific Northwest National Laboratory and Sandia National Laboratories to holistically address the control system cybersecurity of the energy grid, critical infrastructure lifeline sectors, and military systems. Additional examples of collaborations that are enabling the protection of the national electric grid include, but are not limited to:

- ✓ DOE Grid Modernization Laboratory Consortium (GMLC): INL is participating in multiple GMLC project areas, including serving as the project lead in research to address threat detection with an emphasis on cyber analytics and solutions for discerning between physical and cyber events. This project includes INL, Brookhaven National Laboratory, Lawrence Berkeley National Laboratory, Lawrence Livermore National Laboratory, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, and Sandia National Laboratories. Within another proposed GMLC project, INL will collaborate with the University of Louisiana at Lafayette to assess and mitigate potential cyber vulnerabilities and consequences to the grid as a result of connections with electric vehicles and charging stations. INL is also teamed with Brookhaven National Laboratory and other labs to support the inclusion of resilience, cyber and physical security into the New York State Public Service Commission's initiative to reform New York State's energy industry and regulatory practices for grid and market modernization - Reforming the Energy Vision (REV).
- ✓ DOE Cybersecurity Risk Information Sharing Program (CRISP) OT: INL is leading a collaborative effort to enhance the original beyond program, which is constructing an information sharing network of security sensors at participating utilities. INL's role is to extend the monitoring capabilities beyond IT systems to the key industrial control systems within public utilities' operational networks. A collaboration with

U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing: July 12, 2016
S. 3018, the Securing Energy Infrastructure Act,
Protections Designed to Guard Against Energy Disruptions
Questions for the Record Submitted to Mr. Brent Stacey

Argonne National Laboratory, Oak Ridge National Laboratory, and Pacific Northwest National Laboratory, this effort is in support of DOE Office of Electricity Delivery and Energy Reliability (DOE-OE) and the Electricity Information Sharing and Analysis Center (E-ISAC).

- ✓ Ukrainian Cyber Event Assessments and Lessons Learned Training: INL subject matter experts supported DOE, Department of State, Department of Homeland Security (DHS), and the Federal Bureau of Investigation in providing U.S. support to Ukraine in response to the major cyberattack on the Ukrainian power grid. INL participated in two on-site assessments; provided information, analysis results, and review for the SANS report "Analysis of the Cyber Attack on the Ukrainian Power Grid.;" In addition, we provided technical experts supporting a series of unclassified information sharing briefings by DHS in eight major U.S. cities and four webinars. These briefings and webinars reached nearly 1500 government, industry, and research stakeholders.
- ✓ Electromagnetic Pulse/Geomagnetic Disturbance Grid Research: INL, Oak Ridge National Laboratory, and Sandia National Laboratories are supporting DOE-OE Infrastructure Security and Energy Restoration Division with the development of an action plan to conduct research and real-world grid-scale testing to better understand and mitigate effects from electromagnetic pulse and geomagnetic disturbance.
- ✓ INL-Utility Cooperative Research: INL is meeting the objectives of the California Energy Systems for the 21st Century (CES-21) via collaborative research projects with Southern California Edison, Pacific Gas & Electric, San Diego Gas & Electric, Lawrence Livermore National Laboratory, and New Context. These collaborative efforts include, but are not limited to developing cyber-attack scenarios for a representative test bed, modeling scenarios, standardizing the automated methods for exchange of cyber threat information, and advancing toward a Machine-to-Machine Automated Threat Response capability.
- ✓ National and Regional Cyber Outreach: INL personnel routinely participate as national laboratory subject matter experts in the planning and responses for several significant national and regional exercises. Recent examples include:

  1) National Grid Security Exercises: INL supported the planning and execution of North American Electricity Reliability Corporation (NERC) during GridEx III (held November 2015) and is participating in planning and execution efforts for GridEx IV. GridEx III included over 4400 utility and government staff from 364 organizations, the White House National Security Council, departments of

U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing: July 12, 2016
S. 3018, the Securing Energy Infrastructure Act,
Protections Designed to Guard Against Energy Disruptions
Questions for the Record Submitted to Mr. Brent Stacey

Energy, Homeland Security, and Defense, the Federal Emergency Management Administration, National Security Agency, Federal Bureau of Investigation and the National Guard.

2) INL threat analysts and cybersecurity researchers are suppored the Idaho National Guard and Federal Emergency Management Agency in preparations for the Cascadia Rising Exercise – a recent Pacific Northwest exercise that conducted life-saving and life-sustaining response operations in the aftermath of a Cascadia Subduction Zone disaster.

3) INL participated with Utah State Emergency Operations Center representatives during the Cyber Guard 2016 Exercise, a national exercise designed to improve nationwide public-private cooperation and response to cyberattack.

- ✓ Federal, State, and Community Resiliency Assessments: INL supports resiliency assessments across multiple federal, state, and community organizations. INL experts provide analysis and recommendations, as part of the DHS's Regional Resilience Assessment Program (RRAP), for states across the nation (e.g., Arizona, Colorado, Delaware, Louisiana, New York, Texas, Utah, etc.). INL's contributions include recommendations for enhancing the security of fuel supply chain, cooling water supply, communication systems, and the cyber networks that enable the secure generation, transmission, and distribution of electricity.
- ✓ Department of Defense Microgrids: INL researchers were members of an Office of the Secretary of Defense Joint Concept Technology Demonstration (JCTD) project team, SPIDERS – a project which developed, demonstrated and deployed three secure operational microgrids at Joint Base Pearl Harbor-Hickam, Hawaii; Fort Carson Colorado; and Camp Smith, Hawaii. A collaboration of nine funding partners and the integration of technologies from five DOE laboratories, this JCTD resulted in increased reliability and improvements in the cybersecurity of the electric grid.

Question 3: As you mentioned in your testimony, Idaho National Lab is a leader when it comes to securing our critical infrastructure (including industrial control systems). Please describe some of the unique facilities and capabilities available at INL and how can they can be leveraged beyond the energy sector?

The Place - Idaho National Laboratory (INL) is an 890-square-mile multi-program laboratory with multiple testing and research complexes integrated with co-located, networked nuclear and national security facilities. INL has decades of mission experience

in science and engineering discovery and experimentation; highly complex physics-based system design and modeling; and first-of-its-kind construction and operation of sophisticated and full-scale experimental and production facilities. We operate and maintain the laboratory's essential infrastructure that supports power, water, communications, transportation, safety, health, security, environmental protection, and sanitation facilities and services comparable to what can be found small cities. Our research experiences have resulted in an embedded culture that emphasizes deployment of technologies, systems and facilities that deliver significant impacts for national objectives in energy security, national security, and economic growth. INL's science-to-engineering-to-deployment culture represents a unique national and international suite of assets optimized to address current threats to the national power grid and other critical U.S. infrastructure sectors.

The People – INL employs over 4000 scientists, engineers, technicians and support staff with skills and experiences relevant to the protection of energy infrastructure (e.g., power systems and electrical engineering, large-scale user facilities/advanced instrumentation, cyber and information sciences, advanced computer science, visualization and data, etc.) INL's researchers are world-class leaders in their fields due to immediate access to the unique facilities and support infrastructure needed to conduct exploratory proof-of-principle experimentation. For energy infrastructure protection, our research expertise, unique measurements systems, and full-scale experimental equipment and testbeds enable us to apply high performance computing modeling and simulation of systems to validate complex infrastructure interdependencies and physical effects on grid infrastructure components; explore the fundamental physical science concepts and engineering principles of transformational technologies; and validate the performance of these transformative solutions. The breadth of skills and immediate access to unique scientific capabilities enable these researchers to accelerate the transition and impacts of innovative concepts far beyond grid security. Our subject matter experts, many with security clearances, conduct research and perform assessments on government installations for infrastructure security vulnerabilities, on available renewable energy resources and microgrids to ensure an uninterruptable supply of electricity under various situations, and on smart grid technologies to increase energy efficiency and enhance security.

The Facilities – With 111 miles of electrical transmission and distribution lines, 579 buildings, 14 miles of railroad lines, a mass transit system, and 177 miles of paved roads, INL has the nation's largest and most adaptable energy infrastructure research, development, test and evaluation range. The experimental assets for grid research are designed specifically to enable isolated and/or integrated system experimentation of grid

protection concepts for cyber, communications, physical, and/or natural phenomena. The National Power Grid Reliability Test Bed, like other INL research and test bed facilities, is readily accessible for government, industry and academic collaborative research and testing. INL's assets include, but are not limited to:

- The National Power Grid Reliability Test Bed and power research laboratories includes an isolated and customizable utility-scale transmission system linked with state-of-the-art Supervisory Control and Data Acquisition (SCADA), communications, and cyber testing capabilities. This transmission system enables grid-scale science and engineering exploration of electricity system integration challenges while assuring safety, security and resilience against all-hazards.
- INL's Wireless Test Bed and wireless communications research laboratories are equipped with 2nd, 3rd, and 4th generation commercial scale cellular, land mobile radios, wireless local area networks and backhaul with multiple transmission and receiving systems across the full wireless spectrum. INL's Wireless Test Bed enables large-scale development, testing and evaluation of wireless technologies for assuring the reliability and security of communications for government, public safety, and emergency response. Situated in an isolated environment, INL is authorized by the National Telecommunications and Information Administration to operate as an experimental radio station for advanced technology testing and training without putting the public at risk and without impacts to critical or emergency infrastructures.
- The National Security Test Range enables the safe and secure study of violent, high-speed kinetic phenomena on structures and systems, as well as the effectiveness of armor against the threats of explosives and military/commercial ballistic weapons.
- Control System and Cybersecurity Innovation Labs enable the discovery, reverse-engineering, and forensics analysis of vulnerabilities and security performance evaluation at the chip-level to full-scale operational systems.
- Real-Time Digital Simulator (RTDS) Laboratory enables high fidelity, physics-based transient power system simulation for fast, reliable, accurate, and cost-effective study of power systems to test the security and resilience performance of physical devices in multiple configurations (e.g., hardware-in-the-loop, grid-in-the-loop, controller-in-the-loop, etc.,) and validate energy system performance models.

U.S. Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing: July 12, 2016
S. 3018, the Securing Energy Infrastructure Act,
Protections Designed to Guard Against Energy Disruptions
Questions for the Record Submitted to Mr. Brent Stacey

The Capabilities - INL applies our people and facilities to national level security challenges to protect all 16 of our nation's critical infrastructure sectors. Examples include:

- Supporting the DHS Industrial Control System Cyber Emergency Response Team's (ICS-CERT) which provides current cyber threat response, and information sharing, guidance and training on industrial sector protections for U.S. Government and private sector infrastructure asset owners.
- Appling grid, wireless, and cybersecurity research and test beds to support the development of engineering standards for public safety to guide the implementation of a communications network for the First Responder Network Authority (FirstNet), the development of planning guidance for smart grid communications, and the development of cybersecure vehicle-to-vehicle communications systems.
- Translating and transitioning testing results from grid control system cybersecurity and electromagnetic pulse/geomagnetic disturbance effects to better protect nuclear energy, medical devices, and transportation systems.
- Integrating enhanced control system cybersecurity into the common control system architecture, components, and systems within or on military vehicles and facility infrastructure.
- Exploring and evaluating innovative research concepts for protection against high consequence cybersecurity threats to water supply and wastewater systems utilizing INL's Water Security Test Bed. Also examining the potential to design-in control system cybersecurity into next generation renewable and nuclear-hybrid energy systems.
- Deployment of expertise and modeling capabilities to support national cyber and resilience objectives for information sharing through training and education outreach, assessments, and exercises.

Statement for the Record by the

AMERICAN PUBLIC POWER ASSOCIATION (APPA)

Submitted to the

SENATE ENERGY & NATURAL RESOURCES COMMITTEE

SUBCOMMITTEE ON ENERGY

For the July 12, 2016, Subcommittee Hearing to

"Receive testimony on S.3018, the Securing Energy Infrastructure Act, and to examine protections designed to guard against energy disruptions"

The American Public Power Association (APPA) appreciates the opportunity to submit a statement for the record for the Senate Energy & Natural Resources Subcommittee on Energy's hearing to "Receive testimony on S.3018, the Securing Energy Infrastructure Act, and to examine protections designed to guard against energy disruptions." APPA supports and agrees with the testimony of Mr. Duane Highley of the Arkansas Electric Cooperatives Corporation (AECC) on behalf of the National Rural Electric Cooperative Association (NRECA).

Protections Designed to Guard Against Energy Disruptions

The electric utility industry (including public power utilities) takes very seriously its responsibility to maintain a strong electric grid. Efforts to protect against energy disruptions include: mandatory and enforceable standards; increased threat information sharing; public-private partnerships; a "defense-in-depth" strategy; and sector-wide preparation exercises.

Mandatory and Enforceable Standards

The electric utility industry is the only critical infrastructure sector besides nuclear power plants (a part of the overall sector) that has any mandatory and enforceable federal regulatory regime in place for cybersecurity. Congress approved a mandatory and enforceable reliability standards regime for the bulk power system in the Energy Policy Act of 2005, known as Section 215 of the Federal Power Act (FPA). Under 215, the North American Electric Reliability Corporation (NERC), working with electric industry experts, regional entities, and government representatives, drafts reliability and cyber security standards that apply across the North American grid, inclusive of Canada. Participation by industry experts and compliance personnel in the NERC standards development process ensures that the standards are technically sound, fair, and balanced. The Federal Energy Regulatory Commission (FERC) has the power to then approve or remand those standards as they apply in the United States. To ensure compliance, NERC conducts rigorous audits and can levy substantial fines for non-compliance. Additionally, FERC can instruct NERC to develop new or revised reliability standards with a very short turn-around time.

APPA and its members, as well as other utilities, are active participants in the NERC Critical Infrastructure Protection (CIP) standards drafting process on cyber- and physical-security. As attacks on critical electric infrastructure are ever-changing, so must be the nature of our defenses, whether they are designed to protect cyber or physical assets. CIP Version 6 is in effect and became enforceable on July 1, 2016. FERC also approved a physical security standard to protect the Nation's most critical substations that became enforceable on October 1, 2015.

Information Sharing
APPA has long recognized that increased information sharing and appropriately tailored liability protection would further enhance the industry's ability to guard against cyber attacks. As such, APPA strongly supported passage of the Cybersecurity Act of 2015, which was incorporated as Division N of H.R. 2029, the Consolidated Appropriations Act, 2016. The Act sets up policies and procedures for sharing cybersecurity threat information between the federal government and private entities (which include public power) and between private entities and provides limited liability protection for these activities if conducted in accordance with the Act. The Departments of Homeland Security (DHS) and Justice released final guidance on implementation of the Act on June 15, 2016. APPA is reviewing this guidance and is planning education opportunities for members on the topic for summer and fall 2016.

In addition to the Cybersecurity Act of 2015, APPA also strongly supported Section 61003 of P.L. 114-94 (the Fixing America's Surface Transportation Act or "FAST Act"), which gave the Secretary of Energy broader authority to address grid security emergencies under the FPA and clarifies the ability of FERC and other federal agencies to protect sensitive critical electric infrastructure information (CEII) from public disclosure under the Freedom of Information Act (FOIA) and other sunshine laws. Under the FAST Act, FERC-designated CEII would be exempted from disclosure for a period of up to five years with a process to lift the designation or challenge it in court. The bill also requires FERC to facilitate voluntary information sharing between federal, state, local, and tribal authorities, the Electric Reliability Organization, regional entities, and owners, operators, and users of the bulk-power system in the U.S. In addition it establishes sanctions for the unauthorized disclosure of shared information.

Public-Private Partnerships
To maintain and improve upon the high level of reliability consumers expect, electric cooperatives, public power utilities, and investor-owned utilities all work with each other and the NERC, DHS, the Department of Energy (DOE), and FERC on matters of critical infrastructure protection – including sharing needed information about potential threats and vulnerabilities related to the bulk electric system.

In 2013, the electric utility industry reorganized the Electricity Subsector Coordinating Council (ESCC) to ensure high level engagement. The new ESCC serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The ESCC includes utility CEOs and trade association leaders representing all segments of the industry. Their counterparts include senior Administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

"Defense-in-Depth" Sector-Wide Preparation Exercises

The goal of every utility and the industry as a whole is to manage risk prudently. Still, there are tens of thousands of diverse, often remote, facilities throughout the U.S. and Canada that cannot be protected 100 percent from all threats, requiring utilities to prioritize facilities that, if damaged, would have the most severe impacts on their ability to "keep the lights on." As such, the electric power industry employs threat mitigation known as "defense-in-depth" that focuses on preparation, prevention, response, and recovery to a wide variety of hazards to electric grid operations, including natural events, such as severe weather or geomagnetic disturbances (GMDs) caused by solar storms, as well as malicious events such as physical or cyber attacks directed at the grid, and primarily response and recovery for electromagnetic pulses (EMPs) caused by an attack on the homeland via the high-altitude detonation of a nuclear weapon.

Key to reliability efforts are the crisis management and site-specific security plans developed by electric utilities to ensure that operations and infrastructure systems are properly supported. In addition, a number of redundancies are built into the system, in many cases allowing utilities to re-route power around damaged facilities. Utilities also partner with federal, state/ provincial, and local government and law enforcement agencies in both the United States and Canada to ensure that they can respond effectively to any event that may impact their operations.

On November 18-19, 2015, APPA and other members of the electric utility sector participated in Grid Ex III, a simulated combined cyber- and physical-attack exercise organized by NERC. Designed to enhance and improve cyber- and physical-security resources within the electric utility industry, the Grid-Ex drill is held every two years. The first exercise took place in 2011, the second in 2013, and the 2015 drill was the third. The exercise gave the 360 electric entities and government agencies participating the opportunity to check the readiness of their crisis-action plans through a simulated security exercise to self-assess response and recovery capabilities, and to adjust actions and plans as needed, while communicating with industry and government information sharing organizations. Participating utilities faced simulations of prolonged, coordinated cyber-attacks against certain automated systems used by power system operators. The scenario also included coordinated physical attacks against key transmission substations and generation facilities. These attacks caused utilities to enact their crisis-response plans and "walk through" internal security procedures. While the details of the exact simulations are classified, press reports indicated that the threat scenario included attempts to turn out the lights across America, inject computer viruses into grid control systems, bomb transformers and substations, and knock out power lines by the dozen. Grid Ex III was a very useful exercise for APPA and participating public power utilities, allowing them to test their readiness and preparedness for both cyber and physical attacks.

On June 12, 2016, APPA hosted its second annual security tabletop exercise. The exercise scenario featured a coordinated cyber attack similar to the Ukraine cyber attack that occurred in late 2015. Participants included small to medium sized public power utilities. An after-action report to further refine procedures and strengthen public power's response to cyber attacks is underway.

S.3018, the Securing Energy Infrastructure Act

S.3018, the Securing Energy Infrastructure Act, would establish a two-year pilot program at the DOE's national laboratories to identify security vulnerabilities in sections of the grid whose compromise could threaten public safety or national security. Specifically, the legislation directs the study to research, test, develop, and implement "technology platforms and standards to isolate and defend industrial control systems of covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities, including (A) analog and nondigital control systems; (B) purpose-built control systems; and (C) physical controls." Participation in the study would be voluntary and would be overseen by a working group that includes representatives from DOE, DHS, NERC, the Nuclear Regulatory Commission, the intelligence community, and the electric utility industry. APPA believes that the goals and intentions of this legislation are important and worthwhile and appreciates the interest of the legislative sponsors in this critical issue. We would like to stress, however, that it is important to avoid a "one-size-fits-all" strategy to combating the ever-evolving threats to the electric grid that could hamstring the industry from adapting to developing threats. We would like to echo Mr. Duane Highley statement that "…security issues relevant for an entity on the bulk electric system may be very different from another entity due to geography, engineering architecture and redundancies among other differences, just as security issues relevant for the bulk electric system are not necessarily equivalent to issues facing the local distribution system."

Conclusion

APPA appreciates the opportunity to offer these comments to the Subcommittee. We look forward to working with the Subcommittee on the critical issue of protecting the reliability of our nation's electric grid.

U.S. Senate Committee on Energy & Natural Resources
Subcommittee on Energy
304 Dirksen Senate Building
Washington, DC 20510

7/14/2016

RE: Securing Energy Infrastructure Act of 2016

Protect Our Power respectfully requests that the following comments concerning S. 3018, the Securing Energy Infrastructure Act, be included in the record for the Senate Committee on Energy and Natural Resources Subcommittee on Energy's July 12, 2016 hearing on the bill.

Background on Protect Our Power

Protect Our Power (PoP) is a coalition of concerned stakeholders that recognize the importance of a reliable electric system and whose sole purpose is to facilitate efforts by the government, industry and other stakeholders to take the steps necessary to improve the security and resiliency of our nation's power grid. In the wake of emerging threats, including natural threats, such as hurricanes and solar storms, and deliberate attacks such as cyber and physical attacks as well as the potential for a nuclear electromagnetic pulse (EMP) attack, we believe this mission must be an urgent national priority.

Protect Our Power advocates for practical, consensus-driven, timely solutions that will meaningfully address the vulnerability of the electric power grid. To that end, Protect Our Power is convening stakeholders and power system experts to develop and support initiatives—whether legislative, regulatory, policy, or industry-driven—that effectively respond to 21st Century threats to the security of the electric grid.

Comments

PoP supports the goal of S. 3018 to study and better understand the many threats facing our critical electricity infrastructure and evaluate technological changes and advances that could improve the resiliency of the electric grid. PoP encourages the Committee to act expeditiously in advancing this legislation so that this important research, development, and testing can begin. Given the vulnerabilities of the electric grid and potentially catastrophic consequences of a successful attack, time is of the essence.

PoP also urges the Committee, and Congress as a whole, to engage industry, regulators, and other stakeholders to take further action to address this pressing matter of national and economic security. While this legislation reflects a positive step, all should recognize that a comprehensive, coordinated plan of action is required to adequately secure the electric grid against 21st Century threats. PoP's independent research confirms that there is widespread support among the public to address this vital issue. Indeed, according to a national poll conducted by PoP, more than 91 percent of respondents consider electricity to be critically or very important to their day-to-day needs, and 66 percent believe that the current state of the grid is vulnerable to physical or cyber attacks. In short, the public is aware that the electric grid is vulnerable, and considers this vulnerability to be one of vital importance. Further, the poll data also shows that a majority of the public not only appreciates the significance of grid security risks, but supports making investments that are necessary to address such risks. PoP urges further action on practical, consensus-driven solutions to this vital issue.

○