S. HRG. 115–262

CYBERSECURITY THREATS TO THE U.S. ELECTRIC GRID AND TECHNOLOGY ADVANCEMENTS TO MINIMIZE SUCH THREATS, AND TESTIMONY ON S. 79, THE SECURING ENERGY INFRASTRUCTURE ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON ENERGY

OF THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

MARCH 28, 2017

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

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

24–977 WASHINGTON : 2018

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
CORY GARDNER, Colorado	JOE MANCHIN III, West Virginia
LAMAR ALEXANDER, Tennessee	MARTIN HEINRICH, New Mexico
JOHN HOEVEN, North Dakota	MAZIE K. HIRONO, Hawaii
BILL CASSIDY, Louisiana	ANGUS S. KING, JR., Maine
ROB PORTMAN, Ohio	TAMMY DUCKWORTH, Illinois
LUTHER STRANGE, Alabama	CATHERINE CORTEZ MASTO, Nevada

SUBCOMMITTEE ON ENERGY

CORY GARDNER, *Chairman*

JAMES E. RISCH	JOE MANCHIN III
JEFF FLAKE	RON WYDEN
STEVE DAINES	BERNARD SANDERS
LAMAR ALEXANDER	AL FRANKEN
JOHN HOEVEN	MARTIN HEINRICH
BILL CASSIDY	ANGUS S. KING, JR.
ROB PORTMAN	TAMMY DUCKWORTH
LUTHER STRANGE	CATHERINE CORTEZ MASTO

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

CONTENTS

OPENING STATEMENTS

WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

CYBERSECURITY THREATS TO THE U.S. ELECTRIC GRID AND TECHNOLOGY ADVANCEMENTS TO MINIMIZE SUCH THREATS, AND TESTIMONY ON S. 79, THE SECURING ENERGY INFRASTRUCTURE ACT

TUESDAY, MARCH 28, 2017

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

The Subcommittee met, pursuant to notice, at 2:17 p.m. in Room SD–366, Dirksen Senate Office Building, Hon. Cory Gardner, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF HON. CORY GARDNER, U.S. SENATOR FROM COLORADO

Senator GARDNER [presiding]. We will go ahead and get the Subcommittee started. Senator Manchin will be joining us shortly, but thank you very much, as we call this Subcommittee hearing to order.

Good afternoon. This is the Subcommittee on Energy's first 115th Congress hearing. I am honored to chair the Subcommittee this Congress and look forward to working with the Subcommittee's Ranking Member, Senator Manchin.

The Energy Subcommittee is certainly important to my home state of Colorado. In Colorado, we have coal in the northwestern part of the state, oil on the western slope, natural gas and wind on the eastern plains and solar in the San Luis Valley. We are truly an all-of-the-above energy state and very proud of that fact.

We are also home to the Department of Energy's National Renewable Energy Laboratory which is instrumental in research and development for new technologies in advancing grid modernization, renewable energy and energy efficiency that will transform the marketplace.

As Chairman, I look forward to promoting a strong and responsible energy policy that is critical to unleashing the nation's energy potential, and I look forward to using the Subcommittee to advance policies that benefit Coloradans and all Americans.

Today the Subcommittee will examine the cybersecurity threats to the U.S. electric grid and technology advancements to minimize such threats and receive testimony on Senate bill 79, the Securing Energy Infrastructure Act. We will discuss the risks we face and the actions we should follow to protect our energy infrastructure

from the impact of cyberattacks. In addition to defensive strategies, I am also interested in discussing whether there is a need to build preparedness and response capabilities in case of a long-term, widespread outage.

The American people and American businesses depend on reliable and affordable electricity. These same customers expect the over 3,000 utilities in our country to be thinking ahead, coordinating actions and being responsive to our evolving demands.

If we are not prepared for cyberattacks, a Ukraine-like situation could take place in the United States. In 2015 an attack on power companies in Ukraine resulted in 225,000 Ukrainians losing power. Last December there was an attack in Ukraine that resulted in another round of power outages but the strategy on the Ukrainian grid was more complex than the year before.

Hackers are certainly trying to create that kind of havoc here in the United States. One U.S. utility CEO has said, "If I were to share with you the number of attacks that come into the network every day, you would be astounded." And it is not from people working out of their garage. It is from nation states that are trying to penetrate systems.

I am encouraged to see that industry through the Electricity Sector Coordinating Council is working to collaborate and create best practices and partnerships with the government.

The government and industry have also made great strides in cybersecurity through the creation of the National Institute of Standard and Technology, or NIST, cybersecurity framework, and the Electricity Information Sharing and Analysis Center (E-ISAC).

It is concerning, however, that we continue to hear of attacks from so many fronts. Hackers are going after personal information and personal accounts that can be disastrous and financially painful for those affected. We hear of ransomware attacks requiring payments to resume access to machines and controls. We hear of millions of dollars being spent across industry and government to protect from these ever-changing threats to our national progress.

The questions that loom, however, are how, when, where is that next cyberattack going to happen? Are we prepared to react?

I am hopeful that through this hearing and the opportunity we have to hear your testimony today and in the coming months we can strengthen both our preparedness and our response capabilities.

I already see opportunities to enhance our cyber workforce and the need to gain clarity on the coordinated response actions of the Department of Energy Secretary and industry leaders. I am hopeful that we will uncover additional opportunities today.

With that, if you are ready, I will turn it over to our Ranking Member, Senator Manchin, from West Virginia.

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

Senator MANCHIN. Thank you, Mr. Chairman. I want to thank you for scheduling this hearing and for your work on this important issue.

Now I want to thank all of you for being here today, and I am looking forward to the quality of discussions ahead.

I think our states all have a lot in common, particularly because both of our states are domestic energy exporters. I think we both recognize the importance of that role in this nation.

I also want to thank Senators King, Heinrich and Cortez Masto for the roles that they are playing in leadership on this issue.

I appreciate that our witnesses are joining us today for this very timely discussion about the critical nature of our electrical grid and the very real cyber and physical threats that we face.

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, offices, and supplies factories, every day. People and businesses in the northeast and 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 over 80,000 kilowatt hours of electricity, and the EIA consistently reports that West Virginia typically exports more electricity than it consumes. 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. Instances 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 in those 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 cyberattack.

In December 2015, the first successful cyberattack took place against part of Ukraine's electric grid, demonstrating that shutting down the grid is a real possibility. Several hundred thousand customers were without power for several hours and many experts suggest that Russia was responsible.

A year later, in December 2016, there was another power outage, this time in Northern Kiev, Ukraine. For approximately one hour, according to the affected Ukrainian power company, a blackout was caused by a cyberattack which was very similar to the allegedly Russian cyberattack on Ukraine's grid a year prior.

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 79 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 to 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, or FERC as we know it, has identified a small number of critical group-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 intrusion is critical as new technologies and threats continue to emerge from transnational, organized crime, terrorist 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 on the electric grid. While the number has shrunk to 16 percent in 2015, there is much more to be done.

That is why I supported 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. It does not happen often here. The bill included a cyber energy section that I supported when it passed the Senate.

The cyber energy section directed the Secretary of Energy to carry out an energy/cybersecurity workforce development program. It also directed the Secretary of Energy to carry out a supply chain testing program for grid components. As more and more of our grid's components are both network enabled as well as manufactured abroad, we need to be sure that every piece of our national security assets has been rigorously vetted. It also proposed to double the Department's current investments in all energy/cybersecurity programs, and encouraged 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.

Unfortunately, Congress adjourned last year before the Conference Committee was able to complete its work on this legislation, but the need to act still remains.

The ability to deliver energy quickly, securely and without interruption is something that West Virginia prides itself on, which is why I am particularly appreciative of Senator King's passion for this issue. Senator Heinrich and Senator Risch's ongoing efforts on this bill are also to be applauded. I also want to thank the Chair for holding this hearing, which was much needed.

I look forward to the testimony of our witnesses.

Senator GARDNER. Thank you, Senator Manchin.

Before we introduce the witnesses today, Senator King, if you would like to say a few words about S. 79, the Securing Energy and Infrastructure Act.

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

Senator KING. Thank you, Mr. Chairman.

You both have quite eloquently outlined the need. I, in addition to this Committee, sit on both the Armed Services and Intelligence Committees. Over the past four years we have had dozens, if not hundreds, of warnings of cyberattacks against critical infrastructure, and the grid certainly qualifies for that. I characterize what we are looking at now as the longest windup for a punch in world history. We know it is coming, we just don't know where and when and the risks are enormous.

The second thing I wanted to say is that there is no single solution to this problem. The utilities themselves have done amazing and wonderful work in defending themselves. FERC has worked with them. There are lots of solutions percolating around the pilot program that is proposed in S. 79 that basically came out of work that was a result of the Ukraine hack in 2015. In this attack they found that one of the reasons the Ukrainian grid was able to be resilient was that there were some old-fashioned analog switches, and perhaps even places where old Dimitri with his dog had to go out and pull a switch, that saved the grid from a real catastrophe.

What we are talking about here is not rebuilding or re-engineering the entire grid, but to really ask the question, are there some back to the future answers at critical points that might protect us from the kind of attack we know is coming?

It is no coincidence that the four principle sponsors of this bill, myself, Senator Risch, Senator Heinrich and Senator Collins are also all on the Intelligence Committee, and our work on this bill really started in that Committee and has carried through on to this Committee.

So I look forward to the hearing. I appreciate your calling it.

The other thing I want to express is that time is running out. I do not want to go home to my constituents in the middle of a blackout and say well, we might have gotten to this, but we had different committees that had jurisdiction and we really could not quite get at it in the Conference Committee. That is not going to cut it.

I think this qualifies as an emergency, and I hope that we can act promptly. I hope that this is a bill that might get the level of support that it could go through on its own without waiting for a more comprehensive energy bill because that endangers, I think, our taking a practical step that could be of significant help to us.

Thank you, Mr. Chairman.

Senator GARDNER. Thank you, Senator King.

Before we do the formal introductions, we have two members of the Committee that may wish to say a word or two about our witnesses today.

Senator Alexander.

**STATEMENT OF HON. LAMAR ALEXANDER,
U.S. SENATOR FROM TENNESSEE**

Senator ALEXANDER. Thank you, Senator Gardner.

I am delighted to welcome Dr. Thomas Zacharia to the Committee. He is the Deputy Director for Science and Technology at

the Oak Ridge National Laboratory and presides over one of the largest research budgets in our country. I will say two things about him.

One is he developed the computer program at Oak Ridge which has produced the fastest computers in the United States, in any event. And next year, in 2018, there will be a computer five times as fast. That was his doing and his leadership. So he can speak with authority to the question of what can supercomputing do to help us with cybersecurity, with the grid, with waste fraud and abuse and Medicaid and Medicare—anything that has to do with data manipulation, Thomas knows how to build and operate the fastest computers in the world.

Second, the Oak Ridge Laboratory is the largest science and energy laboratory, and he works with a lot of people. He is very well respected by all of the people with whom he works.

So I welcome him here and look forward to his testimony.

Senator GARDNER. Thank you, Senator Alexander.

Senator Franken.

STATEMENT OF HON. AL FRANKEN,
U.S. SENATOR FROM MINNESOTA

Senator FRANKEN. Senator Gardner, Xcel may operate in Colorado, but it is headquartered in Minneapolis.

[Laughter.]

Xcel also serves more than one million people in the Twin Cities area. So, I want to welcome Ben Fowke here today. Thank you, sir.

I know we are going to be discussing cybersecurity, and I look forward to hearing your thoughts on that crucial subject as well as your role on the National Infrastructure Advisory Council which advises the President on crucial infrastructure activity.

But first, I want to commend Xcel for being a leader in generating clean energy and reducing carbon emissions. More than 50 percent of the electricity you supply in Minnesota comes from wind, hydro, solar, biomass or nuclear. This helps us reduce emissions.

Your company is on track to reduce greenhouse emissions to 30 percent of 2005 levels by 2020, and you are not stopping there. You have just announced that you are going to add an additional 3,380 megawatts of wind capacity across seven states.

We are very proud of what Minnesota has done since Governor Pawlenty signed in our renewable energy standard and our energy efficiency resource standards.

I want to thank you for Xcel's leadership, for your personal leadership, and for showing how we can transition to clean sources of electricity while keeping rates low.

I look forward to your testimony, and I think it is terrific that you also operate in other states.

[Laughter.]

Senator GARDNER. Yes. And I, Mr. Fowke, would echo that. Thanks for making it clear to me as a kid who grew up on the eastern plains of Colorado, the dam wind isn't just one word. You can actually do something with it.

[Laughter.]

So, thank you.

In addition to Mr. Fowke and Dr. Zacharia, we are also joined by Michael Bardee, the Director of the Office of Electric Reliability at the Federal Energy Regulatory Commission (FERC), and Mr. John Di Stasio, President of the Large Public Power Council.

Thanks to all of you for being here and your time and testimony today.

Mr. Bardee, if you would like to begin with your testimony? Thank you.

STATEMENT OF MICHAEL BARDEE, DIRECTOR, OFFICE OF ELECTRIC RELIABILITY, FEDERAL ENERGY REGULATORY COMMISSION

Mr. BARDEE. Thank you, Chairman Gardner.

Chairman and members of the Subcommittee, thank you for the opportunity to testify. My name is Michael Bardee, and I'm the Director of FERC's Office of Electric Reliability. I am here today as a Commission staff witness and my remarks do not necessarily represent the views of the Commission or any individual Commissioner.

In the Energy Policy Act of 2005 Congress gave the Commission a responsibility to oversee mandatory, enforceable reliability standards for the nation's Bulk-Power System, excluding Alaska and Hawaii. Cybersecurity is an important part of this responsibility.

In 2008, the Commission approved NERC's first set of cybersecurity or CIP standards while also directing NERC to develop changes. Since then, the Commission has approved various changes to the CIP standards. Last year, utilities implemented version five of the CIP standards for high and medium impact assets. This year, utilities are implementing version five for low-impact assets.

Last July, the Commission directed NERC to develop a standard on supply chain risk management. There is no requirement for any specific controls, nor did FERC seek one size fits all requirements. Instead, FERC said the standard should define the objectives while allowing flexibility on how to meet those objectives. NERC is working on a standard now and is due to submit it to the Commission in September.

Also in July, FERC sought public comment on whether to modify the CIP standards for the protection of control centers used to monitor and control the Bulk-Power System. FERC cited the 2015 cyberattack on the grid in Ukraine as an example of how cyber systems used to operate and maintain a grid, unless protected adequately, can create cyber risks. FERC is reviewing the comments submitted in response and considering whether further action is appropriate on these issues.

While mandatory standards are an important part of the Commission's work on cybersecurity, FERC also worked with industry in other ways, sharing information, encouraging best practices and providing assistance when requested, including through our Office of Energy Infrastructure Security.

The goal of these efforts is to mitigate the risk of a cyber incident, but if such an event ever does happen, the industry also needs to be prepared to restore the grid. For this reason, last year, FERC completed a report with NERC and its regional entities on grid restoration and recovery. The report was based on working

closely with a number of utilities and recommended various practices and additional studies. Work on those additional studies is ongoing.

The work proposed in S. 79 could help utilities to maintain a secure electric grid. Utilities have come to rely increasingly on digital tools for operating the Bulk-Power System. A broad scale reversion to predigital technology is uneconomic, unjustified and perhaps even impossible.

S. 79 focuses on only the most critical systems of the covered entities. Also, S. 79 does not require adoption of any particular technology and instead requires only research and testing. Any decision on implementation would be made only after sufficient research and testing.

I would suggest one small change to S. 79 and that is to add FERC to the list of entities specifically included as a member of the working group in the bill.

Thank you for allowing me to testify today. I would be glad to address any questions you may have.

[The prepared statement of Mr. Bardee follows:]

Testimony of Michael A. Bardee
Director, Office of Electric Reliability
Federal Energy Regulatory Commission
Before the Subcommittee on Energy
Committee on Energy and Natural Resources
United States Senate
March 28, 2017

Introduction

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

The Commission's role on reliability is to help protect and improve the reliability of the Nation's Bulk-Power System through effective regulatory oversight as established in the Energy Policy Act of 2005 (EPAct 2005). My testimony summarizes the Commission's oversight of the reliability of the Bulk-Power System and, specifically, the Commission's implementation of that authority with respect to cybersecurity. I then address S. 79, the Securing Energy Infrastructure Act.

FERC's Reliability Authority

In EPAct 2005, Congress tasked the Commission with a responsibility to oversee mandatory, enforceable reliability standards for the Nation's Bulk-Power System (excluding Alaska and Hawaii). This authority is in section 215 of the Federal Power Act. Section 215 applies only to the Bulk-Power System, not facilities used in local distribution.

Section 215 requires the Commission to select an Electric Reliability Organization (ERO) that is responsible for proposing, for Commission review and approval, reliability standards to help protect and improve the reliability of the Nation's Bulk-Power System. The Commission certified as the ERO the North American Electric Reliability Corporation (NERC). The reliability standards apply to the users, owners and operators of the Bulk-Power System and become mandatory in the United States only after Commission approval. The ERO also is authorized to impose, after notice and opportunity for a hearing, penalties for violations of the reliability standards, subject to Commission review and approval.

The Commission may approve proposed reliability standards or modifications to the standards if it finds them "just, reasonable, not unduly discriminatory or preferential, and in the public interest." If the Commission disapproves a proposed standard or modification, section 215 requires the Commission to remand it to the ERO for further consideration. The Commission, upon its own motion or upon complaint, may direct the ERO to submit a proposed standard or modification on a specific matter but it does not have the authority to modify or author a standard.

FERC and Cybersecurity

Cybersecurity is an important part of the Commission's responsibility to oversee reliability standards for the Bulk-Power System. In 2006, NERC proposed to the Commission an initial set of cybersecurity standards, known as the Critical Infrastructure Protection (CIP) standards. Critical infrastructure, as defined by NERC for purposes of the CIP standards, includes facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the "bulk electric system." In 2008, the Commission approved NERC's proposed CIP reliability standards while also directing NERC to develop modifications. Since then, the Commission has approved various changes to the CIP standards. The CIP standards specify mandatory requirements for utilities, including: how to identify and categorize cyber assets and systems; processes and procedures for maintaining these systems; and ensuring that only appropriate personnel have access to these systems, among others. Last year, utilities implemented version 5 of the CIP standards for high- and medium-impact assets. This year, utilities are implementing version 5 for low-impact assets.

In July 2016, the Commission directed NERC to develop a reliability standard addressing the supply chain for industrial control system hardware, software, and related services associated with the bulk electric system. Specifically, FERC directed NERC to develop an objective-based standard that would require each affected utility to develop and implement a plan that includes security controls for its cyber supply chain. FERC ruled that the standard should address four areas: ensuring that the software used to run these systems is authentic; ensuring that remote access by vendors to these systems is secure; information system planning; and vendor risk management and procurement controls. There is no requirement for any specific controls, nor does FERC require any "one-size-fits-all" requirements. Instead, FERC said that the standard should require utilities to develop a plan to meet the four objectives, while allowing flexibility on how to meet the objectives. NERC is working on a standard now, and is due to submit it to the Commission in September 2017.

Also in July 2016, FERC issued a Notice of Inquiry (NOI) on whether to modify the CIP standards regarding the cyber protection of control centers used to monitor and control the Bulk-Power System. FERC cited the 2015 cyberattack on the electric grid in

Ukraine as an example of how cyber systems used to operate and maintain interconnected networks more efficiently can have the unintended effect of creating cyber vulnerabilities. FERC sought comment on possible changes to the CIP standards to address separation from the Internet and to require a computer practice for preventing unauthorized programs from running, known as "application whitelisting." FERC is reviewing the comments submitted in response to the NOI, and considering whether further action is appropriate on these issues.

While mandatory standards are an important component of the Commission's work on cybersecurity, FERC also works with industry in other ways to enhance security. For example, FERC's Office of Energy Infrastructure Security (OEIS) provides leadership, expertise, and assistance in identifying, communicating, and seeking comprehensive solutions to significant potential cyber and physical security risks to the energy infrastructure under the Commission's jurisdiction. OEIS works directly with governmental and private sector energy industry entities to identify and share information on threats and vulnerabilities, and to promote voluntary mitigation practices that are complementary to mandatory regulations promulgated and enforced by the Commission and by state authorities. Engaging with the regulated community outside of the traditional regulatory process facilitates the necessary exchange of timely information and subsequent implementation of state-of-the-art protective measures.

The goal of the Commission's CIP standards and other cyber-related efforts is to mitigate the risk of a cyber incident that harms the reliability of the electric grid. However, in case such an event ever happens, utilities also need to be prepared to restore and recover the Bulk-Power System. For this reason, in January 2016, FERC completed a report with NERC and its Regional Entities on restoration and recovery of the grid. The joint review by FERC and NERC staff gathered information from a sample of utilities, and found they have extensive incident response and recovery plans. The report recommended various practices, such as verifying and testing modifications to a system restoration plan, obtaining insight from utilities that have experienced widespread outages, and obtaining independent technical review of recovery plans. The report also recommended certain follow-up studies, such as how to prepare for a loss of Supervisory Control and Data Acquisition (SCADA) computers and other data sources. Work on the additional studies is ongoing.

Other Efforts

Other agencies and organizations also contribute to the reliability and security of the electric grid. The Department of Energy, for example, is the Sector-Specific Agency for electrical infrastructure. In that role, DOE works with industry, state and local agencies, and other stakeholders to help protect our electric grid. This work may take the form of research performed by the various national laboratories, as proposed in S. 79.

Other examples are the Cybersecurity Risk Information Sharing Program (CRISP) and the Electricity Subsector Cybersecurity Capability Maturity Model (C2M2).

Similarly, security is addressed by the Electricity Subsector Coordinating Council, a public/private partnership for CEOs of critical infrastructure owners and operators to engage directly with senior government officials on policy-level security issues. This includes not only FERC and DOE, but also the Department of Homeland Security, the Federal Bureau of Investigation and others.

A secure electric grid is vital to our Nation. There is no "silver bullet" that can protect the grid. Instead, it depends on the efforts of many organizations and individuals, and requires ongoing adaptation, innovation and vigilance. And it requires ongoing dialogue and cooperation, to ensure that our efforts are not at cross-purposes or inefficient.

S. 79

S. 79, the Securing Energy Infrastructure Act, would establish a pilot program to study cyber vulnerabilities and consider solutions for isolating and protecting industrial control systems. Participation in the study would be voluntary, and would include a diverse working group. The program would involve 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." The effort would include research on analog and non-digital control systems; purpose-built control systems; and physical controls. The bill would authorize an appropriation of $10 million for the pilot program and $1.5 million for the related report and other work.

The effort proposed in S. 79 could potentially aid the utility industry, FERC and others to maintain a secure electric grid. Utilities have come to rely increasingly on digital tools for monitoring and operating the Bulk-Power System. These tools have enhanced the efficiency and effectiveness of utility operations significantly. A broad-scale reversion to pre-digital technology is uneconomic, unjustified, and perhaps even impossible. But I do not see S. 79 as proposing such action. Instead, S. 79 focuses on "the most critical systems of the covered entities." More importantly, S. 79 does not require adoption of any particular technology, and instead requires research and testing to determine if certain tools and technologies, when applied to limited circumstances, can enhance the security of the most critical systems. If this program succeeds in identifying more secure approaches for the most critical systems, the implementation of these approaches could be justified, depending on factors such as effects on operational efficiency. Over time, these approaches, if successful, also could be incorporated into new designs for an evolving Bulk-Power System. However, any decision on implementation should be made only after sufficient research and testing. These

approaches also may be useful not only in the context of the Bulk-Power System but in other industrial control systems too.

I would suggest one small change to S. 79. The working group required by S. 79 would specifically include the Department of Energy, the Nuclear Regulatory Commission, NERC and several other organizations, but not explicitly FERC. I believe FERC should also be listed as a member in the working group.

Conclusion

FERC will continue to work with the utility industry to seek ways to maintain and enhance the security of the electric grid. While mandatory reliability standards are an appropriate tool at times in this effort, other approaches are also important. S. 79 can support the goal of grid security by seeking unusual ways to reduce our risk without unduly sacrificing efficiency.

Thank you for allowing me to testify today. I would be glad to address any questions you may have.

Senator GARDNER. Thank you, Mr. Bardee.
Mr. Fowke.

STATEMENT OF BENJAMIN FOWKE III, CHAIRMAN OF THE BOARD, PRESIDENT & CHIEF EXECUTIVE OFFICER, XCEL ENERGY INC.

Mr. FOWKE. Senator Gardner, thank you for the invitation to speak at this important event. My name is Ben Fowke, and I'm the CEO of Xcel Energy. We're an energy company serving 3.5 million electric customers and two million natural gas customers in eight western and mid-western states.

I'm also a member of the Electric Sector Coordinating Council, or ESCC, and a member of the National Infrastructure Advisory Council, or NIAC, which advises the President on the protection of critical infrastructure.

Today I want to give you Xcel Energy's perspective on cybersecurity. Our modern society depends on electricity. Left unprotected from cyberthreats, the grid and electric service we all depend on could be at risk. Fortunately, Xcel Energy and other utilities have cybersecurity programs designed to adapt and to respond to this growing threat. And while no program is perfect, I believe that our industry's approach should give the Subcommittee increased confidence in the grid security. That confidence, however, should be taken in context. Attacks on our grid continue to grow in number and in sophistication, and it's really easy to fall behind.

It's clear we need better coordination with the DOE, the DHS and other Federal agencies. We need better, more timely information sharing, and we need new approaches to protect the devices that run the grid. Together, these strategies will enhance our cybersecurity defenses and the reliability of the power system.

Let me begin by acknowledging a difficult reality, the cyberthreat is growing. In 2016, Xcel Energy identified over 500,000 individual cyberattacks on our network. And although we're attacked daily, we're most concerned about potential attacks targeting the grid control systems.

Grid industrial control systems use digital technology to do their work and, like anything else that uses digital technology, these systems could be hacked. Without proper controls and monitoring a cyberattack of the control system could force the grid offline.

In response to this threat we work continuously to implement a flexible, effective, cybersecurity program. Our program separates and protects the control system from the Internet. We also use strong passwords and strictly control employee access to our critical systems. Our network is monitored by a dedicated team of cyber analysts on a 24/7 basis. We act immediately on actionable threat intelligence from government and private sources. We routinely install antivirus and antimalware programs. We also hunt for indications of compromise in order to detect and eliminate threats. Finally, we perform third party penetration testing of the network to test the effectiveness of our defenses.

Now despite these best efforts, no program is perfect; therefore, system recovery is one of our program's highest priorities. And while the challenges of system restoration would be different after

a cyberattack, our industry's experience with system restoration after storms and other outages does give us a leg up.

So, our cyber programs continue to improve but our program is and always will be a work in progress. There will always be more to do. We continue to look for ways technology can help protect the grid. For example, information sharing tools must become more sophisticated as the attacks become more sophisticated, and our arsenal of information sharing tools is continuously improving. Real-time machine-to-machine information sharing will further enhance our ability to respond to grid attacks, and we're working with other sectors to boost these capabilities. We're also beginning to deploy monitoring technologies to look for anomalies on the network that could indicate the presence of malware.

Turning to national cybersecurity policy. The electric industry, the DOE, the DHS, are working together through the ESCC to establish robust national cybersecurity efforts. My written testimony provides an overview of the programs spearheaded by the ESCC to enhance the nation's cybersecurity effectiveness; however, as I stated, there's always more to do and Congress and the Administration can help.

First, in a recent scoping session, NIAC has recommended to the President that the nation adopt a new transformational national framework for cybersecurity. The NIAC scoping study points to a fundamental problem with the current approach and that despite recent progress, national cybersecurity policy is often uncoordinated and unfocused. And while not speaking on the behalf of the Council, I believe the recommendations of the NIAC scoping study are urgently needed.

Second, in our experience, Federal agencies are often slow to provide classified information regarding cyberthreats to utilities. While protection of the nation's secrets is vital, a better process is needed to ensure that we have the necessary information in a timely fashion.

Finally, I believe we need both more research into cyber safeguards and the development of improved standards for software that controls the operational devices that were on the grid.

Thank you for the opportunity to be here with you today. I'd be happy to answer any questions.

[The prepared statement of Mr. Fowke follows:]

Testimony of

Benjamin G. S. Fowke III

Chairman of the Board, President & Chief Executive Officer

Xcel Energy Inc.

before the

U.S. Senate Committee on Energy & Natural Resources

Subcommittee on Energy

hearing to

Examine Cybersecurity Threats to the US Electrical Grid and Technology Advancements to Minimize the Threat

Chairman Gardner, Ranking Member Manchin, and members of the Subcommittee, thank you for the invitation to speak at this important hearing.

My name is Ben Fowke, and I am the CEO of Xcel Energy, an integrated energy company serving 3.5 million electric customers and 2 million natural gas customers. Headquartered in Minneapolis, we serve parts of eight Western and Midwestern states, including the Twin Cities of Minnesota, Denver and the Colorado Front Range, and the Texas Panhandle. We have a balanced energy mix that includes natural gas, coal, nuclear and renewables. We are also the nation's No. 1 utility wind energy provider with more than 8,000 megawatts on our system.

I am pleased to join you today to discuss the critical issue of cybersecurity and the potential threat to the electric grid. As a CEO of a major electricity supplier, one of my highest priorities is protecting Xcel Energy's customers from loss of electric service due to this growing threat. In conjunction with this priority, I have also joined with leaders in the electric sector, government and other lifeline sectors to help develop national programs and strategies to promote the protection of the nation's critical infrastructure. I am a member of the Electric Sector Coordinating Council, or ESCC, which serves as the principle liaison between the federal government and the electric power sector. I am also a member of the National Infrastructure Advisory Council, or NIAC, where I join with other leaders in the private sector to advise the President on ways that the nation can protect its critical infrastructure.

Xcel Energy and the utility industry recognize the significant threat associated with cybersecurity. Our modern society depends on electricity – and left unprotected, the grid and the reliability of electric service that we all depend on would be at risk. Fortunately, as I will discuss today, Xcel Energy and other utilities have developed cybersecurity systems and programs designed to adapt and respond to the evolving cyber threat. While no program is perfect, and constant vigilance is critical, I believe that our industry's approach should give our customers, the subcommittee and the American public increased confidence in the security of the electric grid.

That confidence, however, should be seen in the context of the significance of the challenge before us. Attacks on our grid continue to grow in number and sophistication. We in the industry have a responsibility to meet this mutating threat, but we need support from Congress and our federal partners. As my testimony indicates, we need better coordination with the Department of Energy, Department of Homeland Security and other agencies. We need better, more timely and efficient information sharing (including machine-to-machine information sharing technologies), and quicker dissemination of classified information regarding security threats. We need new research into technologies and strategies to protect the grid, including the technologies embedded in the operational devices that run our electric systems. Together, these strategies and the others I discuss today will enhance and maintain our cybersecurity defenses and help enhance the reliability of the electric grid.

The Cyber Threat to the Grid is Growing.

Like virtually every company in America, Xcel Energy is subject to a growing cyber threat. In 2016, Xcel Energy identified over 500,000 individual cyber attacks on our network. We are attacked daily, and, each year, the number of attempted intrusions grows. In the first quarter of this year, we have seen a 10% increase in the attacks against our network and systems since the prior year.

Most cyberattacks against a utility are similar to the attacks targeting any other company. These attacks seek personal or corporate data, attempt to defraud the company or its customers or hold the company's network hostage in a "ransomware" attack. While attacks from cybercriminals and "hacktivists" can do much damage to any company, utilities like Xcel Energy have an even greater concern, the same concern that prompted today's hearing: attacks from terrorists or nation-states targeting the control systems for the electric grid.

Most electric grids are controlled by industrial control systems, often called "Energy Management Systems" or the "Supervisory Control and Data Acquisition," or "SCADA" system. A SCADA system allows utility operators to control the flow of power efficiently to maintain reliable, low priced electric service. Using digital communication and control technology, a

SCADA system gives operators the ability to monitor power flows and voltage and adjust system resources to minimize electric service interruptions.

SCADA systems are used to control both the bulk electric system, i.e. the high voltage transmission system that delivers power to multiple communities across a wide geographic area, and the local distribution system. SCADA can open or close breakers, activate electric generation, shed load and take other steps to protect the grid from outages. SCADA systems for one utility or region are interconnected to other utilities or regions, helping to maintain electric reliability across broad swaths of the country. Modern electricity operations would be greatly impaired without SCADA.

Unfortunately, the convenience and efficiency of SCADA systems also leaves them vulnerable to cyberattack. SCADA uses digital communication and control, and, like anything that uses digital technology, it can be hacked without proper controls and vigilant monitoring. A cyberattack of the SCADA system could allow a third party to override the operator's control of the electric system and take malicious actions designed to prevent the delivery of power to customers. This subcommittee is aware of the attack on the Ukrainian electric system, which showed one possible pathway for the use of cyber tools to disrupt electric operation. The Ukrainian attack was the result of a chain of events that could have been disrupted had the Ukrainian utilities used many of the cybersecurity programs I will describe today. However, the success of the attack demonstrates that such an attack is possible in North America and confirms the need for grid operators to be vigilant.

Cybercriminals can gain this kind of control through several strategies, many surprisingly simple. They may simply steal or guess an operator's password. They may use "phishing" – emails that include malware that, once opened by the recipient, will download a file onto the system that allows access to the network, potentially to gain access to or control of the SCADA system. They may spread malware through "watering holes," i.e. compromised websites or ad content on legitimate sites. They may imbed malware in physical devices that are installed in the SCADA system or elsewhere on the grid and download their malware automatically into the control software of the SCADA. They may interfere with the SCADA system control and communication through a denial of service attack that overwhelms the system with information unrelated to its operation. Without appropriate monitoring, controls and response (such as I will describe shortly), these different avenues of attack would leave the system vulnerable.

As I previously indicated, most cyberattacks originate from cyber criminals interested in stealing information or dollars or "hacktivists" with a political agenda. Attacks on industrial control systems are different; we believe that the majority of these attacks originate from nation-states or from terrorist organizations who intend harm to America's national security. Because of the challenge of assigning attribution to cyberattacks, it is difficult for Xcel Energy to identify the origin of most attacks against our system.

Xcel Energy is Committed to Creating Robust Programs to Help Defend Against Cyberattacks.

The cybersecurity threat is evolving. Fortunately, up to this point, we are not aware of any successful attack on the American electric system, but the risk is clearly growing. In response, we work continuously to implement a flexible, effective cybersecurity program that proactively adapts our cyber defenses to the rapidly evolving threat before an attack occurs.

Like other utilities, we based our cybersecurity program on the "Dynamic Defense in Depth" cybersecurity framework published by the National Institute of Standards and Technology, or NIST. That framework contains several elements:

- Identify. The NIST Cybersecurity Framework first identifies the potential cyber threats and their impact on our business processes. For a utility, this element focuses on the SCADA system and the threats that I previously identified.

- Protect. The NIST framework creates evolving protections for critical infrastructure, including the electric system and especially the SCADA system. For Xcel Energy, our program separates the SCADA system from the rest of our network and from the internet – a separation known as "enclaving." Enclaving places these systems in a tightly controlled and monitored segment of the network, separate from the rest of the company's IT network and the internet. We employ multiple layers of security controls at the perimeters of these enclaves designed to prevent, detect and respond to unauthorized access attempts. We promote good cyber hygiene by promptly and regularly applying appropriate security patches to vulnerable systems, and strictly controlling and monitoring employee access to our critical systems, particularly those within the SCADA system. We have controls in place designed to mitigate the threat of malicious insiders such as banning the use of thumb drives and other removable media, physical access controls and other measures. We also employ two-factor authentication for our SCADA system, requiring passwords and security codes from two different sources before allowing access.

- Detect. Detection is a key component of the NIST framework. Our network is monitored by a dedicated team of cyber analysts on a 24 hour basis. Collecting data from tens of thousands of systems across the network, the team evaluates millions of individual "events" daily in order to identify and respond to unusual or suspicious activity. We receive prompt and actionable threat intelligence daily from government and private sources regarding potential attacks, malware types and methodologies, and we use this intelligence to adjust our defense posture as necessary. Our program uses this information to detect vulnerabilities in our system before the cybercriminal can exploit them. This element is especially important; in most recent high-profile attacks by nation-states, malware sat undetected in the victim's cyber system for months or years before it was exploited. (This type of malware is known as an Advanced Persistent Threat, or

APT, and it allows an actor to gain a foothold in the network for future attacks.) We also employ a vigorous threat detection program that scans the entire network for vulnerabilities or potential changes to our systems that may indicate a compromise.

- Respond. The NIST framework also requires effective response to cyberattacks. Our program isolates and removes detected malware. We maintain up-to-date patching of our system and implement anti-virus, anti-malware programs to address known and unknown threats. However, because there are an increasing number of previously unknown vulnerabilities, referred to as Zero Day Threats, we cannot rely solely on these controls to detect and counter intrusions into our network. We also "hunt" for indications of compromise on regular basis in order to detect and eliminate APTs. Finally, we perform penetration testing of the network by qualified third parties and select government labs and agencies.

- Recover. Unfortunately, despite our best efforts, no program is perfect. Eventually, an attack against our network or even the SCADA system may be successful. The NIST framework recognizes this fact. Accordingly, we maintain highly detailed incident response and recovery plans, both for prompt restoration of system operations and isolation and elimination of the cyber threat. These plans include development of the capability to run the grid without the SCADA system on a short term basis and participation in cyber mutual assurance and other programs in coordination with the ESCC. To test these plans, we join in multiple annual local, state and national level exercises, such as GridEx. I will discuss these programs and exercises in more detail later in this testimony.

  In fact, system recovery is one of our highest priorities. From the beginning, utilities have had to face threats to their system reliability, including storms, fires, and equipment failures. We have decades of experience bringing our system back from unforeseen outages. While the challenges of system restoration would be different after a cyberattack, our experience with system restoration gives us a leg up on our response.

We believe these elements represent some of the best practices in the industry, and we are continuing to look for ways to improve. For example, one of the key components of our program is system redundancy. We create backup systems to ensure that, if one of our systems is compromised, we can recover operations by turning to a redundant system. We also join other electric providers to strengthen our individual electric systems through the broader network itself. We rely on our neighboring utilities and the regions in which we operate (and, in the same way, they rely on us) to provide backup operations in the event of a significant service disruption.

In addition, under the "Detect" element above, we have joined other utilities to receive information and analysis regarding cyber threats from the E-ISAC – the Electricity Information Sharing and Analysis Center. Managed by the North American Electric Reliability Corporation,

or NERC, the E-ISAC serves as the primary security communications channel for the electricity subsector and enhances the subsector's ability to prepare for and respond to cyber threats. While the E-ISAC is an effective and robust information sharing platform, Xcel Energy has recently expanded its information sharing capabilities by joining with the Financial Services ISAC to create a new information sharing community known as the Energy Analytic Security Exchange (or EASE). EASE will take advantage of the state-of-the art capabilities of the FS-ISAC and, together with our membership in the E-ISAC, enhance our ability to identify and respond to threats to the Xcel Energy grid, in particular threats to the SCADA system.

Our collaboration with the FS-ISAC in creating EASE is part of our effort to design a flexible cybersecurity program to meet the evolving nature of the cyber threat. The success of any cybersecurity program, however, depends first on the people who implement it. At Xcel Energy, I have assembled an excellent team of security professionals. I have hired a Chief Security Officer with 30 years of government and industry experience managing cybersecurity threats. He runs a team consisting of 97 employees, most of who are focused on cybersecurity issues. As the cyber threat has increased, the scope of our cybersecurity program has also grown dramatically. Five years ago, Xcel Energy did not have a Chief Security Officer, and its cybersecurity staff was a fraction of what it is today. As with every aspect of our business, we work hard to ensure that our security program is efficient and cost-effective, but make no mistake: cybersecurity is not free, and our customers are paying for the programs we need to protect the grid.[1]

I am proud of our cybersecurity program and the progress that we are making. However, our program is and always will be a work in progress. It is not perfect, and it must continue to grow and change as we learn more about the threat we face.

Technology Advancements Are Enhancing the Defense of the Grid.

Our enemies are constantly deploying new technologies to attack the electric grid, and we must create our own defensive technologies to respond. The good news is that we are beginning to deploy these new technologies to help respond to these threats. Below is a partial list of some of the technological advancements that are helping us to defend our grid:

Information Sharing Tools. As cyberattacks continue to increase in scope, we need better tools to identify the attacks and respond before they can trigger an outage. Information sharing tools must become more sophisticated as attacks become more sophisticated. Fortunately, our arsenal of information sharing tools is continuously improving. The E-ISAC deploys the Cybersecurity Risk Information Sharing Program, or CRISP, to facilitate the exchange of detailed cybersecurity

[1] In order to maintain an effective cyber security program, we are required to invest in expensive, state-of-the-art technologies to keep pace with the constantly evolving threat. The attackers however, can still heavily rely on exploits that are 10-15 years old and are still as effective as when they first came out.

information between the industry, the E-ISAC, DOE, and Pacific Northwest National Laboratory (PNNL). CRISP has potential to be a valuable information sharing tool. Twenty-six utilities in North America leverage CRISP to obtain secure access to information and analysis of cyber threats identified by the nation's intelligence apparatus.

Information sharing will become more effective if it allows machines to communicate directly with each other without human interaction. Low-cost machine-to-machine information sharing tools, including STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Indicator Information) have now become state-of-the-art information sharing technology for the nation. In fact, the experience of the FS-ISAC with these tools was one of the reasons that we created the EASE program under the FS-ISAC. Real time, machine-to-machine information sharing will enhance our ability to respond to grid attacks before they can impact customers.

Operating Technology Improvements. If the SCADA system, which houses the main computer and processing functions, is the like the brain of the utility's central nervous system, the grid and breakers and other field devices are like the branches with which it communicates. These devices actually do the work of operating the grid. The cyber systems that manage and control these devices are known as operating technology, or OT. The OT system can interface with the company network. Unlike the central SCADA system or the company's network IT systems, which are constantly and often automatically updated with service packs, new releases and bug fixes, these OT devices are frequently running the same software they used when initially installed 10 to 15 years ago. Moreover, these devices have virtually no security capabilities because they were installed at a time when a physical separation from the network IT systems was considered to be "secure." Studies show that upwards of 30% of vulnerabilities identified within OT devices have no patches. Nevertheless, there are some technology upgrades that can help enhance OT security. Specifically, upgrades to the monitoring and control capabilities of the OT systems would greatly improve our ability to protect the grid.

For example, as I mentioned previously, APT malware deposited in a network can lie dormant for years until an enemy decides to exploit it. One of the key components of an effective cybersecurity program is the ability to monitor and identify system threats. Today, we are beginning to deploy new "hunt" technology in our network that will look for anomalies and changes on the network that could indicate the presence of malware. Hunt technology will become critical to protecting the system in the future as the pace of cyberattacks increases.

Similarly, improved monitoring capability within the SCADA itself will provide a real-time detection capability of changes to the environment. Some types of malware include features that mask the execution of an attack while it is occurring. With this masking feature, system operators might not be aware that the system is under attack even as the lights turn off across the grid. Improved monitoring technology can help protect against this kind of attack. Because the SCADA environment is static compared to the average IT environment, changes, especially

numerous changes in a short period of time, are very suspicious. Improved monitoring designed specifically for the SCADA environment would identify new device connections and communications that may demonstrate the presence of cybercriminal in the system.

Industry and the Government Have Developed a Strong Program to Coordinate a Response to Cyber Threats.

Defense of the grid is the responsibility of every utility company in America. However, given the nature of the threat and the nation-wide interconnectedness of the grid, it is also a national security priority. For that reason, the electric industry and federal national security agencies must work together to establish effective cybersecurity programs. Although, as I will discuss later, there is always more to do, I am pleased to report that the nation's cybersecurity programs are strong, collaborative and continuing to evolve to meet the cybersecurity threat.

Cybersecurity Regulation and Emergency Orders. First, the utility industry is subject to mandatory cybersecurity regulations. Under the Federal Power Act and Federal Energy Regulatory Commission oversight, the electric power sector is subject to NERC Critical Infrastructure Protection (CIP) Reliability Standards that include cyber and physical security requirements. Entities found in violation of CIP standards face penalties that can exceed $1 million per violation per day.

These mandatory standards continue to evolve with input from subject matter experts across the industry and government. Currently, the electric power sector must comply with Version 6 of the cybersecurity standards, and additional modifications are underway to add new requirements mirroring best practices in cybersecurity.

In addition to implementing Version 6 of the cybersecurity requirements, NERC and the industry are developing new requirements to address supply chain cybersecurity. The industry also is implementing new mandatory requirements for physical security as part of the broader suite of NERC regulatory standards.

The industry also uses voluntary standards, such as the NIST Cybersecurity Framework I mentioned previously, as well as DOE's Cybersecurity Capability Maturity Model. Like Xcel Energy, electric companies throughout the industry assess their cybersecurity programs and capabilities against this framework and use their assessments to strengthen cybersecurity.

In addition to these mandatory and voluntary standards, Congress recently took steps to ensure a single government entity would have emergency authority and ultimate responsibility in the event of a true grid security emergency resulting from a cyberattack or other types of intentional or existential threats to the grid. The 2015 transportation bill ("Fixing America's Surface Transportation Act" or FAST Act) provides that, upon a Presidential determination of a grid security emergency, DOE has authority to issue an order for emergency measures to be taken by

NERC, a regional entity, or electric sector owners and operators. The industry commends Congress for your foresight in addressing this issue, and we are working with DOE to determine the scope and process for such emergency orders. We also appreciate language in the bill providing liability protections for actions taken in compliance with an order, as well as important protections against public disclosure of sensitive critical energy infrastructure information shared with DOE and FERC.

While regulations, standards and orders can provide a solid foundation for strengthening the industry's security posture, they alone are insufficient. In fact, without more, the standards can lead companies to focus solely on compliance without adapting to a mutating threat. As the threats evolve, the nation's security efforts must evolve too. For that reason, industry coordinates cybersecurity policy developments with the ESCC.

The ESCC's Strategic Plan. The ESCC in its current form arose as a result of a NIAC recommendation, and NIAC points to the ESCC as a model for how critical infrastructure sectors can more effectively partner with government. In fact, the ESCC has been a catalyst for major initiatives that are improving the security posture of the industry and, by extension, the nation.

The ESCC is comprised of the chief executive officers of 22 electric companies (including Xcel Energy) and nine major industry trade associations. This group—which includes all segments of the industry, representing the full scope of electric generation, transmission, and distribution in the United States and Canada—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 incidents or threats to critical infrastructure.

A key characteristic of the ESCC is executive engagement. In addition to providing resources and accountability that have pushed both the government and industry to work together very closely, senior executives on both sides also help to ensure unity of effort and unity of message among their organizations. During an incident, the ESCC's role—while not operational—is to provide situational awareness, ensure coordination with government on response and recovery efforts, and align messaging.

The industry and government leaders are focusing on four main areas that improve the security posture of the industry and the nation:

1. Tools & Technology: Deploying government technologies that improve situational awareness and enable machine-to-machine information sharing, such as those technologies discussed previously in my testimony;

2. Information Flow: Making sure actionable intelligence and threat indicators are communicated to the right people at the right time in the right way;

3. Incident Response and Recovery: Planning and exercising to coordinate responses to an incident;

4. Cross-Sector Coordination: Working closely with other interdependent infrastructure sectors (*e.g.*, communications, downstream natural gas, financial services, water) to ensure all are prepared for, and can respond to, national-level incidents. On behalf of the ESCC, I serve as the electric sector's liaison to the financial sector to help coordinate cybersecurity policies and programs between the two sectors.

Cyber Mutual Assistance. The ESCC builds on existing utility and governmental strengths to respond to this new threat. For example, the electric power industry has long had a culture of mutual assistance; when a weather event or natural disaster impacts a region, crews and lineworkers from all over North America descend on the affected region to restore power. As cyber risks proliferate, the industry, with the ESCC's leadership, has moved to develop a cyber mutual assistance program to aid electric companies in restoring necessary computer systems following a regional or national cyber incident. This program builds on the industry's culture of mutual assistance to develop resource-sharing relationships that can provide surge capacity should a cyber incident exceed the capacity for an individual company to respond. Xcel Energy is participating in the cyber mutual assistance program.

Exercises. The ESCC also works with NERC to simulate the effect of a major cyberattack. Electric companies plan and regularly exercise for a variety of emergency situations—including cyberattacks—that could impact their ability to provide electricity. The largest exercise so far, in November 2015, was the third biennial industry-wide grid security and incident response exercise known as GridEx III, which brought together more than 364 organizations and 4,400 participants from industry, government agencies, and partners in Canada and Mexico to participate in a rigorous and comprehensive two-day drill that simulated coordinated cyber and physical attacks on the energy grid. GridEx III was a continuation of industry-government efforts to participate in exercises that strengthen the security and resiliency of the energy grid.

In its GridEx III After-Action Report, NERC found that, since GridEx II in 2013, industry and government responses to a significant cyber/physical attack continued to improve. The report identified a number of recommendations for industry and government to continue to strengthen their coordination, preparation, and response capabilities. As was the case with GridEx I and II, these recommendations provide a road map for how the ESCC and the government should address security issues. GridEx IV is scheduled for November 2017.

Other recent national-level exercises in which the industry has participated include: Clear Path IV, conducted by DOE in April 2016; Cascadia Rising, sponsored by FEMA in 2016; Cyber Guard, a two-week DOD-NSA cyber exercise involving experts from government and the energy, IT, and transportation sectors; and a Treasury Department Joint Financial Services-Electric Sector Cyber Exercise in August 2016 that examined incident response capabilities and interdependencies between the two sectors.

Supplemental Operations Strategies. One example of "lessons learned" from these exercises and the December 2015 cyber incident affecting Ukraine is a renewed focus on supplemental strategies for operating the energy grid under sub-optimal circumstances. As I discussed previously, the automation of the SCADA system can leave the grid more vulnerable to cyberattacks. Whether resorting to manual operations, engaging in planned separations, leveraging secondary and tertiary back-up systems, or operating in other degraded states, the industry is working with grid experts to explore "extraordinary measures" – before the incident occurs – to limit the impact and facilitate system restoration in the event of a loss of the automatic control of the SCADA. At Xcel Energy, we are working in parallel with the ESCC to develop our own supplemental operating strategies.

National Laboratories. In addition to working with the Departments of Energy, Homeland Security and Defense, the ESCC also works closely with the national laboratories on research and development of cybersecurity and physical security programs and technologies. For example, as I discussed previously, PNNL developed the CRISP information sharing program. In 2016, Sandia National Laboratory hosted the ESCC to present an overview of its cyber and physical security research. Oak Ridge National Laboratories has evaluated the industry's spare transformer program. Idaho National Laboratories has researched cyber vulnerabilities in gas-fired electric generating units and, for Xcel Energy in particular, undertook an assessment of our new SCADA system.

Emerging Issues. As our industry changes, the cybersecurity threats that we confront also evolve, and the ESCC and Xcel Energy are working to address them. For example, new distributed energy resources (DER) and behind-the-meter assets offer both promise and risk to the grid. DERs and microgrids can improve the capabilities of the grid to withstand outages caused by cyberattacks to the central grid resources. With the appropriate protections (such as those found in a microgrid on a military base), DERs can protect participating customers and even serve as resources to help bring the grid back on line. However, DERs can create new vulnerabilities; these technologies are not subject to the same reliability mandates and security requirements that electric companies must meet, and we do not have organizational control over most customer controlled DER systems. DERs are often connected to the internet and may provide potential entry points for cybercriminals to access to electric companies' grid control systems. DERs increase access points to the grid, and an increase in access points creates additional risks.

Similarly, the installation of billions of "smart" consumer devices may create additional risk. These devices – televisions, thermostats, computers, even refrigerators – have direct connection to the internet and are proving to be vulnerable. While devices comprising the "Internet of Things" (IoT) typically are not directly connected to energy grid infrastructure in the same way as DER, electric companies still recognize the risks related to cyber attacks that may seek to leverage the IoT in a way that would impact the energy grid and electric reliability.

The industry already has faced instances of distributed denial of service attacks similar to IoT-leveraged incidents in other business sectors last year. However, these attacks have focused on business systems (such as customer service), and electric reliability has not been impacted. Nevertheless, in coordination with ESCC, the E-ISAC and the government share actionable intelligence with the industry, and electric companies routinely examine their internet-facing systems for vulnerabilities to ensure that all systems have adequate protections in place.

Congress and the Administration Should Consider New Approaches to Prepare the Nation for the Growing Cybersecurity Threat.

While the programs that I have described are strong and demonstrate that the nation and the industry are working hard to prepare for the cyber threat, there is more to do. The cyber threat is growing, and our cybersecurity programs must continuously improve to meet the coming challenges. As we say in Minnesota, we have to skate to where the puck is going to be, and we had better skate there quickly.

NIAC Recommendations. In 2016, the National Security Council requested that NIAC prepare a scoping study of the nation's cybersecurity programs and preparedness and make recommendations regarding aspects of cyber risk that should be addressed to greatly improve cybersecurity and resilience of our nation's critical infrastructure, NIAC completed that scoping study earlier this year. A copy of the presentation outlining the recommendations of the scoping study is attached to my testimony as Exhibit A.

The NIAC scoping study points to a fundamental problem with the current national approach to cybersecurity policy: I believe that, despite the progress of the last five years, cybersecurity policy at the federal level is often uncoordinated and unfocused. DOE, DHS, DOD and other federal agencies have overlapping authorities and programs. Within Congress, eleven different committees have jurisdiction over cybersecurity issues. Although the federal laboratories are helping to advance our understanding of cybersecurity technology issues, they are pursuing individual research on multiple cybersecurity issues without the benefit of a clear, common national research agenda. Even within industry, despite some progress in cross-sector collaboration, the different critical infrastructure sectors do not coordinate as well as they should.

As a result, the NIAC scoping study has recommended that the nation adopt a transformative national framework for cybersecurity for critical infrastructure. That framework should seek to focus a single national cybersecurity strategy in the same way that a single agency or company would create a single strategy to protect itself. In other words, the framework would establish a cybersecurity program for "USA Inc." The framework would create a flexible and responsive approach to cybersecurity, evaluate the appropriate cybersecurity structures and authorities, and integrate both public and private sectors to provide an effective national cyber defense. To accomplish this goal, NIAC has developed a recommendation to the President to launch an effort

to define the scope of this new framework and identify next steps in implementing NIAC's vision.

Although I am a member of the NIAC, I am not speaking today on behalf of the Council. Nevertheless, I believe that the recommendations of the NIAC scoping study are urgently needed. They would expand on the work already underway and build the successes already achieved to establish a more robust, cross-sectorial approach to cybersecurity. I hope that the President will give these recommendations his full consideration, especially as he continues to develop his cybersecurity executive order.

Cybersecurity Legislation. S. 79, is legislation recently introduced by Senators King, Risch, Heinrich and others regarding cybersecurity and the grid. This bill would establish a pilot program between the energy sector and the national laboratories to look at security vulnerabilities, with a particular emphasis on industrial control systems. This work would be guided in part by a public-private working group made up of relevant federal agencies, the national laboratories and the energy industry. Importantly, the bill is clear that participation in this pilot program on the part of utilities would be purely voluntary. The bill includes liability protections for participants and protects sensitive information from disclosure. The Edison Electric Institute, the association that represents all investor-owned utilities in the nation (including Xcel Energy), does not object to the bill. As my testimony demonstrates, close partnerships with the private sector, such as those envisioned under this bill, would yield benefits to the industry as we work to protect the grid.

Information Sharing. As my testimony makes clear, timely sharing of information is critical to the effectiveness of a cybersecurity program. In that regard, I appreciate this committee's role in enacting the Federal Cybersecurity Information Sharing Act in 2015. That law helped promote information sharing necessary to protect the grid. However, information sharing is only as good as the process by which the government provides information to the private sector. Based on our experience, federal agencies are slow to provide classified information to utilities through the ISACs or other channels. While protection of the nation's secrets is vital, a better process could ensure that we have the necessary information in a timely fashion.[2]

Operations Technology. Finally, as I discussed previously, one of the most significant threats to our industry arises from vulnerabilities to the OT that runs control systems and devices. Research into improved OT safeguards (such as hunt capabilities, monitoring, and encryption) would reduce OT vulnerabilities.

[2] To receive classified information from the government, we must have employees with appropriate security clearances. Unfortunately, the Department of Homeland Security has a significant backlog of pending requests for security clearance. DHS could improve information sharing by reducing this backlog and authorizing appropriate utility employees to receive classified information regarding cyber threats.

FERC is attempting to address these OT vulnerabilities by creating a new CIP standard for the utility sector supply chain. In the utility industry, we are concerned that this new standard would put us in the position of policing the cybersecurity programs for our vendors, which would likely be expensive and unsuccessful. A better approach would be to work with the national laboratories to establish appropriate standards for OT cybersecurity for grid-connected devices, including standards for password protection, communication and other aspects of operations. These standards would become important as we see more and more distributed devices interconnect to the grid.

Thank you again for the opportunity to be with you today. I would be happy to answer any questions.

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL (NIAC)

Work Stream #2

CYBER SCOPING STUDY WORKING GROUP

FEBRUARY 16, 2017

- **Mike Wallace,** Former Vice Chairman and COO, Constellation Energy, **Co-Chair**
  Joan McDonald, Principal, JMM Strategic Solutions, **Co-Chair**
  Jan Allman, President, CEO, and General Manager, Marinette Marine Corporation
- **Robert Carr**, Founder and Former Chief Executive Officer, Heartland Payment Systems
- **Ben Fowke,** Chairman and CEO, Xcel Energy
- **Constance Lau,** President and Chief Executive Officer, Hawaiian Electric Industries, Inc.
- **Keith Parker,** General Manager and CEO, Metropolitan Atlanta Rapid Transit Authority
  Beverly Scott, Ph.D., CEO, Beverly Scott Associates, LLC

- *Work Stream #2*

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

- Advises the President of the United States on how to ensure the security and resilience of the Nation's 16 critical infrastructures.*
- Comprises 28 CEOs and senior experts from private companies and state and local government who own, operate, and advise on critical infrastructure.
- Charged with strengthening public-private partnerships that can improve security and resilience among the critical infrastructure sectors.
- Issued 270 recommendations in 27 studies since 2001 that have helped to reduce physical and cyber risks to the Nation's infrastructures.

* *Includes energy, transportation, water, communications, banking and finance, chemicals, critical manufacturing, defense industrial base, information technology, nuclear reactors, commercial facilities, dams, healthcare and public health, emergency services, food and agriculture, and government facilities.*

AGENDA

- Executive Summary
- The Cyber Challenge
- Who We Talked to
- What We Found
- How to Proceed
- Special Request to the Council

EXECUTIVE SUMMARY

- Council was tasked to scope a study on cyber risks in critical infrastructure.
- After interviews with senior leaders, classified briefings, and in-depth analysis of recent cyber studies, the Working Group concludes:
  - **Cyber risks to critical infrastructure are severe and urgent action is needed.**
  - **The path we are on will not get us to where we need to be.**
  - **The Nation needs a radically new approach for securing public and private cyber systems.**
  - **NIAC is the most appropriate body to build a new public-private model for achieving national cybersecurity, including a plan for rapid implementation, and present it to the President for approval.**
- We recommend that the Council **request that the President direct NIAC to develop a broad and compelling public-private approach to secure the nation's critical cyber assets.**

KEY SCOPING QUESTIONS

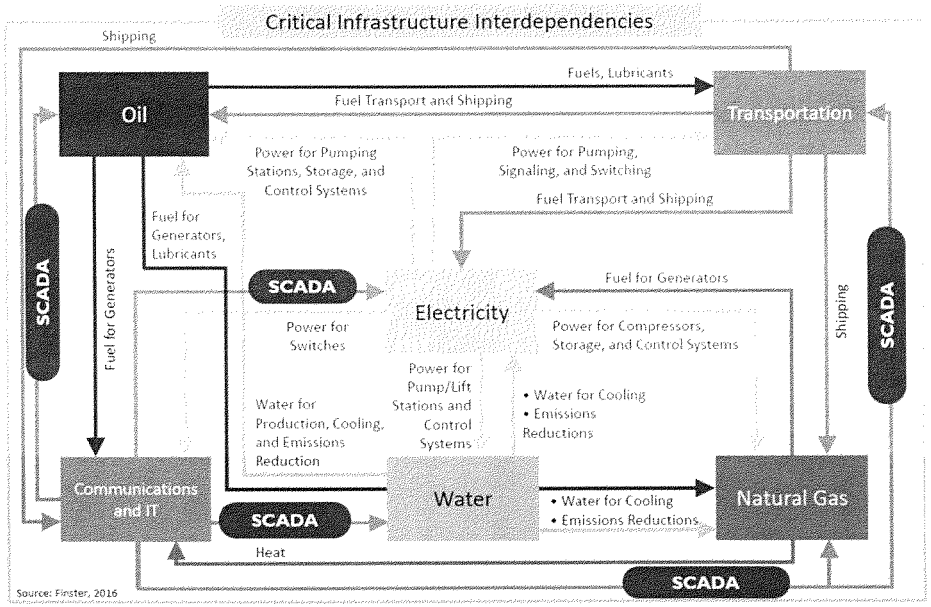
1. What are the most **serious cyber risks** to critical infrastructure?
2. What are the **biggest challenges to reducing these risks**?
3. What are the **roles and responsibilities of the public and private sector** for mitigating cyber risks?
4. What **efforts currently underway** will help reduce cyber risks to critical infrastructure?
5. What are the **gaps in critical infrastructure cybersecurity** that are not being sufficiently addressed?
6. Where can the **NIAC provide the greatest value and leverage** to reduce CI cyber risks for the country?

CYBER RISKS IN CRITICAL INFRASTRUCTURE*

- Cyber risks in critical infrastructure are two-fold:
  - Information and communications technology (**IT**)
  - Operational technologies (including industrial control systems and SCADA systems) (**OT**)
- Cyber attacks on industrial control systems are very serious because they can disrupt vital services, damage critical equipment, threaten human health and safety, and trigger disruptions in other sectors.
- DHS reported 290 cyber attacks on critical infrastructure control systems in 2016. (ICS-CERT)
- DOE concludes that *"the U.S. grid faces imminent danger from cyber attacks, absent a discrete set of actions and clear authorities to inform both responses and threats."*
- Theft of personally identifiable information (PII) and company data is on the rise. Financial institutions experience 300% more cyber attacks than other sectors.
- Internet of Things (IoT) devices, many without strong security, expected to double from 15.4 billion in 2015 to 30.7 billion by 2020.

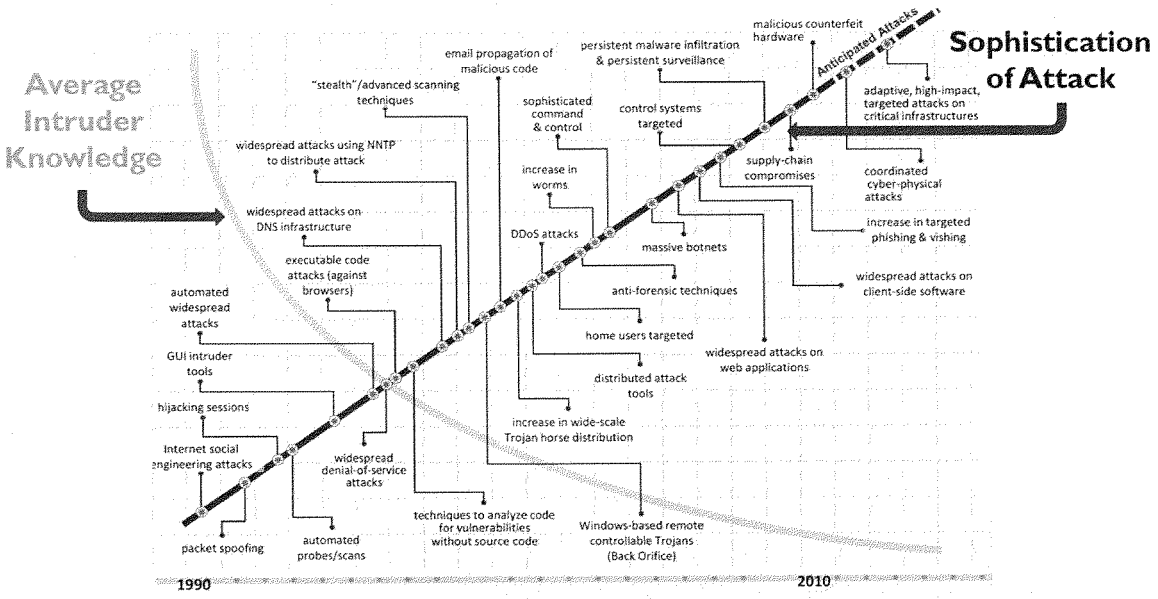
** Most cyber breaches go undetected or unreported; data on cyber attacks, cyber crime, and cybersecurity are very limited.*

INTERDEPENDENCIES COMPOUND CYBER RISKS



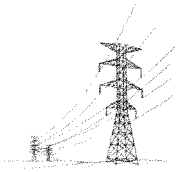
Source: DOE Quadrennial Energy Review 2017

CYBER ATTACKS: MORE SOPHISTICATED, EASIER TO LAUNCH



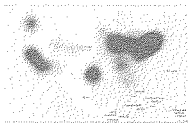
Source: Software Engineering Institute, Carnegie Mellon University

CYBER ATTACKS ON CRITICAL INFRASTRUCTURE



Ukraine Power Grid
December 2015
Electricity Sector

- 225,000 customers lost power
- Military-like planning and execution
- Utilities infiltrated 9 months prior to attack
- Launched with easily available attacks tools



Dyn Attack
October 2016
Multiple Sectors

- Massive botnet DDOS attack involving tens of millions of IP addresses disrupted web traffic
- Compromised ~100,000 insecure IoT devices (webcams, baby monitors, DVRs)
- Caused $110 million in lost revenue and sales

JPMORGAN CHASE & CO.

JPMorgan Chase
July 2014
Banking and Finance Sector

- One of the largest data thefts in history
- Compromised data of 83 million accounts
- Cost of breach likely >$1 billion

Shamoon Attacks
January 2017, 2016, 2012
Oil and Natural Gas Sector

- 2017: Weaponized malware hit 15 state bodies and private companies in Saudi Arabia
- 2012: Wiped out 35,000 hard drives of Saudi Aramco causing >$500 million in losses
- Iranian-backed hackers suspected

COST OF CYBER CRIME AND CYBERSECURITY

$500 billion – Global annual business cost of cyber attacks *(Fortune 2015).*

$6 trillion – Projected annual cost of cybercrime in 2021 *(Cybersecurity Ventures 2016).*

$17 million – Estimated average annual cost of cyber crime for U.S. companies in 2016 *(Ponemon 2016).*

$500 million – Annual spending by one U.S. bank to fight cyber crime *(Forbes 2015).*

$1 trillion – Projected cumulative worldwide spending on cybersecurity from 2017 to 2021 *(Cybersecurity Ventures 2016).*

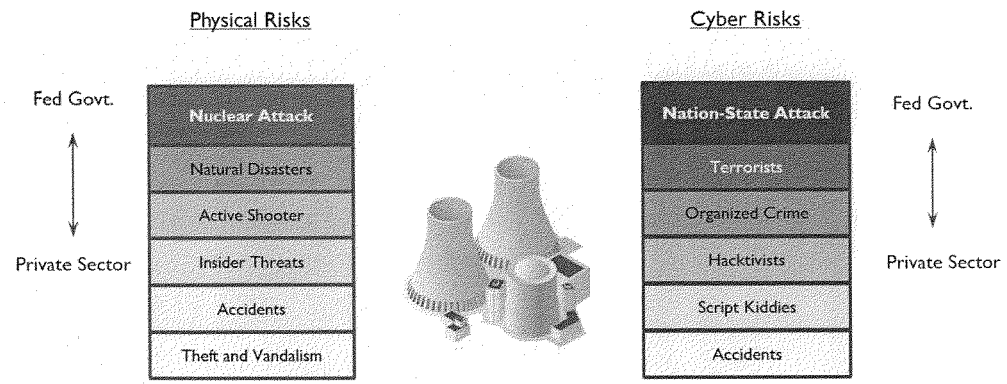
$217 – Estimated cost per record of data breach in the U.S. *(Ponemon 2016).*

$19 billion – Projected FY 2017 spending on cybersecurity by the U.S.

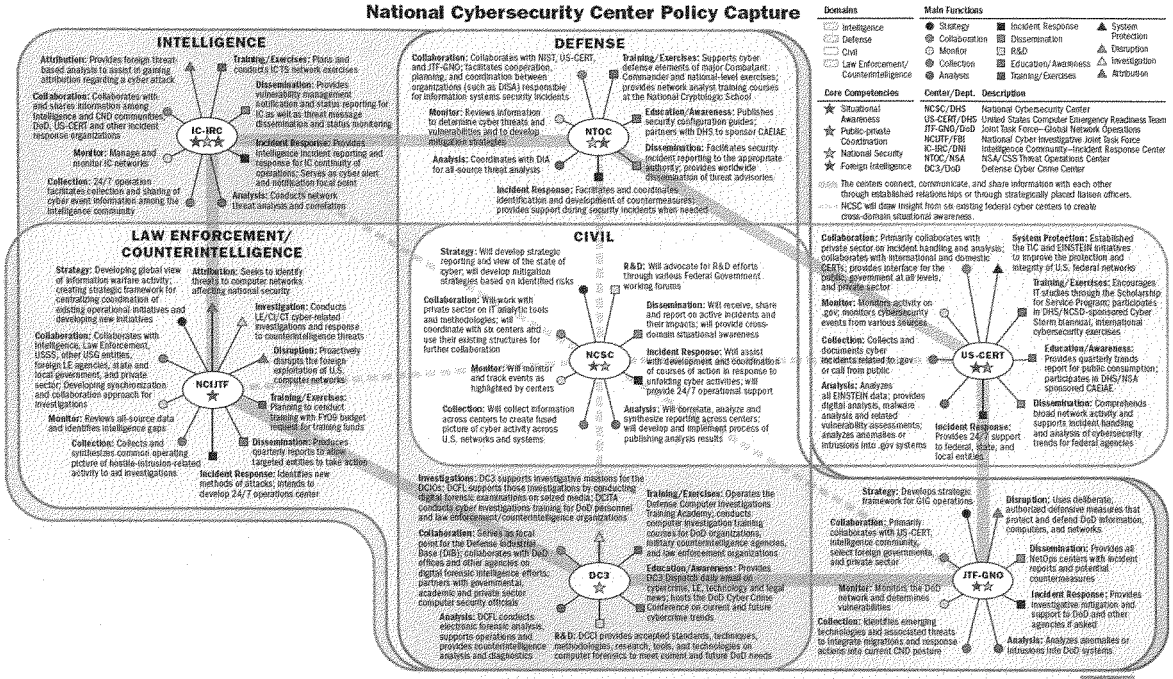
government *(White House 2016)*.

DEFINING PUBLIC AND PRIVATE SECTOR ROLES

Security Roles and Responsibilities for Physical and Cyber Risks



"UNTANGLING" FEDERAL CYBERSECURITY RESPONSIBILITIES (2009)



Source: https://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf, accessed December 2016 (now removed)

CYBER CHALLENGE: KEY TAKEAWAYS

- Cyber risks to critical infrastructure are extensive and urgent
- Attackers have the advantage and their capabilities increasingly outpace our defenses.
- There is no clear national strategy or accountability that indicates who is responsible to defend the collective entities in the Nation against cyber attacks
- Both public and private capabilities and resources are needed to reduce cyber risks to critical infrastructure
- Quick, bold, and decisive action is needed that builds on a foundation of strong public-private partnership

INTERVIEWS

National Security Council Staff

- **Stephanie Morrison**, Director, Critical Infrastructure Policy
- **Monica Maher**, Director, Cybersecurity
- **Asha Tribble**, former NSC Staff
- **Darrell Darnell**, former NSC staff

Intelligence Community

- **Richard Ledgett**, Deputy Director, NSA
- **Glenn Gerstell**, General Counsel, NSA; former NIAC member
- **Lt. Gen Kevin McLaughlin**, Deputy Commander, US Cyber Command
- **Gen. Keith Alexander (ret.),** former Director, NSA; former Commander, US Cyber Command
- **Richard Danzig**, Chairman, Center for a New American Security; Senior Fellow, Johns Hopkins Applied Physics Lab; former Secretary of the Navy

INTERVIEWS

Critical Infrastructure Community

- **Tom Fanning,** Chairman and CEO, Southern Company; Chair, Electricity SCC
- **Alfred Berkeley,** former President and Vice-Chairman, NASDAQ; former NIAC member
- **Scott Aaronson**, Executive Director, Security and Business Continuity, Edison Electric Institute
- **Bill Nelson**, President and CEO, Financial Services Information Sharing and Analysis Center

Government Leaders in Critical Infrastructure

- **Caitlin Durkovich**, Assistant Secretary, Infrastructure Protection, DHS
- **Pat Hoffman**, Assistant Secretary, Electricity Delivery and Energy Reliability, DOE
- **Paul Stockton**, Managing Director, Sonecon; Senior Fellow, Johns Hopkins Applied Physics Lab; former Assistant Secretary for Homeland Defense, DOD
- **Col. Bob Stephan** (Ret.), USAF, former Assistant Secretary, Infrastructure Protection, DHS
- **Jim Caverly,** former Director, Partnership and Outreach Division, DHS
- **Brian Peretti**, Financial Services Critical Infrastructure Program Manager, US Treasury
- **Eric Goldstein**, Senior Counselor to the Under Secretary of the National Protection and Programs Directorate (NPPD), DHS
- **Richard Moore**, Associate Director for Security Policy and Plans, DOT; former Branch Chief, DHS Office of Cyber and Infrastructure Analysis

BRIEFINGS AND PANEL DISCUSSIONS

- National Security Agency (NSA) [classified]
- NSA and US Cyber Command [classified and unclassified]
- Office of the Director of National Intelligence (ODNI) [classified]
- Cybersecurity Emergency Response Team (US-CERT) [classified]
- Mike Assante, SANS Institute – Ukrainian Cyber Attack [unclassified]
- Financial Sector Coordinating Council [unclassified]
- Draper Laboratory [unclassified]
- Federal Bureau of Investigation (FBI) [unclassified]

SELECTED CYBER STUDIES AND STRATEGIES

- Commission on Enhancing National Cybersecurity. ***Report on Securing and Growing the Digital Economy***, 2016.
- Bipartisan Policy Center. ***Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat,*** 2014.
- ***Roadmaps to Secure Control Systems*** (Energy, Chemical, Water, Dams, Transportation), 2006-2011.
- National Institute of Standards and Technology. ***Framework for Improving Critical Infrastructure Cybersecurity,*** 2014.
- U.S. Department of Homeland Security. ***Strategic Principles for Securing the Internet of Things, (IoT),*** 2016.
- U.S. Department of Homeland Security. ***The National Cyber Incident Response Plan*** (Review Draft), 2016.
- U.S. Department of Defense. ***The DOD Cyber Strategy***, 2015.
- Defense Science Board. ***Resilient Military Systems and the Advanced Cyber Threat***, 2013.
- UK Government Communications Headquarters. ***National Cyber Security Strategy 2016-2021***, 2016.
- Homeland Security Advisory Council, Cybersecurity Subcommittee. ***Final Report, Part I – Incident Response***, 2016.
- The President's Review Group on Intelligence and Communications Technologies. ***Liberty and Security in a Changing World, Report and Recommendations***, 2013.
- The White House. ***Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure***, 2009.
- The White House. ***Federal Cybersecurity Research and Development Strategic Plan***, 2016.
- The White House. ***Federal Cybersecurity Workforce Strategy***, 2016.

FINDINGS

1. **Our ability to defend private sector cyber networks is not keeping up with the threat.**
   - Critical infrastructure owners and operators are not doing enough to protect their cyber systems from risks.
   - Industrial control systems (ICS) connected to business IT systems and the internet constitute a *systemic cyber risk* among critical infrastructures.
2. **Cybersecurity of critical infrastructure is a shared responsibility that needs effective public-private partnership to drive joint action.**
   - Federal and private sector resources are not organized effectively to help the private sector secure their critical cyber systems.
   - Information sharing has improved, but still has persistent flaws.
3. **Government efforts over the past 30 years have fallen short in reducing cyber risks in critical infrastructure sectors.**
   - Multiple entities are responsible for various aspects of cybersecurity but the country lacks an integrated, focused approach to defend the Nation.
   - Cyber legislation, regulations, and executive actions are inadequate for motivating private action to improve cybersecurity.
   - Alternative national models for cybersecurity offer promising new approaches.

Finding 1: Our Ability to Defend Private Sector Cyber Networks Is Not Keeping Up with the Threat.

In today's world, attackers have the advantage. The right adversary with the right capabilities and intent can breach just about any system. Rather than react to the latest threat, we must anticipate future trendlines and design systems to defeat them.

A. **Critical infrastructure owners and operators are not doing enough to protect their cyber systems from risks.**

Many companies are not practicing basic cyber hygiene despite the availability of effective tools and practices. Managers often do not fully understand the magnitude or complexity of the risks they face. There is also little incentive to improve cybersecurity in competitive environments.

B. **Industrial control systems (ICS) connected to business IT systems and the internet constitute a *systemic cyber risk* among critical infrastructures.**

Automated, cyber-based control systems improve productivity but also introduce new cyber risks. Interconnected cyber systems within supply chains and across infrastructures means that an ICS cyber breach can cascade to connected systems and cause physical damage and threaten human health and safety. Securing these systems should be a national priority.

Finding 2: Cybersecurity of Critical Infrastructure Is a Shared Responsibility that Needs Effective Public-Private Partnership to Drive Joint Action.

Growing dependence by government, businesses, and communities on critical services means that an attack on critical infrastructure is an attack on civil society. Defense against well-resourced adversaries requires the collective resources of the public and private sectors. This is a national risk management problem that must be addressed at the highest executive levels.

A. **Federal and private sector resources are not organized effectively to help the private sector secure their critical cyber systems.**

Gaps and overlaps in the cybersecurity authorities, missions, roles, and responsibilities of government departments and agencies is inefficient and precarious; a bold new approach is needed. The public and private sectors must compete for a limited pool of highly trained cyber experts, creating a shortage of cybersecurity leadership and expertise.

B. **Information sharing has improved, but still has persistent flaws.**

Intelligence information now being shared with the private sector is not well organized. Successful information sharing requires bi-directional flows that allow for machine-to-machine mitigations. Yet companies are reluctant to use automated services that provide immediate response to cyber attacks due to a lack of trust in government information protection.

Finding 3: Government Efforts Over the Past 30 Years Have Fallen Short in Reducing Cyber Risks in Critical Infrastructure Sectors.

Progress in cybersecurity technologies and policies have not kept pace with rising cyber risks. We have created a patchwork of legislation, policies, and approaches, but lack a cohesive national strategy.

A. **Multiple entities are responsible for various aspects of cybersecurity but the country lacks an integrated, focused approach to defend the Nation.**

- We lack a cohesive framework for cyber defense and our response to a large-scale physical-cyber attack on critical infrastructures today is likely to be inefficient.

B. **Cyber Legislation, Regulations, and Executive Actions Are Inadequate for Motivating Private Action to Improve Cybersecurity.**

- Legislation and policy directives are often blunt tools for cybersecurity. Their slow development lags rapidly changing cyber risks. Unintended consequences can also impede beneficial security efforts. Market-driven approaches with appropriate incentives provides a faster and more flexible way to drive private sector security actions.

C. **Alternative national models for cybersecurity offer promising new approaches.**

- The governments of Israel, UK, and others use novel approaches to mitigate private sector cyber risks. However, their viability within the United States must take into account the large scale and digital footprint of U.S. infrastructure.

THREE URGENT CYBER PRIORITIES

1. **Triage Today's Problems**
   - Implement immediate and urgent fixes to address the most serious cyber risks to critical infrastructure. Focus on the sectors and set of assets that, if compromised, would result in major economic, safety, and security consequences to the U.S.
   - Improve cyber hygiene across all critical infrastructures and consider some form of compliance.
   - Improve information sharing mechanisms, leading to machine-to-machine exchanges
2. **Develop Novel Approaches for Cyber Resilience**
   - Design next-generation cyber systems that are inherently secure, resilient, and self-healing, particularly those that control critical functions. Develop solutions that make it extremely difficult and economically unattractive to extract value.
3. **Strengthen Public-Private Partnership and Leadership**
   1. Develop effective executive-level, public-private mechanisms to strengthen leadership and efficient decisionmaking concerning critical cyber incidents and policy actions.
   2. Streamline, reconfigure, and clarify roles and responsibilities within the federal government

HOW TO PROCEED

- **The path we are on will not get us to where we need to be.** A bold, new, integrated and comprehensive approach is needed to direct the country's cybersecurity needs based on a new model and level of public-private partnership.
- NIAC—the President's cross-sector, senior executive advisors on critical infrastructure—should undertake the development of the framework, structure, authorities, and public and private roles needed to build a new public-private approach to cybersecurity for critical infrastructure.
- Our approach to national cybersecurity must:
  1. Be significantly more impactful and robust, with very specific recommendations for the President for new structures, authorities, roles, responsibilities, staffing, and resource commitments.
  2. Engage senior leaders and key stakeholders to solicit the best ideas.
  3. Address immediate needs and anticipate future needs.
- The Council should ***accelerate*** the launch of the cyber study with a letter to the President.

CYBER STUDY DESIGN

Phase 1: Frame out the proposed public-private model for achieving national cybersecurity.

- Build on the tremendous foundation of previous councils and commissions.
- Propose a new strawman structure, framework, and approach for cybersecurity.

Phase 2: Solicit input from the nation's top leaders and experts to strengthen the model.

- Conduct a series of engagements with the best and brightest experts to develop the features, characteristics, authorities, structure, staffing, governance, leadership, priorities, and resource requirements for this new model.
- Challenge the model, shape it, and improve it.

Phase 3: Refine and recommend a comprehensive national cybersecurity model and execution plan to the POTUS.

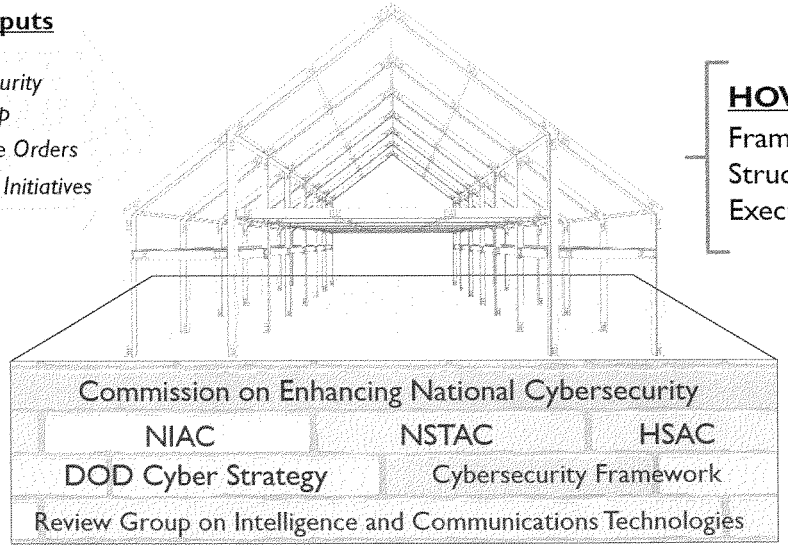
- Recommend a comprehensive approach to direct actions that will provide the speed, focus, and effectiveness to leverage a public-private partnership for the security of the nation's cyber assets, and the critical components these assets control.

NIAC WILL BUILD ON RECENT CYBER STRATEGIES

Proposed NIAC Cyber Study

Dynamic Inputs

- *WH Cybersecurity Advisory Group*
- *New Executive Orders*
- *Congressional Initiatives*



HOW
Framework, Structure, & Execution Plan

WHAT
Cyber Challenges & Solutions

SPECIAL REQUEST TO THE COUNCIL

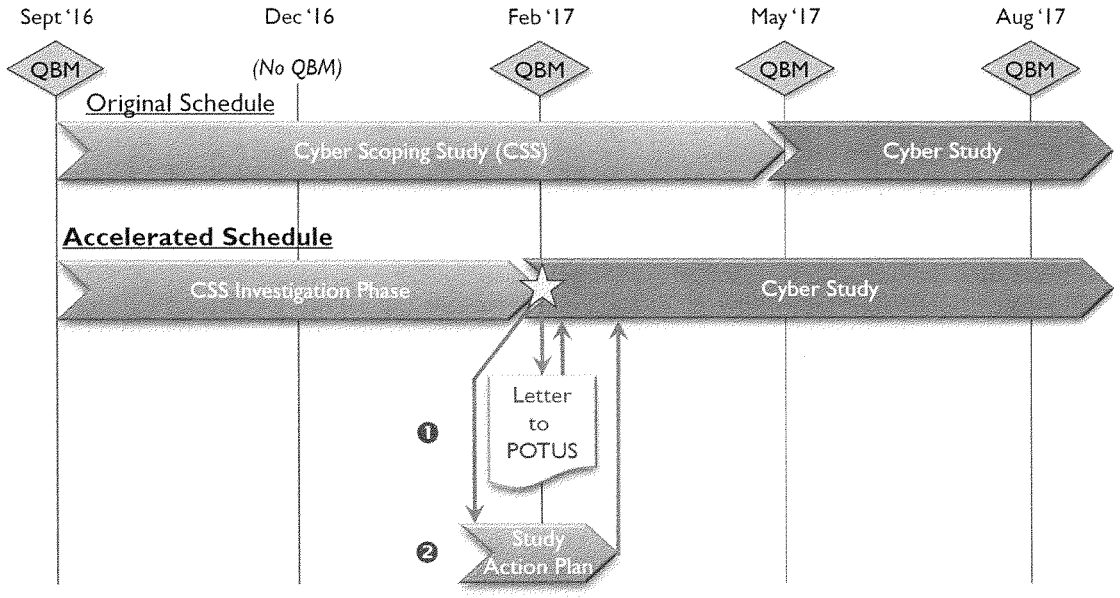
1. Prepare a letter to the President recommending that he direct the Council to immediately begin working with stakeholders on the "new Cyber Study" to develop the framework, structure, public and private roles, and authorities needed to build a new public-private approach to cybersecurity for critical infrastructure that is significantly more impactful and robust.

2. Approve the Working Group's recommendation to end the investigative portion of Cyber Scoping Study and begin work at once to prepare a detailed action plan for the "new Cyber Study" to allow rapid startup once approval is received.

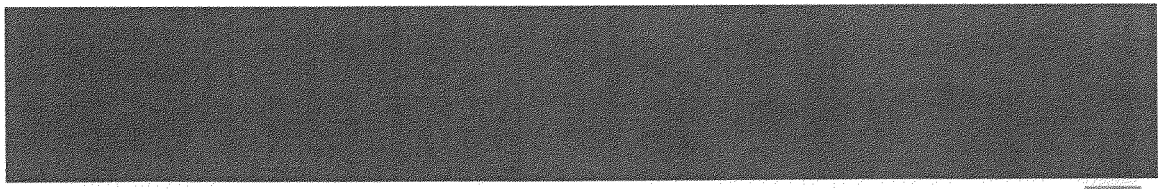
3. Request that the Administration increase staff funding and resources commensurate with the scope, timing, and importance of the cyber study.

How to Proceed

CYBER SCOPING STUDY PROCESS

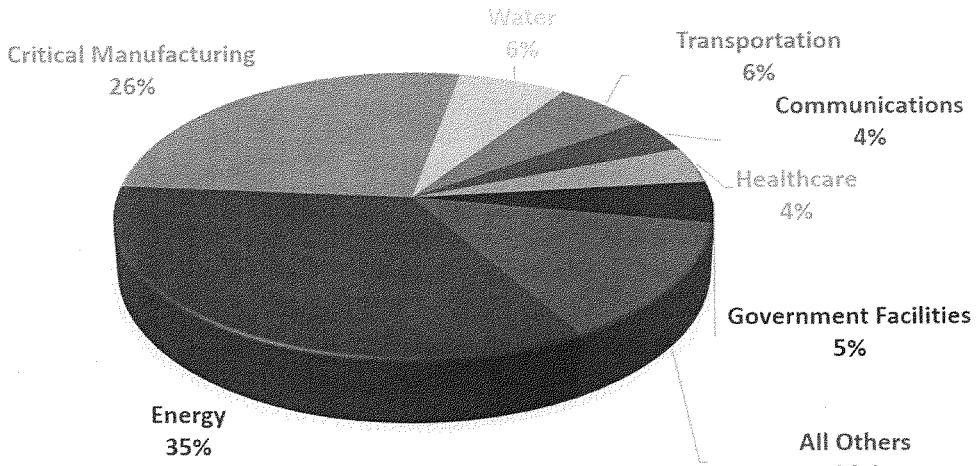


APPENDIX



CYBER ATTACKS ON CRITICAL INFRASTRUCTURE

Cyber Incidents Against Critical Infrastructures Reported to ICS-CERT (2013-2015)*

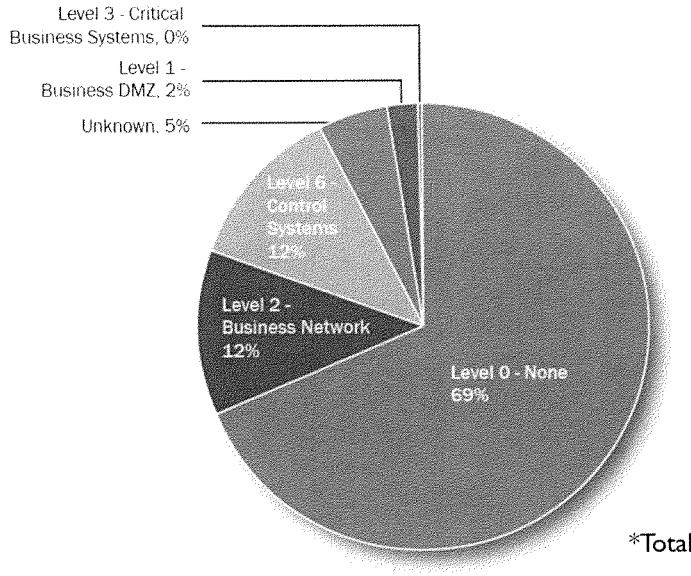


*Total incidents: 796

Source: ICS-CERT Monitors

DEPTH OF CYBER INTRUSION

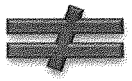
Observed Depth of Intrusion into Critical Infrastructure (FY 2015)*



*Total incidents: 295

Source: ICS-CERT

CYBERSECURITY CONSIDERATIONS IN CRITICAL INFRASTRUCTURES (OT vs. IT)

Operational Technology (OT) / Industrial Control Systems (ICS)  ***Business IT Systems***

- Compromise of OT can disable operations, disrupt critical services to customers, and damage highly specialized equipment.
- OT must be able to survive a cyber incident while sustaining critical functions. Real-time operations are imperative; latency is unacceptable.
- Many OT systems must operate 24/7 with high reliability and availability; no down time for patching/upgrades.
- Some OT components do not have enough computing resources to support additional cybersecurity capabilities.
- OT components may be widely dispersed and located in publicly accessible areas where they are subject to physical tampering.
- OT order of priorities: Availability, Integrity, Confidentiality (AIC); IT order of priorities: Confidentiality, Integrity, Availability (CIA)

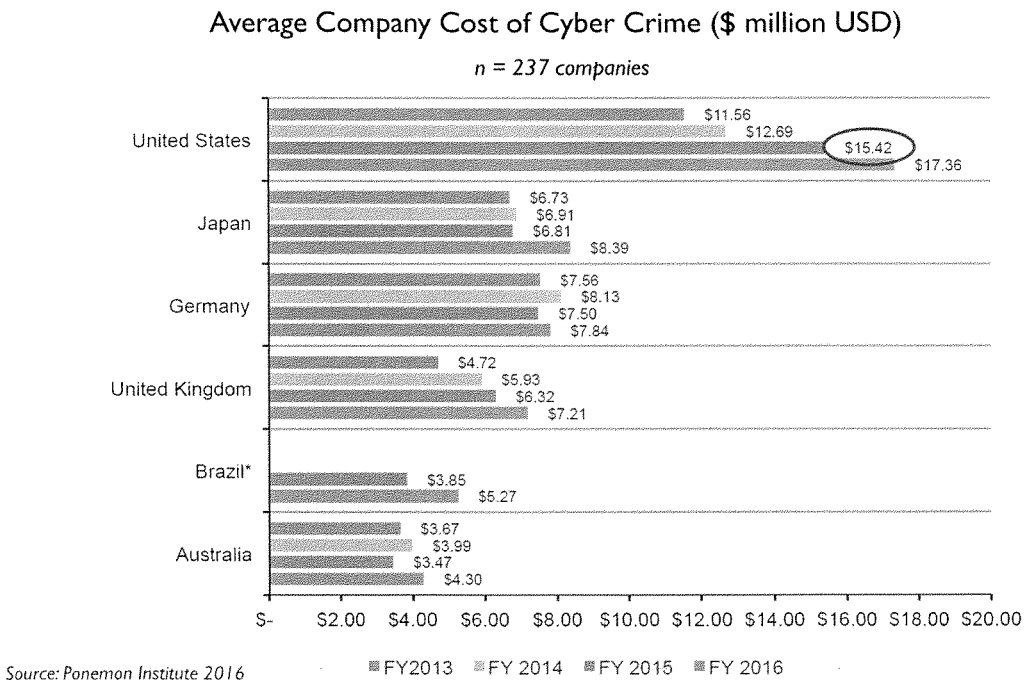
RECENT BREACHES INVOLVING PRIVACY, PII, IP

Incident	Date	Sector(s) Affected	US / Foreign	Likely Source/Attacker	Privacy/PII Impacts
SWIFT attacks	February 2016	**Financial Services**	Foreign	Criminal Hackers, Insiders involved	Attempt to transfer $951M from transferred; other banks hit
OPM Hacks	April & May	**Government Facilities**	US	Nation-State: China	Many different kinds of PII stolen: security clearance information, personal information, finger prints of all Federal employees
Home Depot Breach	September 2014	**Financial Services**	US	Criminal Hackers via 3rd party vendor	56 million credit and debit cards in the U.S. and Canada compromised.
Alcoa spear phishing	May 2014	**Critical Manufacturing**	US	Nation-State: China	PII from company executives potentially exposed. Stolen intellectual property beneficial to
Target Breach	March 2014	**Financial Services**	US	Criminal Hackers via 3rd party vendor	70 million accounts including PII debit cards compromised

RECENT BREACHES INVOLVING ICS, IOT

Incident	Date	Sector(s) Affected	US / Foreign	Likely Source/Attacker	Critical infrastructure impacts
Dyn attack	October 2016	**Communications Financial Services, IT**	US	Hacktivist/unknown	Major Communications and Financial Services company sites (Comcast, Verizon, PayPal, Visa) and services down or slow. Millions of IoT devices
Ukraine / BlackEnergy	December 2015	**Energy**	Foreign	Nation-State: Russia	SCADA vulnerabilities revealed, substations had to be manually controlled. Many US substations don't have manual backup systems.
German steel mill	January 2015	**Critical Manufacturing**	Foreign	Probable Nation State/unknown	"Massive" physical damage to critical be shut down
National Inventory of Dams	May 2013	**Dams**	US	Chinese origin, possible Nation-State	Sensitive information on 79,000 dams included
Saudi Aramco / Shamoon	August 2012	**Energy**	Foreign	Nation-State: Iran	Internal business operations severely disrupted for days; oil production proceeded with no impact to ICS systems due to quick action by the company
U.S. Pipelines	March 2012	**Energy**	US	APT (nation state), possibly China	6-month campaign breached 20+ companies and exfiltrated data on the ICS/SCADA environment
Stuxnet	July 2010	**Energy**	Foreign	Nation-State: U.S./Israel (not confirmed)	Severe damage to centrifuge equipment that were operated well out of safe bounds

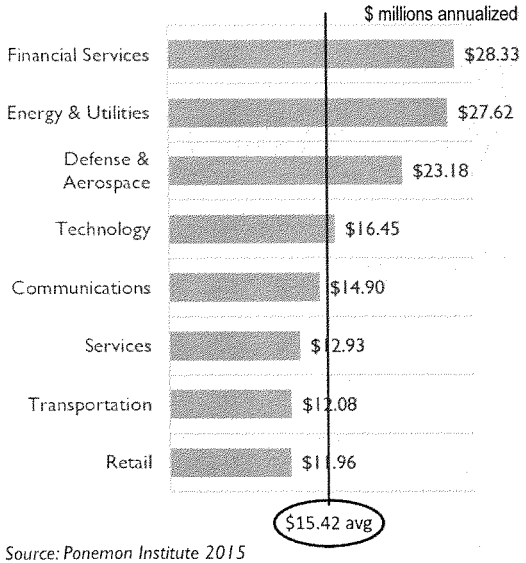
ESTIMATED COST OF CYBER CRIME



Source: Ponemon Institute 2016

THE COST OF CYBERSECURITY

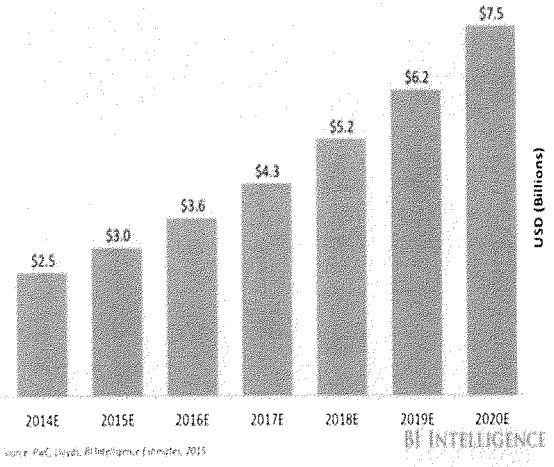
Average US Company Cost of Cyber Crime by Industry Sector in 2015



Source: Ponemon Institute 2015

Estimated Annual Cyber Insurance Premiums Written

Global



OVERVIEW OF FEDERAL EFFORTS

1. Federal Coordination Plans and Strategies
2. Federal Cyber Commissions and Councils
3. Government Cyber Coordination Groups
4. Cyber Legislation, Regulations, Executive Actions, and Policies

FEDERAL COORDINATION PLANS AND STRATEGIES

1. Cybersecurity National Action Plan (2016)
2. Federal Cybersecurity Research and Development Strategic Plan (2016)
3. Federal Cybersecurity Workforce Strategy (2016)
4. DOD Cyber Strategy (2015)
5. The National Cyber Incident Response Plan (2016)

FEDERAL CYBER COMMISSIONS AND COUNCILS

1. Commission on Enhancing National Cybersecurity (CENC), *Report on Securing and Growing the Digital Economy, December 2016*
2. White House, *Joint United States-Canada Electric Grid Security and Resilience Strategy, December 2016*
3. Homeland Security Advisory Council, Cybersecurity Subcommittee, *Report on Incident Response, June 2016*
4. National Security Telecommunications Advisory Committee (NSTAC), *Report on the Internet of Things, November 2014*
5. The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World, December 2013*

➢ *New White House Cybersecurity Advisory Group (2017)*

COMMISSION ON ENHANCING NATIONAL CYBERSECURITY (CENC) – BACKGROUND

- Created by Executive Order 13718 on February 9, 2016
- 12 Commissioners from industry, academia, and former government
- Supported by 6 full-time staff and $5.5 million.
- Charge:
  - Make detailed recommendations to strengthen cybersecurity in both the public and private sectors . . . and bolster partnerships between Federal, State, and local government and the private sector
  - Support the development, promotion, and use of cybersecurity technologies, policies, and best practices
  - Address actions that can be taken over the next decade
- Critical Infrastructure – one of eight topics studied, *and was the most cited topic for Commission consideration in public responses (50% respondents were companies)*
- 6 Imperatives, 16 Recommendations, 52 Actions

CENC: IMPERATIVES

1. Protect, defend, and secure today's information infrastructure and digital networks.
2. Innovate and accelerate investment for the security and growth of digital networks and the digital economy.
3. Prepare consumers to thrive in a digital age.
4. Build cybersecurity workforce capabilities.
5. Better equip government to function effectively and securely in the digital age.
6. Ensure an open, fair, competitive, and secure global digital economy.

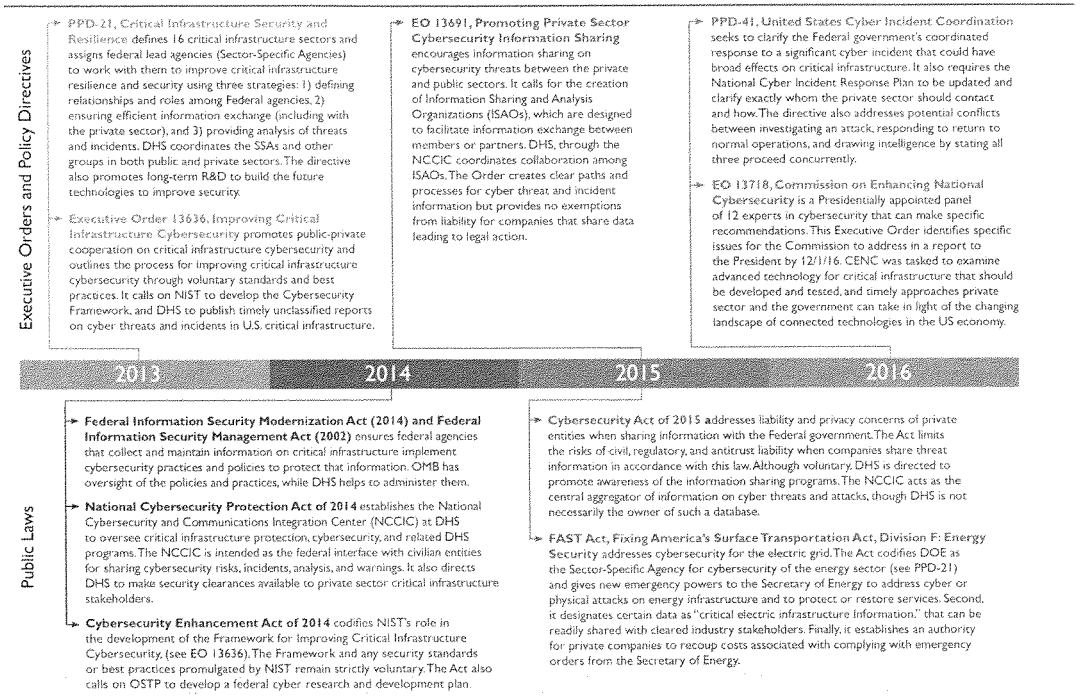
CENC: NOTABLE RECOMMENDATIONS

- Recommendation 1.1: The private sector and the Administration should collaborate on a roadmap for improving security of digital networks
- Recommendation 1.2: Physical-cyber convergence: work closely with the private sector to define and implement a new model for how to defend and secure critical infrastructure
- Recommendation 2.2: Make the development of usable, affordable, inherently secure, and resilient/recoverable systems a top R&D priority
- Recommendation 4.2: Proactively address workforce gaps through capacity building while investing in innovations (e.g. automation, machine learning, and artificial intelligence) that will redistribute this workforce
- Recommendation 5.4: Better match cybersecurity responsibilities with the structure and positions in the executive office
- Recommendation 5.5: Clarify cybersecurity mission responsibilities across departments and agencies

GOVERNMENT COORDINATION GROUPS

1. FBI Field Office Cyber Task Forces (FBI)
2. National Cyber Investigative Joint Task Force (FBI)
3. National Cybersecurity and Communications Integration Center (DHS)
4. US Computer Emergency Readiness Team (US-CERT) (DHS)
5. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (DHS)
6. Cyber Threat Intelligence Integration Center (CTIIC) (ODNI)
7. Intelligence Community Security Coordination Center (ODNI)
8. U.S. Cyber Command Joint Operations Center (NSA/DOD)
9. NSA Central Security Service Cybersecurity Threat Operations Center (NSA)
10. DOD Cyber Crime Center (DC3) (DOD)
11. State Fusion Centers
12. Networking and Information Technology Research and Development Program NITRD (PCAST/OSTP)
13. CIPAC (SCC and GCCs)

CYBER LAWS, EXECUTIVE ORDERS AND DIRECTIVES



What We Heard: CURRENT SITUATION

- Cyber risks to critical infrastructure are numerous and complex. Cyber protection of CI networks is often insufficient and lacks compliance mechanisms.
- Our ability to defend private sector cyber networks does not keep up with the threat. The right adversary with the right capabilities and intent can breach just about any system.
- There are serious physical consequences from a cyber attack on control systems. We can't protect everything so we need to prioritize risks and risk mitigations.
- The Federal Government has limited resources for cybersecurity leadership and expertise, and there is competition over responsibilities.
- Information sharing has improved, but still has its flaws. To be successful, information sharing needs to occur at the speed of the network.

What We Heard: CHALLENGES AND GAPS

- We still don't have frameworks in place to manage a significant disruption to infrastructure, such as a long-duration power outage.
- Greater clarity is needed on the cybersecurity roles and responsibilities of different government departments and agencies.
- Multiple Congressional committees have cyber oversight, making it difficult to get consensus on priorities for focused action.
- Smaller utilities and companies don't have the resources to identify and address unknown cyber risks.
- Much of the information and intelligence now being collected is shared, but it is not organized in a way that makes it readily usable for the private sector.
- Information sharing needs to be bi-directional but industry is reluctant to implement automated services that provide immediate response to cyber attacks.

What We Heard: FUTURE DIRECTION / ADVICE TO NIAC
(1 OF 2)

- Avoid a landscape study. It will only provide a snapshot in time and is unnecessary.
- Focus on an options-based, harmonized approach to systems technology and information sharing regime as an alternative to mandatory regulations
- Examine the implications of a scaled-up, market-driven digital economy, optimized for business, that could introduce massive cyber risks that could cascade across sectors and American communities.
- The study should particularly focus on the lifeline infrastructures, such as electricity and water, and the interconnected nature of cyber.
- Focus on building cybersecurity into infrastructure and on providing assessments or guides on global supply chain risks.

What We Heard: FUTURE DIRECTION / ADVICE TO NIAC
(2 OF 2)

- The study needs to look at novel approaches such as cyber resilience. Start with the assumption that your systems have been compromised.
- Look at models of innovation to understand how technology and innovation dependencies affect future cybersecurity.
- Examine the gap between current cybersecurity investments and capabilities of critical infrastructure, and the actual needs. Recommend what the government should do to close the gap.
- Examine cybersecurity risks associated with supply chains of critical infrastructure.
- Engage with key stakeholders early on to increase buy-in and the NIAC's knowledge of possible cybersecurity regulation

What We Heard: FUTURE DIRECTION / ADVICE TO NIAC
(2 OF 2)

implementation issues.

Senator GARDNER. Thank you, Mr. Fowke.
Mr. Di Stasio.

STATEMENT OF JOHN DI STASIO, PRESIDENT, LARGE PUBLIC POWER COUNCIL

Mr. DI STASIO. Chairman Gardner, Ranking Member Manchin, members of the Subcommittee, thank you for the opportunity to appear before the Subcommittee today.

My name is John Di Stasio, and I'm the President of the Large Public Power Council. Known as the LPPC, the Council represents 26 of the largest state-owned and municipal utilities in the nation, and we provide power to over 30 million people in 13 states.

I'm here to respond to the Committee's interest in cybersecurity threats facing the U.S. electric grid. I'd also like to provide input on S. 79, the Securing Energy Infrastructure Act.

The points I want to emphasize are these. Industry is engaged. While cybersecurity threats to the electric grid are fast evolving and they do require quick, adaptive responses, much is beginning to be known about the threat environment. The electric industry, working with the standards promulgated and enforced by the North American Electric Reliability Corporation, NERC, and also FERC and working with our governmental partners, has effectively responded to known threats and we're actively working to anticipate emerging threats.

Because of the nature of the cybersecurity threats faced by industry, they're evolving rapidly and they're not static so the electric industry has repeatedly emphasized the need for flexible application of cybersecurity regulations that permit industry agility in responding to threats and the ability to implement evolving technology solutions. The electric industry has been grappling with cybersecurity threats for at least a decade. We've learned a lot about the nature of the threats we face in a variety of attack vectors. In response to these threats and with the oversight of FERC, NERC has implemented and enforced the nation's only mandatory suite of cybersecurity standards, the CIP protection standards.

The 2015 cyberattack, as was mentioned, on the Ukrainian grid underscored the electric grid's vulnerability. Although I don't want to understate the concern, I do want to emphasize that techniques used by the attackers were generally understood by the industry and are meaningfully addressed by NERC's reliability standards. Specifically relevant are those CIP standards that provide for electronic security perimeters, access control and malware detection and remediation.

A study by the DHS identified three areas for further review: air gapping, application whitelisting and risks that reside within the supply chain. These areas are under current study by NERC and FERC.

As to air gapping, NERC says, and I agree, that while there are potential security benefits associated with this approach, there are reliability and operational considerations too. So further study is certainly warranted.

Similarly, while application whitelisting is one feasible way to guard against the operation of malware on utility systems, it also presents possible unintended consequences that may include inter-

ference with essential reliability and operational processes. Here again, further study would be useful.

As to the supply chain, NERC is currently in the process of developing a standard at FERC direction. Certainly the procurement of trusted hardware and software is important, but it's not reasonable to ask utilities to police the compliance of vendors and their commitments to follow security practices. We are pressing for an approach to a supply chain standard which also places onus on the vendors to ensure compliance with their commitments to implement sound and reliable security practices.

Because cyberthreats evolve rapidly, it is important that utilities maintain the agility to respond to threats and the ability to implement evolving technology solutions. S. 79 promotes government industry partnership in studying evolving vulnerabilities which will help combat cybersecurity threats; however, LPPC does caution against converting study findings into any one-size-fits-all solutions. The electric industry's response to cybersecurity risk is robust, it's fast evolving and it's intimately tied to efforts by the government to enhance the nation's security posture.

I would never claim that all risks are covered, but a great deal of work is being undertaken in this area. As in any robust security environment, the focus is appropriately not only on prevention, but also on response and recovery.

We welcome the opportunity to work with the members of the Committee to provide further information and receive input on this joint endeavor.

Thank you.

[The prepared statement of Mr. Di Stasio follows:]

Testimony of John Di Stasio
President, Large Public Power Council

Introduction

Chairman Gardner, Ranking Member Manchin and Members of the Subcommittee, thank you for the opportunity to testify today on the electric industry's active and collaborative efforts to anticipate and address cybersecurity threats, and to provide comments on S. 79, the Securing Energy Infrastructure Act. I am John Di Stasio, President of the Large Public Power Council ("LPPC"). LPPC represents 26 of the nation's largest public power systems, which provide power to over 30 million people in thirteen states. Collectively, the LPPC utilities own more than 71,000 megawatts of generation capacity powered by natural gas, nuclear, coal, hydroelectric, wind, solar and other renewable energy sources, and operate about 90 percent of non-federal, public agency owned transmission in the United States.

The points I will emphasize today are:

- Industry is engaged. While cybersecurity threats to the electric grid are fast evolving and require quick, adaptive responses, much is known about the threat environment. The industry, working within the standards promulgated and enforced by the North American Electric Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC), and working with our governmental partners, has effectively responded to known threats, while actively working to anticipate those that are emerging.

- Because the nature of the threats faced by the industry evolves so rapidly, the electric industry has repeatedly emphasized the need for the flexible application of cybersecurity regulations that permits industry agility in responding to threats and implementing evolving technology solutions.

I. The Threat Environment and Existing Responses

The electric industry has been grappling with cybersecurity threats for at least a decade. The public's attention was first dramatically captured in 2007 by the Idaho National Laboratory's "Aurora" experiment suggesting that control systems for generating stations might be hacked and manipulated. Since then, much has been learned about the nature of the threats we face through a variety of attack vectors, including hacking via internet access, phishing (email), watering hole attacks (mined websites), malware (including Stuxnet and reversed engineered versions), and mobile device attacks. In response to these threats, FERC and NERC have promulgated the nation's only mandatory suite of cybersecurity standards, the Critical Infrastructure Protection (CIP) standards, and the electric industry has implemented these standards.

NERC's CIP standards adopt a risk-based approach that begins with an inventory of critical assets and cyber systems, and attaches a comprehensive set of protective measures encompassing security management controls, personnel and training, electronic security

perimeters, physical security for cyber systems, system security management, incident reporting, response planning, recovery, configuration change management and vulnerability assessments, and information protection.

Though the electric industry is involved in the development of the NERC standards through an ANSI-approved process, it does not control the nature of the standards that are ultimately submitted by NERC to FERC for approval, or FERC's oversight. Under the Federal Power Act, FERC's certification of NERC as the nation's Electric Reliability Organization was contingent on NERC's development of procedures assuring its independence from "users and owners and operators of the bulk-power system." Further, FERC has the authority to order NERC to submit to the Commission proposed reliability standards or modifications to reliability standards that address vulnerabilities identified by the Commission. Enforcement of the standards by both NERC and FERC is entirely independent of the industry.

II. Responses to New and Emerging Threats

The cyberattack on the Ukrainian electric grid on December 23, 2015, underscored concern over the electric grid's vulnerability. As reported by the Department of Homeland Security (DHS) on February 25, 2016, and later in additional detail by the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) and SANS Industrial Control System (SANS ICS), the successful cyberattack on a Ukrainian regional electricity distribution company plunged approximately 225,000 customers into darkness. The attack was widely attributed to Russian security services. While service was restored within some hours, the attack underscored the destructive potential of a cyberattack on the electric grid, and highlighted points of vulnerability.

As disclosed in the ES-ISAC/SANS ICS report, hackers gained access to the Ukrainian utility's industrial control system (ICS) network and its supervisory control and data acquisition (SCADA) system via the Internet, enabling them to shut the system down remotely. Access to the Ukrainian utility's control systems was gained through spear phishing - the use of malware and the manipulation of Microsoft Office documents to harvest credentials enabling remote access to the ICS network. I do not want to discount the concern that the attack raises. But I do want to emphasize that these attack vectors are not unknown to U.S. utilities and are meaningfully addressed by NERC's existing reliability standards, as well as other security measures increasingly being adopted by the electric industry (discussed below). Specifically relevant are those CIP standards that provide for electronic security perimeters, access control, and malware detection and remediation.

In its alert and report on the Ukrainian incident, DHS, acting through its Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), also highlighted areas in which further study and potential action are recommended. These include the potential for control center isolation (sometimes referred to as "air gapping"), application "whitelisting" (automated systems permitting only expressly cleared programs to run on utility systems), greater levels of network segmentation, and the prudence in software and hardware procurement (supply chain). These areas are under study by NERC and FERC and, in the case of supply chain security, active standards development is underway.

In Docket No. RM16-18, FERC has asked for comments on whether additional reliability standards are needed to address the potential for control room isolation and application whitelisting. In responsive comments, NERC indicates that both areas are under active study, but also that existing reliability standards guard against related vulnerabilities. NERC also notes that there are operational and reliability drawbacks to each of these approaches that must be weighed carefully. Relevant existing CIP protections include:

- NERC's CIP-005 standard, requirements 1 and 2 of which impose mandatory Electronic Security Perimeters controlling electronic access to Bulk Electric Cyber Systems and securing Remote Access connectivity); and

- CIP-007, requirements 1-5 of which limit network accessible ports; call for active patch management, requires the implementation of methods to detect, deter, prevent and mitigate the threat of malicious code (malware), enables security event monitoring, and enforces system access control.

These standards permit control center isolation, but, as NERC notes, there are operational drawbacks to this approach. For one thing, a utility's ability to access control centers remotely enhances security to the extent it permits otherwise infeasible onsite support from critical vendors whose help is needed to address system failures. Remote access is also important when physical access to facilities by utility personnel is not possible. Further, remote access facilitates vendor patches, which themselves guard against evolving cyber threats. In addition, the ability to receive and transmit real-time data telemetry and security event data is crucial for situational awareness as well as monitoring and analysis.

Similarly, while application whitelisting is one feasible way to guard against the operation of malware on utility systems, the unintended consequences may include interference with future vendor support, conflicts with ongoing patch management and interference with essential programs that may be inadvertently overlooked in the pre-screening process. Here again, further study will be useful.

As to supply chain security (software and hardware procurement), NERC is currently in the process of developing a standard, at FERC's direction. This is an important initiative; one we are following closely. Certainly, the procurement of "trusted" hardware and software, as DHS put it, is an important matter. But having said that, it would not be reasonable to ask utilities to police their suppliers' compliance with security practice commitments the vendors have made. LPPC members are experts at running utility systems, but are not well-positioned to dictate or police the security practices of sophisticated vendors often much larger than the utilities themselves. For that reason, we are pressing for an approach to a supply chain standard which places the onus on vendors to assure compliance with their commitments to implement reliable security practices.

Finally, I want to emphasize the important work that is ongoing with respect to grid recovery and resiliency. This work is critical in order to anticipate the potential that one day our cyber security walls may be breached, despite our best efforts. The focus of this

ongoing work is on the development of systems that can be restarted following incapacitation, on operation of these systems with less than complete electronic control over the grid, and on ongoing service by segments of the grid that may remain operational despite loss of control of other segments. Some of the specific techniques and operational features on which we are focusing attention include the potential for manual operation of certain elements of our systems and facilities (in many cases - e.g., combined cycle gas turbine generators - the degree of digitization will not allow for manual operation), and the use of micro-grids and distributed energy resources.

III. The Importance of Flexible Regulation

Because the nature of the threats faced by the industry evolves so rapidly, the electric industry has repeatedly emphasized the need for the flexible application of regulations that permits agility and a wide variety of evolving responses that are not tied to specific solutions which seem attractive in one context and not the next. Such "performance-based" regulation emphasizes regulatory objectives, and not specific methods. In other words, the key is for the regulator to address "the what and not the how."

NERC's cybersecurity standard CIP-007-6, Requirement 1, for example, addresses protection from malware in just this way, calling for utilities to (1) deploy method(s) to deter, detect, or prevent malicious code; (2) mitigate the threat of detected malicious code; and (3) for those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. This standard does not specify which methods a utility must employ. As NERC explained in its technical guidelines describing the standard: "Due to the wide range of equipment comprising the [Bulk Electric System] Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset."

IV. LPPC's Comments on S. 79

LPPC applauds Senators Risch and King on bipartisan efforts to improve cybersecurity collaboration and research. S. 79 includes several study provisions that should be helpful. Specifically, Section 3 of S. 79 would establish a two-year pilot program within the National Laboratories that would facilitate partnership with relevant entities (including equipment suppliers) to identify new classes of security vulnerabilities. The section further provides that these pilots would support research, development, testing and implementation of technology platforms and standards that would "isolate and defend industrial control systems of covered entities." Section 4 of the bill would establish a working group "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."

However, LPPC cautions against provisions of the bill that call for the development of specific technology applications and prescribed standards designed to "isolate" control systems. We believe the existing framework is demonstrating its ability to address the

underlying concerns this provision seeks to remedy through the study NERC is conducting in connection with FERC's ongoing Notice of Inquiry in FERC Docket No. RM16-18. We look forward to working with the Committee on this issue as the NERC analysis and FERC consideration continues.

V. Other Important Resources and Partnerships

Independent of their engagement in NERC and FERC cybersecurity oversight, LPPC members are actively engaged in a variety of related forums that support cybersecurity threat responses. Some of these are as follows:

A. Reliance on Other Government-Sponsored Reliability Frameworks

LPPC participated directly, along with others in the electric industry, in the process leading to the development of the Cybersecurity Framework in 2014 by the National Institute of Standards and Technology, following a Presidential Directive. As well, LPPC members closely followed the development of the Department of Energy's Cybersecurity Maturity Model. Both of these frameworks provide models for the evaluation of cybersecurity vulnerabilities, and processes for risk management aimed at continuous evolution and improvement. LPPC members routinely use these tools to evaluate their cyber security programs from various perspectives independent of the NERC CIP standards, and to strive for continuous improvement.

B. Information Sharing and Alerts Through the ES-ISAC

The electric industry's primary resource for sharing information of cyber threats—with Federal government support—is the ES-ISAC. Administered by NERC, and operated in coordination with the Electric Sector Coordinating Council (ESCC) and the Department of Energy, the ES-ISAC was chartered to facilitate sharing of information regarding physical and cyber threats, vulnerabilities, incidents and potential protective measures. It serves as the primary security communications channel for the electricity sector, coordinating communications by and between member companies, sharing campaign analysis and incident data from private and public entities, and coordinating event and threat analysis with DOE, FERC and DHS. The ES-ISAC was launched following the issuance of Presidential Decision Directive 63 (PPD-63), along with nearly a dozen other ISACs operating critical infrastructure in other sectors of the economy. The ES-ISAC is among the most robust and effective of these organizations and the electric industry's vehicle of choice for information sharing. An indication of LPPC-member commitment to the ES-ISAC's work is the members' participation in a "Watch Floor Augmentation Program" placing staff from LPPC-member companies in the E-ISAC for one-week periods of time in order to expand coordination of information sharing.

C. Partnership with the Government

At the most senior levels, the electric industry is in close contact with the government through the ESCC. The ESCC serves as the principal link between the Administration and high-level electric industry executives. It is populated by Cabinet-level members from DOE and DHS, senior electric industry executives and trade association leaders. LPPC is

represented on the ESCC and values the direct contact it offers, enabling the Administration and industry to share information regarding ongoing and anticipated risks, and recommended responses. The forum provides an invaluable communication tool.

These contacts extend to other levels of government. The electric industry is in close contact with officials at the Department of Energy working on grid security (the Office of Energy Policy and Systems Analysis and the Office of Electricity Delivery and Energy Reliability) and the Federal Bureau of Investigation. Further, industry officials routinely coordinate with state and local governments in order to maintain the most comprehensive view of threats, risks and vulnerabilities.

D. Cyber Mutual Assistance

The ESCC recently established a voluntary Cyber Mutual Assistance (CMA) Program that is managed by EEI and has nearly 100 member utilities, including investor-owned utilities, public power utilities, electric cooperatives, Canadian utilities, and RTOs/ISOs. LPPC has a representative on the Executive Committee for the CMA Program and several of its members are in the Program. The CMA has a framework in which utilities can assist each other in responding to and recovering from cyber incidents that might exceed the capacity of one or a few entities. The program is structured to provide assistance to electric utilities in rebuilding and recovering necessary computer systems in the event of a regional or national cyber incident.

E. Cyber Security Best Practice Sharing

Along with other members of the electric industry, LPPC members routinely rely on voluntary industry associations for the purpose of strengthening their approach to cybersecurity. Best practices are shared through the North American Transmission Forum and the American Public Power Association's "Improving the Cyber Resiliency and Security Posture of Public Power" (sponsored by the Department of Energy). LPPC has created its own Cyber Security Task Force, charged with the responsibility of sharing best practices, serving to disseminate news of emerging risks, and helping to advocate public policy solutions.

VI. Conclusion

The electric industry's response to cybersecurity risk is robust, fast evolving, and intimately tied to efforts by the government to enhance the nation's security posture. No responsible official involved in the energy industry would claim that all risks are covered, but a great deal of good work is being undertaken in this area, and I am confident that we are intelligently addressing known risks, while making important efforts to anticipate new ones. As in any security environment, there is a great deal of focus on not only prevention, but also response and recovery. We welcome the opportunity to work with members of the Committee to provide further information, and to receive their input in this joint endeavor.

LPPC MEMBER COMPANIES

CELEBRATING 30 YEARS
LPPC
LARGE PUBLIC POWER COUNCIL

Arizona
Salt River Project

California
Imperial Irrigation District
Los Angeles Department of Water & Power
Sacramento Municipal Utilities District (SMUD)

Colorado
Colorado Springs Utilities
Platte River Power Authority

Florida
JEA
Orlando Utilities Commission (OUC)

Georgia
MEAG Power

Nebraska
Nebraska Public Power District
Omaha Public Power District

New York
Long Island Power Authority
New York Power Authority

North Carolina
ElectriCities of NC, Inc.

Oklahoma
Grand River Dam Authority

South Carolina
Santee Cooper

Texas
Austin Energy
CPS Energy
Lower Colorado River Authority

Washington
Chelan County PUD No.1
Clark Public Utilities
Grant County PUD
Seattle City Light
Snohomish County PUD No.1
Tacoma Public Utilities

Puerto Rico
Puerto Rico Electric Power Authority

Senator GARDNER. Thank you.
Dr. Zacharia.

STATEMENT OF DR. THOMAS ZACHARIA, DEPUTY DIRECTOR FOR SCIENCE AND TECHNOLOGY, OAK RIDGE NATIONAL LABORATORY

Dr. ZACHARIA. Chairman Gardner, Ranking Member Cantwell and members of the Subcommittee, thank you for the opportunity to appear before you today. And Senator Alexander, thank you for the kind remarks.

I'm Dr. Thomas Zacharia, Deputy Director of Science and Technology at the U.S. Department of Energy's Oak Ridge National Laboratory (ORNL). The focus of our programs at ORNL is on solving compelling national problems in energy and security. These problems are connected. Energy security is a vital component of our national security.

Last Tuesday, a series of powerful storms swept through East Tennessee. The morning after, I spoke with the Chairman of the Electric Power Board (EPB) in Chattanooga with whom ORNL has a long-standing partnership. The Chairman told me that the severe weather had disrupted services to 65,000 homes in the EPB service area, but thanks to the state-of-the-art control of the EPB system, half of those homes experienced nothing more than just a power flicker and EPB was able to rapidly work to restore service to the other homes.

We know that these same digital systems that are so successful at running the electric grid efficiently and effectively are also vulnerable to cyberattack. The DOE National Laboratory system recognizes this vulnerability and is actively pursuing technology advancements to mitigate this threat.

Often described as the world's largest machine, the U.S. electric grid is a foundation of our competitive national economy and, indeed, our way of life. However, as utilities have increased smart interconnections between grid services to make the system more agile and adaptive and able to preempt disturbances, they have also created some access points for potential cyber disruption.

With the growing sophistication of cyber intrusions, we need to go beyond today's practices. With DOE and electric utilities, we've been exploring ways to get critical infrastructure off the public internet.

Specifically, the following technological advancements and solutions are needed to ensure reliable, efficient, resilient and secure grid infrastructure across the country: eliminate direct connectivity to the internet, implement advanced cyber defensive measures beyond what's possible on the internet, develop supply chain components and Internet of Things devices with security built in, provide wide area situational awareness and decision support by enhancing grid state monitoring with advanced sensing and measurements and use living laboratories in partnerships with utilities and national laboratories to test functionality and resilience of advanced cyber and cyber physical solutions to accelerate transition to practice.

ORNL has developed numerous technologies used to counter cybersecurity threats. These technologies range from hardware device

monitors to software that can detect dormant malicious code, to platforms that can discover and detect the presence of advanced persistent threats.

Cyber physical tools and capabilities include Grid Eye sensors located across the U.S. for real time systems monitoring and EAGLE-I which monitors the nation's energy sector in real time. This can be leveraged with the PNNL-led effort on the Cybersecurity Risk Information Sharing Program (CRISP) to provide cyberthreat information to industry partners.

Without our established public/private partnerships, these technologies will not be adopted by industry. For example, DOE and ORNL are leveraging the EPB automated smart grid and fiber optic network infrastructure to develop next generation of cybersecurity defense systems, including next generation quantum cybersecurity software that has the potential to prevent undetected hacker intrusions into the IT networks.

National labs, including ORNL, are uniquely positioned to address cybersecurity challenges through technology breakthroughs in partnership with the private sector.

One example of the laboratories, the system of laboratories, working together on major challenges is the Grid Modernization Laboratory Consortium, GMLC. This was established as a strategic partnership between DOE and the national laboratories to bring together leading experts, technologies and resources to collaborate on the goal of modernizing the nation's grid.

Thank you for the opportunity to be here today to share with you what we see are some of the solutions to minimize cybersecurity threats to the electric grid and, in turn, further contribute to the security of the nation.

[The prepared statement of Dr. Zacharia follows:]

Statement of Thomas Zacharia, Ph.D.
Deputy Director for Science and Technology, Oak Ridge National Laboratory

Before the
Subcommittee on Energy
Committee on Energy and Natural Resources
U.S. Senate
March 28, 2017

Chairman Gardner, Ranking Member Manchin, and Members of the Committee: Thank you for the opportunity to appear before you today. I am Dr. Thomas Zacharia, Deputy Director of Science and Technology at the U.S. Department of Energy's Oak Ridge National Laboratory (ORNL) in Oak Ridge, Tennessee. It is an honor to provide this briefing on cybersecurity threats to the US electric grid and technology advancements to minimize those threats.

INTRODUCTION

Oak Ridge National Laboratory is the largest Department of Energy (DOE) science and energy laboratory, conducting basic and applied research to deliver transformative solutions to compelling problems in energy and security. ORNL's diverse capabilities span a broad range of scientific and engineering disciplines, enabling the Laboratory to explore fundamental science challenges and to carry out the research needed to accelerate the delivery of solutions to the marketplace. ORNL supports DOE's national missions of:

- Scientific discovery—We assemble teams of experts from multiple disciplines, equip them with powerful instruments and research facilities, and address compelling national problems;
- Clean energy—We deliver technology solutions for energy sources such as nuclear fission/fusion, geothermal, hydropower, and biofuels, as well as energy-efficient buildings, transportation, and manufacturing.
- Security—We develop and deploy "first-of-a-kind" science-based security technologies to make the United States and its critical infrastructure, and the world more secure.

ORNL supports these missions through leadership in four major areas of science and technology:

- Computing—We accelerate scientific discovery and the technology development cycle through modeling and simulation on powerful supercomputers, including Titan, the nation's most powerful system for open scientific computing (third largest in the world), advance data-intensive science, and sustain U.S. leadership in high-performance computing;
- Materials—We integrate basic and applied research to develop advanced materials for energy applications;
- Neutrons—We operate two of the world's leading neutron sources that enable scientists and engineers to gain new insights into materials and biological systems;

- Nuclear—We advance the scientific basis for 21st century nuclear fission and fusion technologies and systems, and we produce isotopes for research, industry, and medicine.

Today's briefing reflects my perspective as the deputy director for science and technology of a national laboratory with an intense focus on solving compelling national problems in energy and security. These problems are closely linked, in that energy security is a vital component of our national security.

Oak Ridge National Laboratory has a long and storied history in working with the electric utility industry to solve complex problems. This has included working with public utilities, large investor-owned companies, municipalities, as well as rural electric cooperatives.

ORNL researchers have developed highly secure Internet of Things (IoT) sensors and systems specifically designed to provide enhanced measurements for improving electric grid operations. Such devices have been installed at Chattanooga Electric Power Board (EPB) substations and are providing extended grid operation measurements to EPB's control center.

ORNL has been engaged with electric utilities and rural co-ops regarding the use of small unmanned aerial systems (UAS)—commonly called "drones"—through our UAS Research Center. A 168-page best practices guide for electric utility usage of drones for system inspections was released this month with more than 3,000 downloads.

Private industry has already developed innovative solutions to secure the grid, but the task is becoming increasingly difficult due to more and progressively sophisticated cyberattacks. New vulnerabilities, such as distributed power generation and the growing number of Internet-connected devices on the system, present additional challenges.

Supply chain vulnerability adds additional complexity to cyberdefense and requires more action. The vulnerabilities encompass technology systems and processes that are typically the responsibility of non-utility organizations like instrumentation, information technology, and control system providers.

SB 79 addresses an approach to deal with the vulnerability of critical components for the electric grid supply chain. The intent of the bill focuses on a critical need to evaluate technology platforms and standards. The next step should be to engage industry, national labs, and academia to develop a national cyber-informed engineering strategy to isolate and defend entities.

What makes the grid smart are the interconnections that enable communications between devices, which in turn make the system more agile, adaptive, and able to preempt disturbances. However, information technology devices embedded throughout the system also create more access points for potential disruption.

According to David Johnson, EPB chief technology officer and vice president for information technology, cybersecurity defense is a daily challenge as the utility fights back against denial of service attacks, physical system attacks, malicious intent attacks, and authentication attacks. "The challenge in today's technology environment is to secure our systems without inhibiting

productivity or service to our customers. The single largest threat to EPB cybersecurity is connection to the public Internet," Johnson said.

Reliance on the Internet for non-secured business connectivity, technical supports for products, and data exchange is the core electric grid attack vector at present. I believe that the experts from EPB are correct that a sustainable solution to electrical grid security is the elimination of the grid's direct connectivity to the Internet, as David Johnson noted.

With the growing sophistication of cyberintrusions, we need to go beyond today's practices. The nation's electric grid needs a new solution, and it needs it now.

With DOE and electric utilities, we have been exploring ways to get critical infrastructure off the public Internet. Some utilities are already moving in this direction by creating a separate architecture for their communications systems. But insulating the grid from increasingly complex attacks requires a multidisciplinary effort that perfectly aligns with the mission of the national laboratories.

GRID VULNERABILITY: A NATIONAL SECURITY THREAT

What's at Stake

The nation's electric grid is a vital resource upon which our economy and citizens' daily lives depend. But it is a system that is uniquely vulnerable to cyberattack at a time when more utility controls and "smart" technology are connected to the public Internet than ever.

The grid is an integral part of the life of every human being living in a developed society. On a personal level, electricity powers many creature comforts in the home, and many conveniences that ease everyday living. Electricity powers commercial and industrial enterprises—the engines of present-day economies. Even for those commercial and industrial processes using other fuels, electricity powers the control systems inherent in those processes. There is no aspect of modern civilization that is not impacted—directly or indirectly—by the electric grid.

There are close inter-dependencies between various critical infrastructures. The telecommunications grid, for instance, carries the signals used to control all aspects of the electric grid. The electric grid, in turn, powers the components of the telecommunications grid. While emergency operating procedures can mitigate the loss of services, neither grid can maintain sustained long-term operations without the other.

Technological Solutions

The national laboratory system is uniquely positioned to address cybersecurity challenges through technology breakthroughs in partnership with the private sector. At Oak Ridge National Laboratory, expertise and capabilities in high-performance computing, data and graph analytics, discrete mathematics, power systems and engineering, embedded systems and wireless technologies, sensors and controls are critical to provide solutions and breakthroughs to detect and deter cyberattacks. ORNL has a long history of discovery and innovations in power systems and critical infrastructure protection technology development and assessment. The lab possesses the capabilities to produce advanced solutions for industry and federal, state, and local agencies.

Specifically, the following technological advancements and solutions are needed to ensure a reliable, efficient, resilient, secure grid infrastructure across the country:

1. Eliminate direct connectivity to the Internet. Taking a page from global cloud firms that have established dedicated VPNs connecting their compute centers, the electric grid networks should be configured similarly, creating a closed and secure system with few, very well protected points of presence (POPs) to the external networks. Those POPs must have the best technologies to ensure they cannot be breached. Dark fiber across the United States may provide a cost-effective protective measure, exploiting advanced communications (5G-LTE, satcom and private wireless) and cybersecurity technologies suitable for the expanding smart grid requirements.
2. Implement advanced cyberdefensive measures beyond what is possible on the public Internet. This includes innovative novel communication security approaches being applied in other sectors and evaluated on the energy infrastructure.
3. Develop supply chain components and Internet of Things devices with security built in.
4. Provide wide-area situational awareness and decision support by enhancing grid state monitoring with advanced sensing and measurements. Build off existing situational awareness tools Cybersecurity Risk Information Sharing Program (CRISP), and Environment for Analysis of Geo-Located Energy Information (EAGLE-I) technologies.
5. Use living laboratories in partnership with utilities and national laboratories to test functionality and resilience of advanced cyber- and cyberphysical solutions to accelerate transition to practice.

Advancements Made
ORNL has developed numerous technologies used in the conduct of cybersecurity (see Appendix A). These technologies range from hardware device monitors (such as BEHOLDER), to software that can detect dormant malicious code (HYPERION), to platforms that can discover and detect the presence of advanced persistent threats (ORCA).

Other cyber-physical tools and capabilities include GridEye sensors located across the U.S. for real-time systems monitoring, and EAGLE-I, Environment for Analysis of Geo-Located Energy Information, which monitors the nation's energy sector in real time. This can be leveraged with the PNNL-led effort on the Cybersecurity Risk Information Sharing Program (CRISP), to provide cyber threat information to industry partners.

Another good example is ORNL working with a private firm to further develop quantum key distribution (QKD) technology as a solution to harden the grid. The technology, called AQCESS (for Accessible QKD for Cost Effective Secret Sharing), greatly increases the number of nodes that can be supported by a single QKD channel. The nodes are cost-effective and can be added at any time, thereby reducing the per-node cost, while enhancing the flexibility and accessibility of a QKD network.

ORNL's unique expertise in advanced manufacturing has supported its creation of low-cost, 3D-printed sensors that can identify voltage issues and power failures as soon as they occur, as well as fuse performance analysis with weather and climate indicators, making grid security, regular maintenance, and disaster response more efficient and cost-effective. These devices can be manufactured in the US with built-in security.

In addition, ORNL is researching unique methods and technologies to harden the grid and its supply chain against harm, whether intended or not. These include: "Fingerprinting" technologies to monitor device behavior at the chip level to identify the presence of malware or attempts at spoofing that could cause harm to critical infrastructure; systems to replace reliance on GPS systems for timing signals and synchronization; and researching the task of getting the grid "off the Internet" by turning to private networks leveraging underutilized fiber optic capabilities.

The Importance of Partnerships

However, without our public-private partnerships, these technologies will not be adopted by industry. ORNL's industry partnerships have been essential to the development, testing, and deployment of innovative technologies to modernize the grid and protect it from both physical- and cyberattack.

ORNL works with several utilities on grid modernization and security innovations, including the Chattanooga Electric Power Board (EPB), Dominion, Duke Energy, Southern Company, and Tennessee Valley Authority.

For instance, ORNL and DOE have enjoyed a productive working relationship with the Chattanooga EPB. These efforts support America's technological leadership, national security, and the goal to create a new, more reliable, and affordable electric utility service for the Internet Age. The EPB smart grid and advanced communications network also make a living laboratory to test new technology developed by ORNL and other labs.

DOE and ORNL are also leveraging the EPB automated smart grid and fiber optic network infrastructure to develop next generation of cybersecurity defense systems, including next-generation quantum cyber security software that has the potential to prevent undetected hacker intrusions into IT networks. The software will be tested in the coming year on EPB dark fiber and later as an integrated part of EPB normal electric system operations data traffic. We will have the ability to test and measure its effectiveness. If could be a game changer for the future of electric grid security.

EPB Chairman Joe Ferguson recently remarked on the value of the DOE EPB working relationship: *"Since we started our partnership with DOE over 3 years ago we have enjoyed real success, the kind of success that makes a difference to EPB business capabilities and to the quality of life enjoyed by the people of our community. I have no doubt that we have just begun to realize the benefits of our success. Together we will go on to even greater achievements in future for all of the people of our country."*

NATIONAL LABORATORY EXPERTISE AND CAPABILITIES

DOE's scientific and technical capabilities are rooted in its system of national laboratories—17 world-class institutions that constitute the most comprehensive research and development network of its kind (see Appendix B). The laboratories work as a network with industry, academia, and other federal agencies to focus on complex, mission-critical research and development activities.

The national laboratories:

- Work at the forefront of fundamental research, unveiling secrets of the basic building blocks of matter and are creating a new generation of materials (including biological and bio-inspired materials) to underpin advances in energy generation, storage, transmission, efficiency, and security.
- Lead in RD&D that supports the national security missions of DOE, and they partner with industry, academia, and other Federal agencies to provide innovative solutions in the broader areas of defense, homeland security, cybersecurity, and intelligence.

Through these activities—conducted at large scales and with significant, long-term investments of resources, including world-class scientific and technical expertise—DOE's national laboratory enterprise serves as an enduring science and technology powerhouse for the nation.

One example of the laboratories working together on major challenges is the Grid Modernization Laboratory Consortium (GMLC). This was established as a strategic partnership between DOE and the national laboratories to bring together leading experts, technologies, and resources to collaborate on the goal of modernizing the nation's grid. The benefits of the GMLC include more efficient use of resources; shared networks; improving learning and preservation of knowledge; enhanced lab coordination and collaboration; and regional perspective and relationships with local stakeholders and industry.

The United States is unique in the breadth and depth of scientific and engineering excellence possessed by its national laboratories and will continue to play a continued leading role in grid modernization, reliability, security and resilience.

CLOSING REMARKS

Sometimes called the world's largest machine, the electric grid is the cornerstone of our economic foundation, U.S. competitiveness, and our way of life. DOE's national laboratory system stands ready to work closely with industry and other institutions to plan and create innovative technical solutions to protect our grid. Thank you again for the opportunity to provide this briefing. I welcome your questions on this important topic.

APPENDIX A

Summary of ORNL and National Lab Cyber R&D Capabilities for Energy Sector Protection

The National Laboratory complex is well-suited to explore and develop technological solutions towards protecting the energy grid. Partnerships with government, industry and academia have been longstanding and mature. The national laboratories transition early stage research and development technologies to fielded and operational tools/platforms via partnerships with industry and Federal government partners.

Key ORNL Cyber-Physical Capabilities

- **Facilities**
  - **Distributed Energy Control and Communication (DECC)** laboratory for testing and evaluating emerging energy security tools and techniques
  - **Complete System-Level, Efficient & Interoperable Solution for Microgrid Integrated Control (CSEISMIC)** for testing and evaluation of microgrid control and security
  - **Real-Time Digital Simulator (RTDS)** for simulating electrical nodes on the power grid. ORNL capability to simulate 366 nodes
- **Tools**
  - **Grideye** sensors located across the U.S. for real-time monitoring of power grid
  - **Visualizing Energy Resources Dynamically on the Earth (VERDE)** is a visualization and analysis system designed to predict possible energy system outages as well as help first-responders rapidly locate the outages when they occur
  - **EAGLE-I** is a comprehensive, real-time energy monitoring dashboard developed by DOE/OE for integration with VERDE
  - **Oak Ridge Cyber Analytics (ORCA)** is a real-time cybersecurity platform for detecting advanced persistent threats and 0-day exploits
  - **Situ** is a real-time cyber situational awareness tool capable of determining anomalies in network related traffic
  - **Timing Authentication Secured by Quantum Correlations (TASQC)** a ground-based timing capability for secure communications
  - **Hyperion** is a cyber security technology designed to look inside an executable program and determine software's function or behavior without the use of the software's source code.
  - **BEHOLDER** in partnership with General Electric Research, ORNL is developing technology that exploits fine-grained timing data collected from remote network and SCADA (supervisory control and data acquisition) devices to reveal the presence of

software and network intrusions.

National Laboratory Partnerships for Cyber-Physical Security

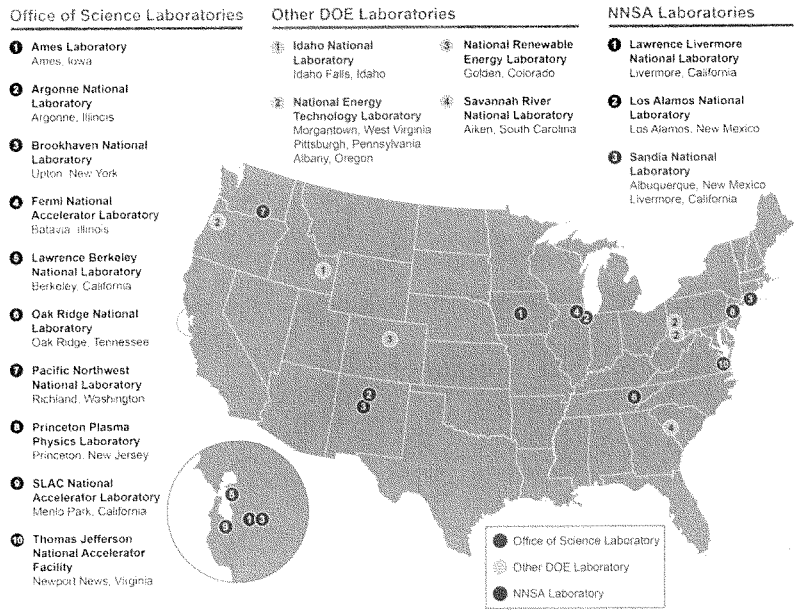
- **Cybersecurity Risk Information Sharing Program (CRISP)**
  - Partnership between PNNL, INL, ANL, and ORNL funded by DOE
  - Provide cyber threat information to industry partners
- **Cyber Analytic Tools and Techniques (CATT)**
  - Partnership between PNNL, INL, ANL and ORNL funded by DOE/OE and DOE/IN
  - Provide automated & advanced cyber analytics capabilities for industry partners and IC
- **Cybersecurity R&D Gap Analysis**
  - Partnership between PNNL, ANL, LLNL, ORNL, and Battelle-Memorial
  - Two year effort to determine cybersecurity R&D gaps and develop way-ahead strategy

National Electric Gird Cybersecurity R&D Needs

- **Anticipatory Threat Determination**: the ability to provide threat predictions to accurately predict emerging/advanced threats
- **Dynamic Resource Allocation:** the ability to dynamically sense a given network and adapt its resources to "harden" critical resources based on realized environment changes
- **Alternative Timing Capabilities:** the ability to use non-GPS timing systems to avoid spoofing of critical timing signals
- **Real-time Device and User Authentication:** the ability to ensure that devices/software have not been tampered with as well as granting user access based on multiple levels of authentication

APPENDIX B

Map of the DOE Laboratory System



Senator GARDNER. Thank you, Dr. Zacharia.

I know Senator Alexander has a hard stop, so, Senator Alexander, I am happy to yield to you if you would like to ask some questions.

Senator ALEXANDER. Thank you, Mr. Chairman, I appreciate that very much. So I will just ask one question.

Dr. Zacharia, ever since I have been here, which is now about 14 years, the Congress and the Administrations have put a priority on building supercomputers, and I believe you have built the fastest supercomputing system in our country. Is that right?

Dr. ZACHARIA. That is correct, Senator.

Senator ALEXANDER. And it is going to increase in 2018 by a factor of five, is that correct too?

Dr. ZACHARIA. Factor five was 2004.

Senator ALEXANDER. Well, let me ask, in fairly specific terms, what difference does it make if we have the fastest computer, or the second, or the third, or the fourth, or the fifth, or the sixth, in terms of cybersecurity and monitoring our grid?

Dr. ZACHARIA. Senator Alexander, thank you for the question.

Like any other system, leadership in supercomputing is absolutely essential because the Chinese and other nations use a supercomputer for just the same advantages that we seek to achieve in this country. So, the Chinese system that is currently, that the Chinese have two systems that is the fastest in the world today. Many of the applications that they're using are for cybersecurity, both defensive and offensive cybersecurity, as well as other materials and technologies.

It's absolutely essential that we maintain the ability to match and deter cybersecurity threats. The way the supercomputer comes into play is that as the grid system particularly as the nation's electric grid system have deployed new technologies to make them more smart so they can deliver better services to their consumers.

They've also become much more data aware. They produce a lot of data. There are lots of sensors. What supercomputers allows us to do is to monitor the data real time, analyze it, do some of the deep data analysis and just like you might have heard, IBM Watson, to be able to actually make decisions on the fly, to do cognitive computing.

The summit system that is going to be deployed in 2018, even though it's going to be five times faster, it also has a co-processor that allows you to do real time data analysis and decision-making. So these are some of the advantages in terms of being able to stay at the leading edge to make sure that the nation's grid system is protected and we have the necessary tools and capabilities to do that.

Senator ALEXANDER. Thank you, Dr. Zacharia, and thank you, Mr. Chairman, for your courtesy.

Senator GARDNER. Thank you, Senator Alexander. I will now turn to the Ranking Member of the Committee, Senator Cantwell.

Senator CANTWELL. Thank you.

I am also happy you have the fastest supercomputer.

[Laughter.]

When every particle in a storm can be put into an algorithm and you can process that information so the United States can have

more data, instead of going to the Europeans, who right now have a faster or at least, in my understanding, have better, more accurate information on Sandy than we did in the United States—we need to keep going. We need to give you all the capacity for that and more because this weather aspect is so, so important.

I see your colleague is nodding because when utilities know that that level of damage is going to occur, they can better plan for it. They can relocate assets, get them there in time, all sorts of things.

So anyway, on the cyber front, Dr. Zacharia, you mentioned the supply chain. We also had a hearing on cybersecurity in the Commerce Committee, which I found very interesting because a lot of the discussion focused on private sector entities. I definitely believe in collaboration here between the universities, the utilities and the private sector on where we go forward. But we did not get too much into the supply chain. We talked a lot about education, how we need to have these various two-year and four-year academic degrees on cybersecurity. We do not, currently, have enough focus on that. But we did not talk enough about the supply chain and supply chain risk. Could you elaborate on that?

Dr. ZACHARIA. So, it is, Senator Cantwell, thank you very much for the question.

It's certainly clear that the supply chain is vulnerable and there is clear evidence that the supply chain, some of the key components that are used, is vulnerable for cyber intrusion. I think it is really important for laboratories like the DOE lab system working with private sector and university partners to have the ability to test and validate the components that go into our grid system, because they are so essential to maintaining the security of the system while delivering the kind of services the consumer expects today.

Senator CANTWELL. So are you worried about a direct threat or just not understanding the supply chain and the dynamics of products?

Dr. ZACHARIA. Well, I think that it is really important for us to ensure that we understand the supply chain of critical components on what we consider as an essential part of our U.S. economy which is the electric grid.

And so, while I cannot speak to specific issues about a particular component, I think it's essential that we pay attention to the security threats and vulnerabilities associated with the supply chain.

Senator CANTWELL. Okay.

Anybody else?

Mr. FOWKE. I would just add that these operating technologies are increasingly converging with IT technologies. And so, when you think about the hardware that we use to run the grid, there's chips and other IT type technologies embedded in that and without standards that protect and make sure that we have the necessary cybersecurity overlays that equipment and the ability to monitor that equipment, then we're really flying blind.

I think there's a lot of work that can be done in making sure that what's on the grid and, quite frankly, ultimately what's in somebody's home, in the interim of things is secured in a way that, I think, we all would come to expect.

Senator CANTWELL. And that is a group discussion as well?

Mr. FOWKE. Yes.

Senator CANTWELL. To get there, it is everybody discussing and participating in that?

Mr. FOWKE. Yup.

Senator CANTWELL. Well we definitely need to think about that and the recommendations from the Quadrennial Energy Review on cybersecurity, and we definitely need to get those implemented.

Thank you, Mr. Chairman.

Senator GARDNER. Thank you, Senator Cantwell.

Throughout the testimony and in your written testimony, I have seen a number of acronyms. I think, if you just look at what is involved in cybersecurity, so far, we have covered DOE, NIST, DHS, NSA, CIP, E-ISAC, is that how you say it, I, S, A, C, E-ISAC, FS-ISAC, ESCC, NIAC, NERC and FERC. It is clear where we go in cyber, so I think that is part of the challenge that we have.

Senator Cantwell mentioned that she had a Commerce Committee hearing on cyber. Later this week I am going to be holding a Foreign Relations hearing where we are going to talk about cyber. Here in Energy Committee, we are talking about cyber and all these acronyms.

Mr. Fowke, you mentioned at the beginning of your testimony one of the things that we need to work on is better coordination with the Department of Energy, Department of Homeland Security and the other agencies that we highlighted here.

I have introduced a bipartisan bill to create a Senate Select Committee on Cybersecurity, trying to answer some of these jurisdictional questions. Over half of the Committees in the United States Senate have some jurisdiction, either in the rules or self-claimed jurisdiction, over cybersecurity. I think nine committees have held 20 hearings on some cyber element.

What are your thoughts on creating a Senate Select Committee on Cybersecurity that would have jurisdiction over cybersecurity, cyberspace, which would oversee and strengthen U.S. data prevention, data breach prevention strategy, other cyber activities? Would it have a value, the Select Committee on Cybersecurity, that would help the energy industry organize government rules and responsibilities?

Mr. FOWKE. Yes, Senator Gardner, I think it would.

And let me apologize for the use of the acronyms. That's how you get your testimony in in five minutes.

Senator GARDNER. It wasn't just you.

[Laughter.]

Mr. FOWKE. Oh.

As I said in my testimony and as the NIAC scoping study points out, we just need to coordinate better. I mean, there's a lot of work being done, but it's being done by a lot of agencies. It's being done by a lot of Congressional committees, and there's a lot of industry work that's being done as well.

I think we're getting better at coordinating, but the bad actors are getting better at attacking us at the same time.

So, to the extent we can have a more coordinated, focused effort, you know, it doesn't—it reminds me a little bit about the difference between watching a professional soccer team and kids that are six years old. Everybody is going to the ball, but you've got to play in

your swim lanes and as a team. I think that's what you're suggesting.

I would caution that sometimes we rush to pass the legislation and we ought to make sure that there isn't unintended consequences with that legislation too. And I really think the tone at the top is where we start and then we work our way down. And that way we can have a coordinated response.

Senator GARDNER. Mr. Fowke, follow up on that too.

Is there any kind of coordination that Congress can help provide industry, or in the various organizations that you are a member of? Will you, through industry and your partners in government, come up with the correct coordination on your own or is it something that Congress needs to provide guidance with?

Mr. FOWKE. We need help getting the information.

As I mentioned in my testimony, quite often, by the time we hear about a potential threat or a threat from the government, we've known about it for quite a long time through private sources or industry communication, et cetera. And I think the reason for that is we struggle on taking what could be classified information, declassifying it and getting it out quickly.

The second thing we struggle with is where there is a need to keep it classified. I think we've got a six to eight-month backlog per individual to try to get classified status. So you might want to share the classified information, but you can't share it because the people aren't cleared.

In an age where we're talking machine to machine, that is, that's quite a hindrance. We need to do better with that because we have the tools in place, another acronym, CRISP, the detection software. That's a good system and right now the information is going right into the lab and it's basically where it stays. So, we need to start getting a two-way flow of, what I think, could be very valuable information.

Senator GARDNER. So if I understand the problem, there's a twofold challenge, right?

You have the challenge of getting the information from the Federal Government, information that you need to protect the grid, the system, your power system. And secondly, of course, is getting people who can then receive that information with the proper classification. Is that correct?

Mr. FOWKE. That's correct.

Senator GARDNER. There is a story that I wanted to share with you. I am sure on the Committee, you have all heard this story. It was reported in E&E news. It is a story of, I guess it was a security test, where they had a person come into the utility, basically to audit their security. Apparently the security auditor told him that he had seen equipment in the utility, in the utility control room, that would not be allowed in a federal installation because it is vulnerable to hackers. The security auditor said, in a federal installation that piece of equipment would not be allowed to be in it because of its vulnerability. The head of the utility company asked, what is that equipment? And the response was, I can't tell you, it's classified.

[Laughter.]

So, that is the problem.

Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you, Mr. Chair, and I appreciate the comments today.

This is an area that I worked in as the Attorney General of the State of Nevada and something that I saw from a state perspective that we needed to address but was always concerned about the federal interaction. Now I am on the federal side and I see the same, kind of, bifurcation where there is a lack of communication, not only at the federal level, but the communication at the federal level and the states. And that is the question I have from the very beginning.

Mr. Bardee, it is a two-part question relating to how information, with respect to threats and remediation, is conveyed to state officials? And it goes back to some of the concerns that we have talked about with acronyms and the number of committees and commissions that are out there.

I understand that the Electricity ISAC is responsible for situational awareness, incident management and communications regarding cyberthreats to the grid. But the Electricity ISAC is only one of 20 different ISACs. States participate directly in only one which is the multi-state ISAC. So, how does the cyberthreat information regarding the electric grid get to those state officials?

Mr. BARDEE. There are a number of informal mechanisms by which that information can be shared. Our agency, for example, particularly in our Office of Energy Infrastructure Security, reaches out to the states and tries to work with them and share information and assist them, as appropriate. I know the Department of Energy does, too.

And the more sensitive information, the classified information, generally, it originates in other parts of the Federal Government, Department of Homeland Security, for example. And we are a recipient of that sometimes, but we're not the source of it.

So I would say that it is a challenge to ensure that the states are getting all of the information they need, given the ways in which that information may come into the government. But it's an ongoing effort and we are looking for ways to improve that. I, for example, and some of my colleagues are going to be meeting with NARUC, I think in about two weeks, to discuss cybersecurity. And this, I would expect, to be part of the conversation.

Senator CORTEZ MASTO. Yes.

I would appreciate more of a direct interaction at the state level and not through different task forces or multi-levels. I know the state counterparts would appreciate that. I think this is an effort that we have to look beyond, not just the federal level, but at the state level. Everybody should be working to address the cyberthreats that we see, so I appreciate your comments.

Let me just open this up. I understand that the second installment of the QER noted that the traditional definition of reliability may be insufficient to ensure system integrity and available electric power in the face of physical attacks and cyberthreats, among other things, and that the security of the systems, particularly cybersecurity, is a growing concern. Would you agree with that assessment from the QER?

I will open that up to anyone.

Mr. DI STASIO. I would say, I think, FERC addressed part of this as a—it was mentioned previously about the 2013 Metcalf attack in California. At that time, I was a CEO of a neighboring utility in California, so that was a very real incident for us.

FERC added a standard on physical security that really directed utilities to make a risk-based assessment of where to harden the system from both physical attacks and we've already got the CIP standards that are focused on doing the same for cyber.

But again, these risks are evolving. They're emerging. They're not static. So it becomes more of a prioritization of which of the systems and which of the components within the system are going to provide the greatest risk mitigation and doing those first. And that's what we're really in the midst of undertaking right now.

Senator CORTEZ MASTO. I appreciate that.

One final question, Dr. Zacharia. You mentioned a suggestion that one way to answer the concern about cybersecurity threats is that we eliminate the grid or any type of critical infrastructure from the internet. Can you expand on that? Do you think that is possible, particularly with the evolution of technology, the Internet of Things and everybody being connected, including smart meters, which we have in the State of Nevada?

Dr. ZACHARIA. Senator, what I meant to say was that it should be disconnected from the commercial internet. So let me expand on that.

Our own experience is that when Oak Ridge National Laboratory, about a dozen or so years ago, was deploying one of the fastest supercomputers in the world, we did not have very high speed network connectivity into the laboratory. And the way that we solved that problem was that there is actually dark fiber that most of the major utilities have in the right of way. Generally it is usually used with control systems and it has redundant pairs of fiber. We were able to work with the utilities, in this case, TVA, to get a pair of fiber that is completely separate and isolated from the commercial internet provider.

One of the suggestions is that there is a tremendous amount of dark fiber that is available on the right of way—using these dark fiber as a way to create a separate, you know, sort of air-gapped, network connectivity because I think it is really important that the consumers are used to a certain level of service and it's not good to go back. And one way to provide that service is to actually have dedicated network and using dark fiber that is already available in the ground today.

Senator CORTEZ MASTO. Thank you. Thank you very much.

Senator GARDNER. Thank you.

Senator King.

Senator KING. Thank you, Mr. Chairman.

First, a sort of basic question.

Mr. Bardee, is there one national grid? My understanding is that the entire nation is not connected. There are regional grids. Am I correct?

Mr. BARDEE. The best way to describe it is that there are three interconnections in the United States.

One, basically within Texas, not fully congruent but basically one for the western third of the United States, and the rest in the East.

Senator KING. Are those three connected? In other words, could you bring down the entire nation at one time or would you have to do three?

Mr. BARDEE. There are very limited connections between those three. So generally, if there is a problem in one of the interconnections it does not affect the other two.

Senator KING. Let me talk about the sophistication of the attacks. My understanding is that the level of sophistication is going up.

Mr. Fowke, you mentioned 500,000 attacks. That is astonishing. A lot of those are poking and prodding and testing and trying to find vulnerabilities and that these attacks are getting more sophisticated all the time. Is that correct?

Mr. FOWKE. Yes, I would not say the 500,000 are sophisticated, all sophisticated nation states, but the problem with trying to categorize what might just be something like, you know, a benign, well it's not benign, but a phishing attempt. Something we all get is that there might be more behind what looks like run of the mill type, you know, virus or malware that's trying to be implanted.

And what happens is if you get phished and it's allowed to get onto your network, that virus, that malware, will hunt around for as long as it takes, searching out weaknesses that can get it into something more important, like your——

Senator KING. And it can also lie dormant for some period of time.

Mr. FOWKE. Yes.

I believe that is another acronym. I think it is called APT, but Advanced——

Dr. ZACHARIA. Persistent Threat.

Mr. FOWKE. There, thank you.

Senator KING. Advanced Persistent Threat.

Mr. FOWKE. Right.

Senator KING. But what we are seeing here is the nature of warfare changing before our eyes. And the Russians, particularly, are playing a weak hand, very effectively, and it is on the cheap. For the cost of one tank they can hire 500 hackers or trolls or whatever.

We know that this is a part of their foreign policy strategy in terms of elections, in terms of other kinds of disruptions to western countries. And this is, really, a threat that the likes we have not seen.

By the way, Mr. Chair, I like the idea of the Select Committee on Cybersecurity. You get to tell Senator McCain that you are taking cyber away from Armed Services.

[Laughter.]

Senator GARDNER. He co-sponsored it.

I don't know if he knows the full implication of that.

[Laughter.]

Senator KING. I think that is an important idea.

Well again, several of you mentioned S. 79. We are not trying to do anything prescriptive here, but we are trying to test hopeful, promising technology to link the utility community with the national labs. What I hear many of you saying is coordination is one

of the key elements of this and I am talking, we are talking, about coordination on a specific project.

But on the broader sense, I think, good coordination is one of the most important things that we can try to develop. We need this country to develop a cyber strategy, Deterrents 2.0, so that we are not being purely defensive, that there is an offensive capability and that our adversaries understand that and that there is some kind of risk involved with their continuing to prod our grid.

I really appreciate the testimony here today and look forward to working with you. If you have suggestions or input how we can—and I take your suggestion, Mr. Bardee, that FERC should be part of that committee that analyzes what the labs and the utilities come up with. So, I think that's a good suggestion. We will add that to the bill.

Thank you.

Thank you, Gentlemen.

Senator GARDNER. Thank you.

Senator Franken.

Senator FRANKEN. Thank you, Mr. Chairman.

Earlier this month, President Trump released his budget blueprint which calls for an overall cut of $1.7 billion to the Energy Department. The budget slashes investment in both basic and applied energy research and development, including the complete elimination of ARPA-E.

More broadly, these cuts would threaten the expertise found at our national labs, a resource that is the envy of the world. One of the programs specifically mentioned for significant cuts is the Office of Electricity Delivery and Energy Reliability. Now, both our national labs in the Office of Electricity are engaged in critical work regarding cybersecurity.

Mr. Di Stasio, your testimony mentions close coordination between your industry and the DOE Office of Electricity. Can you elaborate on that collaboration and what severe cuts to that office would mean from an industry perspective?

Mr. DI STASIO. Yes, Senator.

We've worked closely with the Office of Energy Delivery and Reliability, both on the development of smart technologies to advance smart grid and so forth, but also on reliability risks related to cyber.

It was mentioned earlier one of the acronyms of CRISP is essentially a tool to allow the triangulation of threat trends across multiple systems versus individual systems dealing with it by themselves, and we worked with the Office of Energy Delivery and Reliability to help better understand that and also to get it with our members so that we could get more folks to join up.

We have also worked closely, their office has been instrumental, in developing the request that came out of the FAST Act that was passed in 2015 that directed us to have an essential transformer spare system and also to deal with transportation.

Senator FRANKEN. How is that working?

Mr. DI STASIO. Well, it's yet to be communicated back to the office.

Senator FRANKEN. Because we had the physical assault on the transformers and——

Mr. DI STASIO. Well, so the issue is that there's a discreet number of very large transformers that pose, kind of, a disproportionate impact on the grid, should they be impacted. And actually, an analysis, and I was complementing Dr. Zacharia, was done by Oak Ridge labs to identify what the threat landscape looked like in utility planning terms. That technical analysis then went to DOE, who in fact, is then supposed to come back to Congress, through House Energy and Commerce, to provide a report on what we should do. So those are just two examples where this office has been a critical interface for us as utilities, with the Federal Government and that capacity. If it didn't exist in that office, it needs to exist somewhere because it's very important work.

Senator FRANKEN. So, again, what do these kinds of Draconian cuts, what will that mean to your work, Mr. Fowke?

Mr. FOWKE. I don't know, Senator, but I can give you a definitive answer on that. I know the research is important and if these budget cuts cut some of the research out that we're talking about here, I think the whole——

Senator FRANKEN. They are going to.

Mr. FOWKE. ——would suffer for it.

Senator FRANKEN. Okay.

The majority of severe power outages are weather related. Heat waves diminish the performance of our electrical system and at the same time cause extreme loads as people run their air conditioners. Droughts cause outages because they impact lower hydropower reserves and smaller supply of cooling water for coal and nuclear plants. Hurricanes and flooding can cause widespread outages, damaging both the grid and generation facilities.

The Transportation bill we passed in 2015 provides the Energy Secretary with the authority to address grid-related security emergencies caused by cyberattacks, physical attacks, electromagnetic pulses or geomagnetic disturbances. Conspicuously, conspicuously absent is the biggest actual threat to the grid, outages by extreme weather which we will be seeing more as climate changes.

The recently released Quadrennial Energy Review notes that cyber terrorists are likely to use natural disasters as force multipliers, to quote the report, "By timing grid attacks to correspond with natural disasters, intelligent multi-site attacks by knowledgeable attackers targeting the specialized components, could result in widespread, long-term, power outages from which it could take several weeks to recover."

How well is your industry prepared to deal with multiple, simultaneous problems? How might timing a cyberattack to correspond with a weather-related problem amplify the impact of the attack?

That is for anyone.

Mr. FOWKE. Senator, I think that's a great question, and I think it would be naive to think that the bad guys would only attack us on a good day.

And so, what our industry is drilling constantly around is exactly that, a physical or a storm outage, natural disaster, combined with a cyberattack because if you then take out communications you start to get to a situation where you're not sure if it's cyber or if it's physical or if you can count on the signals that you're getting from your grid.

So, it gets back to how do we operate this grid blind? How do we coordinate with each other? How do we assume the telecom, telecommunications will be operating?

We did it an elaborate grid exercise a couple years ago, and I think we learned a lot. But I think we also found that there's a lot of resilience built into the grid too. But we can't drill enough on that.

Senator GARDNER. Senator Heinrich.

Senator HEINRICH. Thank you, Chairman.

For either or both, Mr. Fowke or Mr. Di Stasio, one of the issues we follow very closely on the Intelligence Committee is how we monitor individuals that are suspected of being already involved in terrorist activities. You can imagine these are exactly the people that you do not want running your critical control centers.

What personnel controls does the utility industry have in place when conducting security clearances, background checks, and do you think they are sufficient? In addition, are there additional federal resources, like the FBI's Terrorist Screening Center, that could potentially improve that process for the industry, if you had access to those?

Mr. DI STASIO. Senator, that is a concern because the human resources element of cyber is a significant risk as well.

Most all of us, by requirements of standards and also our personnel policies, make sure that we tightly control ingress and egress. We do have advanced background checks for certain sensitive classifications.

I will say in the recent past our national association, the American Public Power Association, as well as others, have been working with the FBI to get access to advanced background screening for certain personnel. And that language is being considered and developed now.

Senator HEINRICH. Great.

Mr. DI STASIO. I think, I do think, it's an important point not to overlook that while some progress has been made, more needs to be made and especially given the fact that there's diversity of state policy around this.

Again, I represent municipal utilities, so we also have different sunshine laws in different states and different statutes.

Senator HEINRICH. Yes.

Mr. DI STASIO. And so, trying to harmonize all of that into something coherent is a fairly significant undertaking. But it is on the radar screen, if you will, as how to best deal with some of the human resource issues.

Senator HEINRICH. Mr. Fowke, I believe you mentioned the time-based challenge of getting security clearances. Was that you?

Mr. FOWKE. Yes.

Senator HEINRICH. The bottleneck there, is it personnel or funding to do the analysis for those clearances and is that all on the Federal Government side of the ledger?

Mr. FOWKE. Well, it's an elaborate process, as you know, and so I think it's a time-based manual effort. It's the manpower which translates to the funding, I would assume.

Senator HEINRICH. If that funding is reduced over the course of the budget process, what would that mean for being able to adequately manage that risk?

Mr. FOWKE. Well, if the funding came out of that aspect of the security clearance, then I would suspect it would slow it down. And right now, as I mentioned, it's six to eight months.

Senator HEINRICH. Pretty slow as it is.

Mr. FOWKE. Yes.

Senator HEINRICH. Okay.

Mr. Bardee, I am pretty excited about FERC's proposed rule on energy storage and distributed energy resources, participating in organized wholesale markets. With these additional players from the distribution side participating in the bulk power market, does the Federal Power Act provide FERC sufficient authority to assure both security and reliability of the grid?

Mr. BARDEE. Senator, that's an issue we need to do more work on.

Those types of resources bring value to the markets because they diversify our sources of supply, but at the same time, ensuring that the grid can be operated reliably by having visibility of what those resources will do under certain circumstances and having control, if necessary, is difficult under the structure we have now where FERC is responsible for the Bulk-Power System and states are responsible for the local distribution systems that many of these resources connect to.

So, I think we are very much looking at that issue, trying to be creative about ways we can address that issue. And I know the industry is too, because they're as much focused on that issue as we are. Solutions are not easy though.

Senator HEINRICH. I think that is going to be particularly important. It is pretty clear that that is the direction markets are headed.

And I think we are going to see more DERs. We are going to see more demand response. We are going to see more storage. All aggregated in, you know, spread across the grid and getting the rules of the road worked out at the front end rather than responding to issues as they arise is going to be particularly important.

Thank you, Mr. Chairman.

Senator GARDNER. Thank you very much.

If members want to stick around, we will go ahead and have another round of questions, if you do not mind.

I wanted to just highlight a couple of things based on what has already been brought up.

Mr. Fowke, you mentioned you have about 100 people working in cybersecurity or security areas where just a short time ago you didn't really have any. Is that correct?

Mr. FOWKE. That's correct.

Senator GARDNER. Mr. Bardee, how many people at FERC have expertise in cyber?

Mr. BARDEE. On my staff, about 25 and in other places, maybe another 20.

Senator GARDNER. And what is the total staff?

Mr. BARDEE. Total staff of the agency is about 1,400.

Senator GARDNER. Fourteen hundred.

What would it have been two or three years ago?

Mr. BARDEE. Cybersecurity was a smaller part. If you went back several years, a very small part.

Senator GARDNER. Yes.

Mr. Di Stasio, the Cyber Mutual Assistance Program that you talked about in your testimony and others talked about in their testimony, 10 years ago today in Holly, Colorado, there was a tornado, a very devastating tornado. We saw a lot of utilities from around the region, around the country, come together to fix the physical damage that had occurred, the power lines, the telephone poles, utilities, you name it.

This Cyber Mutual Assistance Program seems to be the same thing, but in a digital sense. But yet, we seem to only have about 100 members participating today out of the 3,000 utilities in the country. Why is that? Why don't we see more people involved?

Mr. DI STASIO. I think, Senator, or Chairman, I think it will continue to grow. The reality is across those 93 utilities that are current members to the Cyber Mutual Assistance Task Force, they probably represent a significant number of customers in states.

And again, if you think about this issue of prioritizing the risk, just as we've done with NERC where we have both high, medium and low risks and as Mr. Bardee mentioned, we're now getting to the low risks, but the high and medium have been addressed first. And I would suggest that we could certainly provide it in the record the numbers of customers and systems that are represented across those 93. So, it's not a straight calculation.

Senator GARDNER. Thank you.

Mr. Bardee, Mr. Fowke, in terms of the numbers of people working in cyber, is there a workforce need that you see that Congress could help with in terms of developing a greater workforce in cyber?

Mr. FOWKE. Well, it's not an easy position to fill, I can tell you that, Mr. Chairman. And where we are typically filling it or quite often we're filling it for the military ranks. It's one of the things we're focused on at Xcel Energy, just on the broad sense.

But I think a program within the military that would help transition vets to civilian and give them those cyber type training, that they will be able to apply in the civil world, would be an absolutely great program. If you think about it, many of them already have a security clearance, as some of the other problems that I was suggesting that could be readily transferred over, it's my understanding. So, that, to me, is a great opportunity.

Senator GARDNER. Thank you.

Dr. Zacharia, exascale computing is the next big step in advanced computational research efforts led by the DOE labs. Would these expanded national lab capabilities enable critical infrastructure cyberattack scenario evaluation and protection plan evaluation? And if so, could you talk about the labs that would be involved in that exercise?

Dr. ZACHARIA. Thank you, Mr. Chairman.

Exascale computing program is actually a program that is led by multiple laboratories. The leadership is actually six labs and Oak Ridge National Laboratory has a responsibility to deliver the project.

One of the things that the department has done in terms of deploying the exascale is simultaneously there is a program to deliver up the applications that will run on these machines when these machines are deployed.

And so, these are, sort of, called codex signs and in the area of cybersecurity there are a number of such programs that have been started, like typically what DOE Office of Science does, is that there is RFP and the peer review, call for proposals peer review, and the selection of the best proposals.

And I can tell you that in the area of cyber there is a co-design project that is led by your laboratory, the National Renewable Energy Laboratory.

Senator GARDNER. Could you say that again? I am sorry, what was that?

[Laughter.]

Dr. ZACHARIA. I think one of her finest actually is the Director of NREL, so NREL and PNNL are co-leading that activity for us, for the exascale computing project, and it's really critical.

And if I may add, Senator, early on there was a discussion about the Office of Electricity. One of things that the Office of Electricity, one of the programs that they have is EAGLE-I, which is a situational awareness program that actually gets information in a region that services about 100 million users.

The other thing that exascale computers allow you to do is to take that information, real time, digest that information and be part of a proactive way of both understanding the vulnerability of the grid as well as unloads on that so you can make preventative measures and be aware, grid aware strategy, for cybersecurity.

Senator GARDNER. Great. Thank you.

Senator Cortez Masto, if you would like to go a second round?

Senator CORTEZ MASTO. Thank you, Mr. Chair.

And very quickly because, obviously, this is a complicated, complicated issue that we are dealing with here, and I am struck by what I am hearing. Mr. Fowke, I think you said it clearly in your speaking points when you said the national policy on cybersecurity is uncoordinated and unfocused. That has been my concern from a state perspective watching what is happening.

I am curious, and I am going to open this up to the panel. Is there a model out there? Is there something that we should be looking at that the states may have come up with that is a great model for us to be looking at at the federal level? Or is there something that you can give us hope where we should be looking to address cybersecurity in general across this country?

Mr. FOWKE. I think we should look at state level. I think that the fusion centers that you might have heard about, Senator. I think they can work very well.

I also think we ought to look overseas. I mean, there are nations, albeit, much smaller than the USA that, I think, coordinate much better than we do in the United States. And I think we should be open to best practices wherever they are.

Senator CORTEZ MASTO. Thank you.

Mr. DI STASIO. Senator, one of the things that we also got a lot of value out of was undertaking after a Presidential Order or Directive in 2014, to talk about coordination across the federal agencies.

We responded to that and developed what was called, and worked with DOE, actually, on what was called a maturity model.

And so, part of that is, I think, we would prefer to—we've got a very robust cyber compliance and enforcement program through the NERC standards, directed by FERC. We would like to be able to build upon that regime.

We also talked about the Electric Subsector Coordinating Council, the work with DOE, the work with DHS, some of the suggestions in S. 79.

I do think we've come a long way. We certainly have a greater ways to go, but I feel like we've got some of the essential building blocks in place dealing with some of these things like clearances, timely and actionable information sharing and the work that the labs can do to enhance situational awareness. All of those, to me, provide the next rounding out of the current state of mitigation of these risks.

Senator CORTEZ MASTO. Thank you. I appreciate the comments. Thank you, Mr. Chair.

Senator GARDNER. Senator King.

Senator KING. I have a very quick follow-up on that.

Is there a central clearinghouse of hacks where there is one place where a grid operator can look and say, okay, here is what is going on in Pennsylvania? Here is what is going on in California? Is there a central website? I hesitate to use the term because maybe that is not what you want in this situation, but someplace where this—I am after how good the communication and coordination really is.

Mr. DI STASIO. The place that's most closely associated with that type of a description is really the E-ISAC which is the information center and clearinghouse. They actually——

Senator KING. Is that government or is that private sector?

Mr. DI STASIO. It's government, and they actually have a watch floor program that operators can go and participate. I've actually had the opportunity to go in there myself. And they look at a variety of, not just cyber, but all types of potential threats and disruptions to the grid and that becomes, probably, the most robust information sharing source we have.

Mr. FOWKE. I might just add, I think, the gold standard for ISACs is the FS-ISAC. That's the financial services ISAC, and they actually are now talking machine to machine. It's much more private sector versus government-oriented.

But we recently joined it and we were the first electric utility to do that. I think there will be more because it's one more channel and one more sector coordination, where we talk about coordination, that's right available to us and we're already getting good information from that.

But to me, it also pushes the issues that I've been saying before, we're not, not only it's federal agencies not coordinating. We're not coordinating across sectors as well as we should too. And these ISACs, if they were better coordinated together, I think that would be a great opportunity.

Senator KING. I think that is a very good point because if there is going to be an attack it probably will not be just one sector, it

could be electricity, gas, financial and coordinating across sectors, I think, would be very important.

Mr. Chairman, I want to thank you for this hearing, and I want to thank our witnesses.

This has been very illuminating. Hopefully our discussion doesn't have to end today. As you are going home and you think, I should have said this or here is a suggestion, please pass it back to the Committee because this is an area of absolutely vital concern and could not be more important to the people that we all represent. So thank you very much for your testimony.

Thank you, Mr. Chairman.

Senator GARDNER. Thank you.

The good news is for all of you the record will remain open for two weeks if you would like to add that additional thought.

For the information of members, questions for the record are due tomorrow by close of business, and we would appreciate your responses as soon as possible.

A final question, or maybe comments, if I could, starting with you, Mr. Bardee.

As we close this hearing today, and I do truly appreciate your time and testimony today because this is a very useful exercise as we learn more about the problem ourselves and challenge ourselves and try to do our best to coordinate the moving pieces of this.

If each of you could give one or two things to summarize your top recommendations of Congressional action that would enhance our grid cybersecurity preparedness or response capabilities, what would it be? You have talked a lot about it here at the hearing, but maybe you can summarize that again, the top two recommendations.

Mr. BARDEE. I think from my perspective dealing with electric reliability. One of them is actually bills like S. 79, ensuring that we can get the research that it is difficult for the private sector to commit as much in the way of resources for.

Senator GARDNER. Thank you for that.

Mr. BARDEE. And the other would be if there are ways to improve the kind of personnel training that Mr. Fowke was discussing earlier to get us people who have skills, not just in cybersecurity, but also in power system engineering. Those people are very valuable.

Senator GARDNER. Mr. Fowke?

Mr. FOWKE. Well, I said a lot about information sharing so I'll say something I didn't say yet. We talk about sophisticated cyberattacks and they are growing, but you know how most attacks occur? Not following basic cyber hygiene. And that's how a lot of this gets started. So I think we need to start thinking about how we can educate and, I dare say, mandate some basic cyber standards across industry and government which, I think, is long overdue.

Senator GARDNER. Mr. Di Stasio?

Mr. DI STASIO. I would suggest that we build upon the regulatory framework and the coordination that is starting to occur. We have been at this for 10 years and I will say 2009 in the House, I testified on the Grid Act. And we have come a very long way since then but still have quite a bit to do.

But if we could deal with some of the issues that have been mentioned around clearances, human resource training, getting a certain level of maturity and understanding of the risks and then increase coordination with the government, whether that becomes through some consolidation of jurisdictions or whether we do it as we have.

Senator GARDNER. Dr. Zacharia?

Dr. ZACHARIA. Let me echo the sentiment I think that the Senate bill 79 has it exactly right. In that based on our experience with working with the Electric Power Board Utility in Chattanooga, I think having a pilot where you bring together the Federal Government, industry and the national laboratories, the best of these three entities together to have a two-year pilot to really explore what is possible to get out in front of this evolving challenge is probably the best thing that we can do because bringing those three players together, getting them to work together, share information, understand each other's both capabilities and challenges, I think would allow us to make significant progress.

So, thank you very much for this opportunity.

Senator GARDNER. Well, thanks again to members of the Committee. As I said, the QFRs are due tomorrow by close of business.

We appreciate your time and testimony today.

With that, we will adjourn the Committee.

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

APPENDIX MATERIAL SUBMITTED

II

115TH CONGRESS
1ST SESSION

S. 79

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

JANUARY 10, 2017

Mr. KING (for himself, Mr. RISCH, Mr. HEINRICH, Ms. COLLINS, and Mr. CRAPO) 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 180 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) partnering with covered entities in the energy sector (including critical component manufacturers in the supply chain) 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, in partnership with covered entities, 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 non-digital 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.

○

FEDERAL ENERGY REGULATORY COMMISSION
Washington, DC 20426

Office of Electric Reliability

April 18, 2017

The Honorable Corey Gardner
Chairman
Subcommittee on Energy
Committee on Energy and Natural Resources
United States Senate
Washington, D.C. 20510

Dear Chairman Gardner:

Thank you for the opportunity to testify on March 28, 2017 before the Subcommittee on Energy on the subject of cybersecurity threats to the U.S. electric grid and technology advancements to minimize such threat and on S. 79, the Secure Energy Infrastructure Act. Enclosed are responses to the post-hearing questions the Subcommittee has asked that I answer.

Should you require additional information, please let me know.

Sincerely,

Michael A. Bardee
Director, Office of Electric Reliability

QUESTIONS FOR MR. BARDEE
03.28.17 Subcommittee on Energy

FROM SENATOR CANTWELL

In the second installment of the Quadrennial Energy Review (QER) issued in January, 2017, the Department of Energy noted that electricity generation has become much more reliant on natural gas being delivered by natural gas pipelines.

The QER stated: "DOE, pursuant to FAST Act authorities and in coordination with FERC, should assess current cybersecurity protections for U.S. natural gas pipelines and associated infrastructure to determine whether additional or mandatory measures are needed to protect the electricity system. If the assessment concludes that additional cybersecurity protections—including mandatory cybersecurity protocols—for natural gas pipelines and associated infrastructure are necessary to protect the electricity system, such measures and protocols should be developed and implemented. This work should build on existing assessments, including those underway at the Transportation Security Administration."

1. **What role does FERC currently have with respect to cybersecurity of natural gas pipelines?**

Response

FERC currently possesses rate-making authority and certificate authority for interstate natural gas pipelines while the Transportation Security Administration (TSA) has primary authority over pipeline security, which includes cybersecurity. FERC and TSA have developed a joint, voluntary assessment program to conduct in-depth cybersecurity reviews of pipeline entities. TSA staff and FERC staff completed two "architectural reviews" of cybersecurity for natural gas pipelines in the past 10 months.

Separately, the North American Electric Reliability Corporation (NERC), the FERC-certified Electric Reliability Organization, recently announced a new effort to improve coordination on potential security risks related to critical electricity and natural gas pipeline infrastructure. The effort involves cooperation between the Downstream Natural Gas Information Sharing and Analysis Center (DNG-ISAC) and Electricity Information Sharing and Analysis Center (E-ISAC). The E-ISAC, although operated by NERC, functions as an independent group and is organizationally isolated from NERC's processes.

2. **Should natural gas pipelines have additional or mandatory cybersecurity standards?**

Response

Congress and TSA are in the best position to evaluate TSA's current natural gas pipeline security authority to determine if natural gas pipelines should be subject to

additional or mandatory cybersecurity standards. TSA currently has the authority to establish mandatory cybersecurity regulations for natural gas pipelines.

3. **Should an assessment be performed of current cybersecurity protections for U.S. natural gas pipelines and associated infrastructure to determine whether additional or mandatory measures are needed to protected the electricity system?**

Response

The TSA has oversight authority of the cybersecurity of the U.S. natural gas pipelines and would better be able to answer the question as to whether additional or mandatory measures are needed at this time. However, an assessment by the Department of Energy could also help inform any decision on the need for additional and/or mandatory standards for natural gas pipelines. Should such an assessment be conducted, FERC would offer support for that effort.

FROM SENATOR MANCHIN

In the aftermath of the attack on the Pacific Gas & Electric substation in Metcalf, California – the Federal Energy Regulatory Commission required NERC (the North American Electric Reliability Council) to propose standards requiring transmission owners to address physical security risks and vulnerabilities that could impact the reliable operation of the grid. In 2013, another attack in Arkansas illustrated the grid's potential vulnerability to carefully planned physical attacks to equipment essential to keeping the lights on. The FBI arrested a man in Lonoke County Arkansas for several attacks on the transmission grid, including deliberately setting fire to Entergy's 500 kV substation.

1. **Please share your perspective on to the seriousness of the attacks and, based on this experience, what emerging technologies, if any, are primed to protect against physical attacks on the grid?**

Response

The referenced attacks on the Bulk-Power System are serious and could potentially have resulted in instability, uncontrolled separation, or cascading outages within the interconnection. The seriousness of these attacks was highlighted by the response by the federal government and private sector. Since the NERC Reliability Standards at the time of the Metcalf incident did not fully address physical security, FERC directed NERC to create a new reliability standard, CIP-014-1, which was approved by FERC in November 2014. The purpose of CIP-014-2, the current version of the mandatory and enforceable standard, is to enhance physical security measures at critical Bulk-Power System facilities (i.e., stations and substations) and thereby lessen the overall vulnerability to physical attacks.

QUESTIONS FOR MR. BARDEE
03.28.17 Subcommittee on Energy

There are various methods and new technologies that can be utilized by transmission owners and operators to enhance physical security at critical Bulk-Power System facilities. NERC Reliability Standard CIP-014-2 is technology-neutral; further, FERC staff does not recommend specific technologies. FERC staff, however, is aware that many transmission owners and operators have been enhancing the physical security posture at their critical Bulk-Power System facilities through various means, including through improved security measures and actions to improve the resiliency of the Bulk-Power System.

In addition to FERC's actions related to the NERC Reliability Standards, it also provides assistance to the industry and other agencies with the identification and application of best practices for physical security measures. In collaboration with federal partners, FERC supports analysis and targeted outreach to identify, develop, and share information on threats and vulnerabilities with its jurisdictional infrastructure stakeholders and state public utility commissions.

United States Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing on March 28, 2017
Cybersecurity Threats to the U.S. Electric Grid
and Technology Advancements to Minimize such Threats and to Receive
Testimony on S. 79, the Security Energy Infrastructure Act
Question for the Record Submitted to Mr. Benjamin Fowke III

Question from Senator Joe Manchin III

Question: In the aftermath of the attack on the Pacific Gas & Electric substation in Metcalf, California – the Federal Energy Regulatory Commission required NERC (the North American Electric Reliability Council) to propose standards requiring transmission owners to address physical security risks and vulnerabilities that could impact the reliable operation of the grid. In 2013, another attack in Arkansas illustrated the grid's potential vulnerability to carefully planned physical attacks to equipment essential to keeping the lights on. The FBI arrested a man in Lonoke County Arkansas for several attacks on the transmission grid, including deliberately setting fire to Entergy's 500 kV substation.

Please share your perspective on to the seriousness of the attacks and, based on this experience, what emerging technologies, if any, are primed to protect against physical attacks on the grid?

Answer: We take the physical security of our infrastructure very seriously; the Metcalf and Arkansas incidents underscored the evolving nature of the threat. Xcel Energy has an integrated cyber and physical security program that we continuously improve in order to protect our critical infrastructure. Our industry is subject to mandatory physical standards set by the North American Electric Reliability Corporation (NERC) under Critical Infrastructure Protection Standard 14 (CIP-014). This standard requires identification of critical facilities, evaluation of potential threats and vulnerabilities, and the development of a risk-based physical security plan that has been independently verified by a third-party. CIP-014 is a step in the right direction, but Xcel Energy is going beyond mandated standards by deploying advanced technology with a particular focus on improving access control, surveillance, and data analytics. We continue to evaluate potential technology that could help address physical and cyber threats.

CELEBRATING 30 YEARS
LPPC
LARGE PUBLIC POWER COUNCIL

April 11, 2017

The Honorable Cory Gardner
Chairman, Subcommittee on Energy
Committee on Energy and Natural Resources
304 Dirksen Senate Office Building
Washington, D.C. 20515

The Honorable Joe Manchin
Ranking Member, Subcommittee on Energy
Committee on Energy and Natural Resources
304 Dirksen Senate Office Building
Washington, D.C. 20515

Dear Subcommittee Chairman Gardner and Subcommittee Ranking Member Manchin,

On behalf of the Large Public Power Council, thank you for the opportunity to testify at the Senate Energy and Natural Resources Subcommittee on Energy's hearing on March 28th regarding industry efforts to engage on cyber security. Per your request, we are providing the following comments for the record in response to questions posed during and following the hearing.

During the hearing Subcommittee Chairman Gardner asked how to engage more utilities in the Electricity Subsector Coordinating Council's (ESCC) Cyber Mutual Assistance (CMA) Program. I would like to provide for the record the following information gathered by the Edison Electric Institute:

> CMA participating utilities are serving approximately 80% of all US electricity customers. By counting utilities that serve customers within the United States, and excluding Independent System Operators (ISOs), Regional Transmission Organizations (RTOs) and Canadian entities, EEI determined that there are over 118 million customers represented by utilities that participate in CMA. In fact, the impact and reach of CMA is significantly higher than that, given the level of participation by ISOs and RTOs who do not directly serve end-use customers.

We believe the CMA provides significant value to utilities and their customers, and we support efforts to engage utilities in this voluntary program.

Following the hearing, citing attacks in California and Arkansas, Subcommittee Ranking Member Manchin asked for our perspective on the seriousness of these attacks and, based on these experiences, what emerging technologies, if any, are primed to protect against physical attacks on the grid. The physical attacks to the grid in both California and Arkansas were cause for great concern. These attacks raised concerns to a heightened level due to their sophistication and potential for wide-spread damage.

For physical attacks, and more recently cyber attacks, the electric industry does have a well-developed and robust information sharing framework. Through tools like the North American Electric Reliability Corporation (NERC) Electricity Information Sharing and Analysis Center (E-ISAC) Portal and the Department of Homeland Security Critical Infrastructure sector program, grid operators share information with local, state and federal law enforcement as well as other industry

partners. Comprehensive post-incident analysis related to physical attacks has been conducted in order to raise vulnerability awareness and to prevent similar attacks. These analyses are shared, through a variety of industry forums.

The NERC Physical Security Reliability Standard (CIP-014-2) directed by the Federal Energy Regulatory Commission (FERC) in a March 7, 2014 Order requires the identification and protection of transmission stations and transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or cascading within an interconnection.

The purpose of the Standard is to enhance physical security measures for the most critical Bulk-Power System facilities and thereby lessen the overall vulnerability of the Bulk-Power System facilities against physical attacks. The Standard became effective in October 2015. Specific security practices and technologies were not prescribed by the Standard; however, assessments did focus on security strategies designed to detect, deter, delay and respond to incidents.

Most hardening involves a combination of enhanced physical barriers, such as larger walls preventing visibility into critical sites. Another common measure is controlling proximity and access through secondary perimeters and controls. Technology is also deployed to protect assets. Advanced intrusion detection systems, video surveillance cameras with thermal video and analytic capabilities are used regularly to enhance physical security. In some cases, increased security patrols or a physical security presence at the site are utilized. Some combinations of these techniques, along with increased coordination with law enforcement, serve to reduce the risks of physical attacks. Finally, many grid operators are building security into their system design protocols configuring or separating their systems to build redundancy.

Lastly, during the hearing witnesses were invited to provide additional feedback on S. 79, the Security Energy Infrastructure Act. We would like to echo comments made by Mr. Michael Bardee, Director of the Office of Electric Reliability at FERC, for the inclusion of FERC in the working group established by S. 79. We believe the studies set forth in S. 79 would benefit greatly by the inclusion of FERC.

Thank you again for the opportunity to testify, and we look forward to continued dialog on these critical issues.

Sincerely,

John Di Stasio
President
Large Public Power Council

United States Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing on March 28, 2017
Cybersecurity Threats to the U.S. Electric Grid and Technology Advancements to Minimize such Threats and to Receive Testimony on S. 79, the Security Energy Infrastructure Act
Questions for the Record Submitted to Dr. Thomas Zacharia

Questions from Chairman Lisa Murkowski

Question 1: In your statement, you described how "ORNL researchers have developed highly secure Internet of Things (IoT) sensors and systems specifically designed to provide enhanced measurements for improving electric grid operations." Further, you explained that such, "devices have been installed at Chattanooga Electric Power Board (EPB) substations and are providing extended grid operation measurements to EPB's control center." Regarding those statements:

a. Can you provide more detail on the IoT devices, "designed to provide enhanced measurements for improving electric grid operations?" Specifically, what devices are being considered for installation across the grid?

b. What types of IoT devices should we expect to be available for grid operations over the coming ten years?

c. How can ORNL (and other DOE labs) assist industry in ensuring that such devices are secure against cyber threats?

ANSWER:

a. Can you provide more detail on the IoT devices, "designed to provide enhanced measurements for improving electric grid operations?" Specifically, what devices are being considered for installation across the grid?

ORNL has developed low-cost IoT devices designed to provide enhanced awareness of the equipment and systems operating within the energy infrastructure. These IoT devices work through a "sensor suite" package that currently monitors 17 different parameters including meteorological measurements, cellphone signal presence, electric and magnetic fields, solar irradiance, and the presence of certain drones. They are deployed within substations or any other location in the utility with communications connectivity.

These devices are inexpensive and provide measurements with sufficient precision to be useful for triggering alarms and alerts – meeting the sensing needs of utilities. Device components include microcontrollers with sufficient computational capabilities to allow intelligent pre-processing of multiple measured values. Associated components handle the communications requirements using wireless, optical fiber, or traditional Ethernet. The enclosure is a lockable, weather-tolerant design with suitable ingress/egress characteristics. An overarching design goal is the development of an affordable system that provides multiple parameters useful to the host utility. This information will enable operators to take appropriate actions in response to system events, and ultimately will be used by automatic control schemes.

United States Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing on March 28, 2017
Cybersecurity Threats to the U.S. Electric Grid and Technology Advancements to Minimize such Threats and to Receive Testimony on S. 79, the Security Energy Infrastructure Act
Questions for the Record Submitted to Dr. Thomas Zacharia

A photograph of the sensor enclosure with accompanying communications network media converter (optical fiber to wired Ethernet or secured 900 MHz WiFi) is provided as Figure 1.

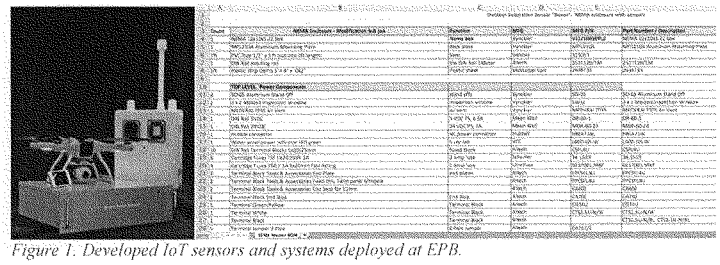


Figure 1. Developed IoT sensors and systems deployed at EPB.

In answer to the second part of question a, namely: *Specifically, what devices are being considered for installation across the grid?*

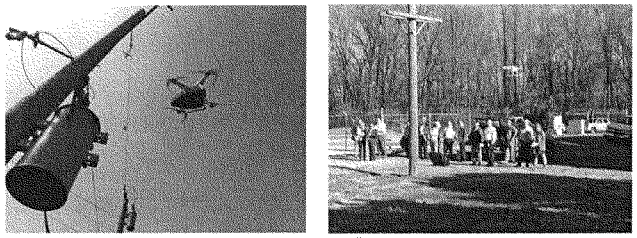
In addition to the fixed systems, utility representatives have expressed a need to have similar sensing capabilities on a mobile platform (truck or drone). To date, ORNL has flown and tested a drone carrying subset of the sensing system at EPB's Training Site (de-energized lines) as a proof of concept.

Representatives of the National Rural Electric Cooperative Association, which represents the interests of more than 900 electric cooperatives in the United States, and a number ofseveral their member electric co-operatives, visited Chattanooga to participate in proof-of-concept trials.

On March 3, 2017, the complete Bill of Materials, reference designs and associated source code were released to the International Society for Automation (ISA) Test & Measurement Division and Communication Division to allow organizations to consider commercializing the systems.

The drone-sensor pod configuration has been tested within EPB's network to monitor various parameters of operational distribution transformers. A photograph of the drone-sensor pod in action is provided as Figure 2. Note that this combination of IP-addressable grid sensors is essentially a "grid-specialized" flying IoT sensor package, meaning the measurements are not stored on board, but transmitted through the EPB core network, thereby allowing individuals within the utility's control center to have real-time access to the data. The same security features

described for the fixed modules apply to the drone-sensor system. Note that the drone-sensor pod was being flown by utility personnel following FAA regulations[1].



(a) (b)

Figure 2. (a) Mobile IoT – drone-sensor pod – taking measurements of an EPB distribution transformer. (b) NRECA and affiliated electric co-operatives flying drones with sensors at EPB Training Site (2016).

ANSWER:

b. What types of IoT devices should we expect to be available for grid operations over the coming ten years?

Within the next 10 years, it is anticipated that sensors and systems such as those just reviewed, will proliferate throughout the electric grid. One way the National Laboratories are contributing to this is through a transition to practice effort under the Grid Modernization activities.

Specifically, from a grid operations perspective, it is anticipated that sensors and systems shown below in Figure 3 will be commercialized and deployed as "IoT grid devices."

[1] A report entitled *"An Early Survey of Best Practices for the Use of Small Unmanned Aerial Systems (UAS) by the Electric Utility Industry", February 2017, was developed by ORNL's UAS Research Center. The manual is available online @* https://ornl.info.gov/sites/publications/Files/Pub73072.pdf

United States Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing on March 28, 2017
Cybersecurity Threats to the U.S. Electric Grid and Technology Advancements to Minimize such Threats and to Receive Testimony on S. 79, the Security Energy Infrastructure Act
Questions for the Record Submitted to Dr. Thomas Zacharia

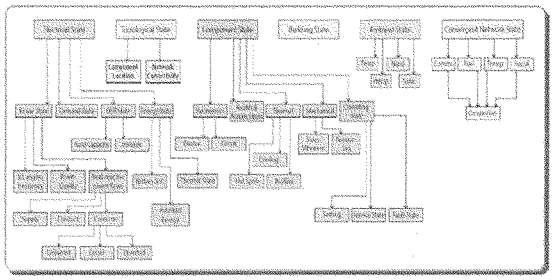


Figure 3. Identified "next generation" extended grid state sensors.

The general area of Internet of Things (IoT) devices versus Industrial IoT (IIoT) devices is hotly debated with numerous organizations and consortia attempting to define IoT/IIoT. IIoT is a specialized version IoT – implemented in ruggedized packages suitable for industrial application environments. IIoT benefits from data flowing through standard-based networks. IIoT systems are in the process of disrupting the ongoing practice of using proprietary networks, and putting into place a common standards-based networking technology.

During a recent Department of Commerce workshop pertaining to the government's role in IoT/IIoT,[2] the convergence of IT technology and OT (operational technology) for industrial automation and utility grid environments was described as well underway. Grid Operations may have a slightly different context with respect to IoT energy monitoring and management systems being deployed in distribution systems at customer sites (large commercial to residential). Examining a complete distribution system as potentially a collection of microgrids – with distributed energy resources located throughout the service area – leads to a significantly expanded set of sensors and systems that are expected to be commercialized in the next ten years. A "utility as a collection of microgrids," as exemplified in Figure 4, is a business model being contemplated by EPB and others. The sheer number of sensors required for optimal synchronization of generation and load in such a system will demand development and integration of data from IoT sensors to the grid operation control centers. The sensors will provide the utility of the future with service area electrical characteristics and customer demographic for individual electric utility assets such as feeders and associated automated switch pairs.[3]

[2] U.S. Department of Commerce Internet of Things (IoT) Workshop September 1, 2016, United States Patent and Trademark Office (USPTO) – Madison Hall.

[3] per J. Ingraham, EPB VP Strategic Research, during a technology review at ORNL, 6APR17

United States Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing on March 28, 2017
Cybersecurity Threats to the U.S. Electric Grid and Technology Advancements to Minimize such Threats and to Receive Testimony on S. 79, the Security Energy Infrastructure Act
Questions for the Record Submitted to Dr. Thomas Zacharia

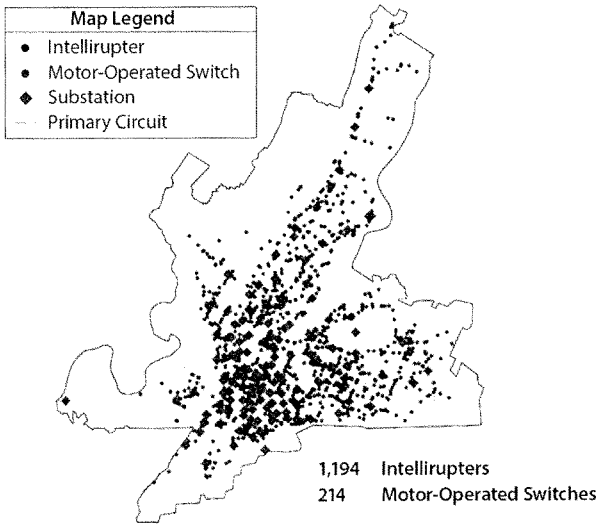


Figure 4. Consideration of the EPB service network as a collection of microgrids.

ANSWER:

c. *How can ORNL (and other DOE labs) assist industry in ensuring that such devices are secure against cyber threats?*

ORNL and other National Laboratories, serving as trusted entities, can assist industry in developing testing metrics and performance fingerprinting with companion testing system designs to be used by the private sector to conduct such tests.

An example of a successful model to follow is one used in the development and standardization of industrial wireless systems. Within this model, DOE sponsored a number of laboratories to participate in development. The security and operational compliance of devices claiming to meet the required specifications would be submitted to a private sector testing organization before being vetted by the end user members – which could include representatives from the petrochemical, chemical, pharmaceutical, and manufacturing sectors[4].

[4] Again, more information is available upon request.

United States Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing on March 28, 2017
Cybersecurity Threats to the U.S. Electric Grid and Technology Advancements to Minimize such Threats and to Receive Testimony on S. 79, the Security Energy Infrastructure Act
Questions for the Record Submitted to Dr. Thomas Zacharia

Note that grid security is different from standard cyber security where there are a multitude of private and governmental organizations willing to test IT cyber systems. The grid represents cyberphysical security (i.e., systems such as the energy grid where physical and software components are tightly interwoven), meaning the use of widespread sensing, communication and control to operate physical devices and systems safely and reliably. In the development of processes and procedures and ensuring that such devices are secure against cyber threats, it is imperative that testing of potential solutions be conducted not in an IT-centric framework, but rather in a system/situation where an operational model/replication of a functioning electric utility is incorporated (i.e., in an operational technology (OT) environment). A few of these types of systems already exist in the DOE National Laboratory complex.

Question 2: You also make five numbered points about, "technological advancements and solutions … needed to ensure a reliable, efficient, resilient, secure grid infrastructure." Regarding those five points:

a. Can you further define the "dark fiber across the United States?" To the extent that it is already owned by electric utilities, should those utilities be using that fiber to carry more of their communications traffic, even if that additional traffic can be carried more efficiently and securely by using other communication carriers? Should utilities be reporting their unused capacity on dark fiber to the government?

b. Regarding the objective of eliminating direct connectivity to the internet, should all corporate functions of a utility be so isolated from the internet, or only systems that control grid assets? If everything were isolated, how would the utility then communicate with their customers, especially on matters like billing, metering, customer usage data, and storm recovery? If those functions were not isolated, then do utilities need to have an "air gap" between operational functions and those corporate functions that communicate with operational functions?

c. How is your point about eliminating direct connectivity to the internet different from efforts today by utilities to minimize their contact points with the internet?
d. Given that the internet is the communications channel for a large proportion of phone and email traffic, how would an electric utility eliminate direct connectivity to the internet and still be able to have its employees use telephones and email?

e. What are the "novel communication security approaches being applied in other sectors" and how would they be "evaluated on the energy infrastructure?"

f. How might ORNL help to assure that IoT devices have "security built in?"

g. To what extent should the CRISP and EAGLE projects be coordinating their efforts with similar work sponsored by DOE or other government agencies? What are the advantages of consolidating programs like CRISP and EAGLE with similar cyber programs, and what are the disadvantages of such a consolidation? In your experience, do similar programs encourage competition in meeting the security needs of industry? Or are multiple programs largely duplicative and a waste of scarce resources?

h. What are "living laboratories?" How have such laboratories been effective in accelerating our ability to defend against threats?

ANSWER:

a. Can you further define the "dark fiber across the United States?" To the extent that it is already owned by electric utilities, should those utilities be using that fiber to carry more of their communications traffic, even if that additional traffic can be carried more efficiently and securely by using other communication carriers? Should utilities be reporting their unused capacity on dark fiber to the government?

Dark fiber is the unlit or unused optical fiber installed across the nation but not yet being utilized. ORNL has performed an assessment of this fiber, and the results were consistent with a report authored by faculty at the University of Wisconsin[5]. The dark fiber across the United States is notionally shown in Figure 5. This diagram also shows the critical grid generation and interconnection assets across the nation. The exact amount of optical fiber owned and operated by utilities is currently not known, however, discussions with fiber asset owners indicate that the inventory is considerable.

[5] "InterTubes: A Study of the US Long-haul Fiber-optic Infrastructure", Durairajan (et al), SIGCOMM '15, August 17–21, 2015, London, United Kingdom

United States Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing on March 28, 2017
Cybersecurity Threats to the U.S. Electric Grid and Technology Advancements to Minimize such Threats and to Receive Testimony on S. 79, the Security Energy Infrastructure Act
Questions for the Record Submitted to Dr. Thomas Zacharia

Figure 5. Notional diagram of dark fiber and the critical grid infrastructure components.

In answer to the question: *"Should utilities be reporting their unused capacity on dark fiber to the government?"* It would be beneficial to obtain this information, possibly with a short questionnaire identifying the type, location, and status of the fiber, dates of installation, ownership, etc.

ANSWER:

b. *Regarding the objective of eliminating direct connectivity to the internet, should all corporate functions of a utility be so isolated from the internet, or only systems that control grid assets? If everything were isolated, how would the utility then communicate with their customers, especially on matters like billing, metering, customer usage data, and storm recovery? If those functions were not isolated, then do utilities need to have an "air gap" between operational functions and those corporate functions that communicate with operational functions?*

There is no definitive answer to these questions because each utility environment is different. However, generally speaking, only the most mission-critical systems should be isolated from the internet. These are usually systems that control the operation of physical assets.

This set of questions directly addresses the Internet dependencies present in utilities of all sizes. A report published in March 2017 entitled "An Assessment of Electric Utilities Dependence on

United States Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing on March 28, 2017
Cybersecurity Threats to the U.S. Electric Grid and Technology Advancements to Minimize such Threats and to Receive Testimony on S. 79, the Security Energy Infrastructure Act
Questions for the Record Submitted to Dr. Thomas Zacharia

The Public Internet," ORNL/TN-2017/188 discusses both business operations dependency and most utilities SCADA system internet dependency.

Discussions with and surveys of many utilities indicate that grid asset control functions and systems may be isolated from Internet traffic and are configured to be far more secure than traditional IT architectures. There is a need for clear definitions of architectures (both physical and logical) – appropriately sized for the various types of utilities. In other words, a "toolkit" consisting of hardware, software, operations architectures, and appropriate business practices to determine the appropriate extent of internet connectivity for each business function needs to be developed.

To the question: *"should all corporate functions of a utility be so isolated from the internet..."* The answer is no, but a logical method for determining the appropriate extent of internet connectivity of utility information (from SCADA to billing to customer usage patterns) needs to be implemented.

Regarding the companion question *"if not isolated, then.."* Cybersecurity needs to go beyond isolation. Air gaps (i.e., physical separation of networks), while commonly used, cannot be relied upon in practice. Having said that, there needs to be a significant change to the "we have a better firewall than you" mentality that is pervasive in the utility vendor view of cybersecurity. Figure 6 depicts an architecture where specific utility operations – and utility-to-utility communications – are shielded from the Internet via a wide assortment of technologies. Referencing Figure 6, note that in a phased approach, initially the protected communications involve generation, transmission and distribution, but specifically not to the residence.

Communications with the customer including billing and utility status reports are handled by the utility with the customer being able to access such information via standard (but further cybersecured) methods. As the cyberphysical security envelope includes the residential meter and from a distribution utility perspective "behind the meter," then the need for further secured bi-directional information flow from that side of the residential meter to the utility needs to occur. This includes a review of the specific security flaws that are in certain vendor-supplied Advanced Metering Infrastructure (AMI) devices and systems.

United States Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing on March 28, 2017
Cybersecurity Threats to the U.S. Electric Grid and Technology Advancements to Minimize such Threats and to Receive Testimony on S. 79, the Security Energy Infrastructure Act
Questions for the Record Submitted to Dr. Thomas Zacharia

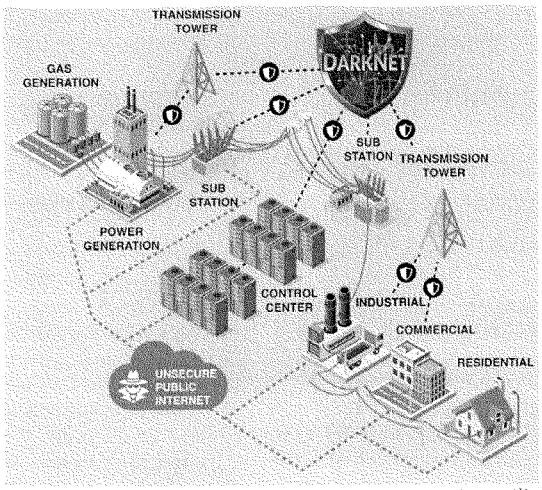


Figure 6. Reference architecture for scaling the project across various utility domains.

ANSWER:

c. *How is your point about eliminating direct connectivity to the internet different from efforts today by utilities to minimize their contact points with the internet?*

The two concepts are similar. ORNL's concept involves minimizing connections to the internet, and assuring that the few connections are not compromised. ORNL's implementation, as presented in Figure 6's reference architecture (from generation to transmission to distribution), is designed to provide a robust suite of tools, technical assistance, and support resources – both in infrastructure deployment and a sustaining tool kit of solutions for ongoing operations.

ORNL's concept is national in scope, not focused on the interests of a single utility, but will offer a range of implementation options that can be incrementally adopted by the utilities as their resources and business models permit. Many large utilities already operate a separate communication architecture for their mission-critical systems, however, many smaller utilities have not taken this approach for various reasons. Advanced cyber concepts developed within the laboratories can enhance the cybersecurity of both of these utility classes.

United States Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing on March 28, 2017
Cybersecurity Threats to the U.S. Electric Grid and Technology Advancements to Minimize such Threats and to Receive Testimony on S. 79, the Security Energy Infrastructure Act
Questions for the Record Submitted to Dr. Thomas Zacharia

ANSWER:

d. Given that the internet is the communications channel for a large proportion of phone and email traffic, how would an electric utility eliminate direct connectivity to the internet and still be able to have its employees use telephones and email?

It is not anticipated that utility-customer communications such as telephone and email traffic will be taken off the public internet. However, it is expected that architecturally – in hardware and database structures – there be a complete separation of that traffic from utility operations information sets.

The complete disconnection of a utility's operations from the public internet is not economical or practical. Rather, it is envisioned that the utilities – individually and collectively - will operate with communications connectivity within "enclaves." For example, the inter-control-center communications will operate within one enclave with certain operational characteristics while another business operations function – such as telephone support – will operate within a separate enclave with different operational characteristics. The various enclaves will function with security and operational characteristics tailored to the criticality of the business processes supported. The design is similar but not identical to the manner in which classified networks are deployed.

ANSWER:

e. What are the "novel communication security approaches being applied in other sectors" and how would they be "evaluated on the energy infrastructure?"

An example of such a "...security approach..." is blockchain (or variants). Blockchains are distributed databases used to record transactions on "blocks" of data/information, and make modification to previously recorded blocks impossible to perform. This enhances the security of the block. This approach is currently being used for HIPAA compliance in patient record transport, in financial transactions, and is being considered for utility use, initially for financial transaction security. Blockchain would be a valuable tool for verification of extended grid state sensor readings prior to being accepted by the utility's SCADA. A concern expressed to ORNL by utilities is the potential for sensors to be spoofed. Using a blockchain concept for sensor-SCADA transmission does not ensure that the reading itself is correct, but it can be used for validating/verifying the message envelope within which the encrypted sensor reading is placed. Note that this is not a replacement for a VPN, but rather a method for sensors deployed in the utility's infrastructure (or the grid itself) to be validated by other sensors.

Evaluation on the energy infrastructure of a concept such as this involves initially modeling the networks, simulating traffic flow patterns from deployed sensors, and verifying that the software

build within the sensor operates according to the rules established for this specific blockchain. A deployment of actual devices within a real-time digital electric grid simulator follows to verify operation, ending in a deployment of actual devices within a segment of an operational utility network.

ANSWER:

f. How might ORNL help to assure that IoT devices have "security built in?"

ORNL considers the cyberphysical system currently being contemplated as defining the rules for operating and integrating the deployed network elements. Assurance of built-in cybersecurity for the grid cyberphysical network may take the form of additional security specifications at the beginning of the product development cycle, along with performance testing of developed system. Specific technologies must be researched for the grid sensors and systems with cyberphysical security being an absolute first principle, not an afterthought to an IoT device.

A survey of the current information on IoT security yields company after company and article after article essentially restating the same old premises: NIST architecture, firewalls, data diodes, password protection, etc. etc. These old premises are simply not working. The daily onslaught of cyber-attacks continues with increased sophistication and increasingly targets industrial and utility systems. A visit to the Consumer Electronics Show (CES 2017, Las Vegas, January) showed hundreds/thousands of IoT devices meant for home automation, home security, energy management, vehicle systems, etc. In the majority of instances, security was an afterthought to the developed device. Today, no identifiable actual standards exist for IoT let alone cybersecurity of IoT devices.

ANSWER:

g. To what extent should the CRISP and EAGLE projects be coordinating their efforts with similar work sponsored by DOE or other government agencies? What are the advantages of consolidating programs like CRISP and EAGLE with similar cyber programs, and what are the disadvantages of such a consolidation? In your experience, do similar programs encourage competition in meeting the security needs of industry? Or are multiple programs largely duplicative and a waste of scarce resources?

While CRISP focuses on network traffic, EAGLE-I is providing situational awareness of the electric system including information such as status of outages throughout the country. By combining these tools, the linkage between cyber incidents and impacts on the nation's grid could potentially be linked, creating a capability that currently does not exist. Having different approaches to situational awareness across the energy infrastructure may provide more

innovative concepts to meet industry security needs. However, if this approach is taken, it should be a deliberate approach coordinated at the appropriate level.

ANSWER:

b. What are "living laboratories?" How have such laboratories been effective in accelerating our ability to defend against threats?

Living laboratories are defined as components and systems within utilities that are available for select cyberphysical security testing. An example is EPB allowing the IoT sensors and systems mentioned earlier in this document to be deployed within their network, but on an isolated segment. After a series of tests, the devices were then brought step by step closer into the operational utility with performance validation/verification testing occurring at each step. That activity and interaction with EPB exemplifies ORNL's definition of a living laboratory.

Question 3: In your statement, you describe how, "ORNL is researching unique methods and technologies to harden the grid and its supply chain against harm, whether intended or not." Specifically, you describe "Fingerprinting" to monitor device behavior at the chip level. This technology could help, "identify the presence of malware or attempts at spoofing that could cause harm to critical infrastructure." On the topic of Fingerprinting:

a. What are the "fingerprinting technologies" that monitor device behavior?

b. Does fingerprinting technology have any potential application for the IoT? How?

ANSWER:

a. What are the "fingerprinting technologies" that monitor device behavior?

Fingerprinting technologies measure physical aspects of the performance of individual electronic components that make up devices (e.g. threshold voltage, voltage offsets, leakage currents, etc.). Because of manufacturing variability, every device has a unique set of measurements for the performance of the components. Fingerprinting variation in the performance or matching of two or more devices (threshold voltage matching, current matching, etc.), and specific performance of larger circuits such as memory, oscillators and amplifiers provides a set of results allowing unique chip identification. Careful design of these readout and monitoring technologies can be used to amplify variations resulting in a highly unique (secure) signature or fingerprint. An example is device authentication that utilizes Physically-Unclonable Functions (PUFs) within existing memory structures to secure device transactions providing encryption-key management.

United States Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing on March 28, 2017
Cybersecurity Threats to the U.S. Electric Grid and Technology Advancements to Minimize such Threats and to Receive Testimony on S. 79, the Security Energy Infrastructure Act
Questions for the Record Submitted to Dr. Thomas Zacharia

The use of watermarking technologies, such as patterned radiation exposure of electronics, could also be employed to impart spatially programmed device offset voltages for identification of a single chip or runs of chips. This technology would be undetectable with known imaging technologies, but would be easily decoded with incorporated and hidden readout electronics.

ANSWER:

b. Does fingerprinting technology have any potential application for the IoT? How?

Both fingerprinting and watermarking technologies have broad application to any hardware system using integrated circuits. IoT hardware could broadly incorporate this technology to verify undesired supply chain component tampering including replacement. This is particularly important in sensitive or high reliability applications. A commercially-available example is Intrinsic-ID which is targeted primarily at the IoT for microprocessor-based applications. Samsung is also involved in fingerprinting for device authentication. This type of technology will be a major part of the IoT as time progresses.

Questions from Senator Joe Manchin III

Question 1: I think we would miss an opportunity here today if we did not mention electromagnetic pulses (EMPs) and the potential havoc they could wreak on our electric system. Here in the Senate Energy Committee we included the "GRID Act" in the Energy Policy Modernization Act which would have directed the Secretary of Energy to develop the Department's technical expertise in the protection of electric systems (generation and transmission) against geomagnetic storms or malicious actors who use EMPs. There was similar legislation in the House. Understanding that these EMPs could be manmade or intentional, I'm curious as to what technologies exist today and what technologies you are exploring to address this potentially devastating type of event.

What is your organization doing to protect against the threat of EMPs – naturally-occurring or intentional?

I believe Faraday cages have been used for many years to protect electronics and computer solutions. Is that a solution that can be explored for our bulk power system? Or is this a solution for the customer side?

ANSWER:

Electromagnetic pulses (EMP) and impacts on the energy infrastructure have been a concern for many years with differing views on the overall system impacts. The EMP from high altitude

(>30 km) nuclear bursts follows a pattern that can be characterized approximately by three consecutive electromagnetic field waveform components, typically referred to as E1, E2, and E3 (see Figure 1). Each has its unique characteristics, effects on the grid, and mitigation measures.

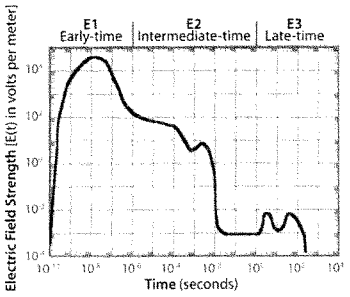


Figure 1. Pulse created by high-altitude nuclear burst.

E1 is a fast-rising, short-duration pulse that may create large, potentially destructive, electric surges in conductors and electronics. The E2 component creates an overvoltage of lesser peak amplitude and longer duration, as compared to E1, and is similar to a lightning strike, albeit extending to a very large geographical area (as much as E1, thus potentially affecting many systems simultaneously). The E3 component is characterized by a large-scale, slowly varying, prolonged perturbation of the geomagnetic field. This, similarly to geomagnetic disturbances (GMDs) generated by the solar activity, may cause anomalous currents in the windings of power transformers connected to long transmission lines, possibly leading to serious damage to the transformers themselves due to harmonic generation and heating resulting from magnetic core saturation.

Traditional mitigation products may include electromagnetic shielding enclosures (for E1/E2). Faraday-cage type shielding is the most effective and is applicable in many, or most, cases at the utility-level. DOD has done quite a bit more, starting with their "TEMPEST" standard.

Present-day technology can effectively block the impact of geomagnetic disturbances and the effects of the tail-end of High-Altitude EMPs (E3) from a nuclear blast. Products are commercially available, and in a few cases, have been already installed, to protect large power transformers. Another device on the market is a "dc-blocking device" for GMD and E3.

The obstacles for a system-wide implementation of such a hardening approach are not technical. Rather, they are of an economic nature, since there is no clear picture that provides the utilities with a cost-benefit analysis, and, as a result, the regulatory and industry standard landscape has

not been developed to the point of being able to provide a consistent set of guidelines.

ORNL is actively involved in studying and evaluating impacts from both EMP and geomagnetic disturbances (GMD) on the electric grid and its components. ORNL is strongly engaged in the activities of the Mission Executive Council working group on EMP and GMD, led by DOE's Infrastructure Security and Energy Restoration (ISER), to foster a coherent action plan in the area.

Currently, ORNL is leading a $2.2 million / 2.5-year effort with a research team that includes Lawrence Livermore National Laboratory (LLNL) and partners from academia and industry. This project, being funded out of the DOE's Grid Modernization Laboratory Consortium (GMLC), is capitalizing on past experiences including extensive work conducted at ORNL in the early '90s and focusing on the vulnerability of the large power (transmission-class) transformers, as the most critical components of the power grid. The study is being conducted with a synergistic combination of theory, modeling and vetted experimental efforts, with the purpose of quantifying the potential damage level arising from realistic threat scenarios, and defining the best avenues for implementation of technical solutions to protect the grid. ORNL also completed an assessment of the adequacy of the inventory of spare large power transformers that could be deployed if needed to recover from a major event damaging large parts of the electric grid.

Question 2: In the aftermath of the attack on the Pacific Gas & Electric substation in Metcalf, California – the Federal Energy Regulatory Commission required NERC (the North American Electric Reliability Council) to propose standards requiring transmission owners to address physical security risks and vulnerabilities that could impact the reliable operation of the grid. In 2013, another attack in Arkansas illustrated the grid's potential vulnerability to carefully planned physical attacks to equipment essential to keeping the lights on. The FBI arrested a man in Lonoke County Arkansas for several attacks on the transmission grid, including deliberately setting fire to Entergy's 500 kV substation.

Please share your perspective on to the seriousness of the attacks and, based on this experience, what emerging technologies, if any, are primed to protect against physical attacks on the grid?

ANSWER:

Infrastructure vulnerability is a legitimate threat to our country, evident in the April 2013 attack on Pacific Gas and Electric Co.'s Metcalf substation near San Jose, Calif. Although no major power outage transpired, it increased awareness of the importance of securing our energy infrastructure. Concerns over the ability to quickly replace high voltage equipment due to their long lead times continue to be raised. After the Metcalf incident, FERC called for new physical security protections for critical nodes of the interstate high-voltage power network, resulting in

United States Senate Committee on Energy and Natural Resources
Subcommittee on Energy Hearing on March 28, 2017
Cybersecurity Threats to the U.S. Electric Grid and Technology
Advancements to Minimize such Threats and to Receive Testimony
on S. 79, the Security Energy Infrastructure Act
Questions for the Record Submitted to Dr. Thomas Zacharia

NERC Standard CIP-014, "Physical Security." Through this process, owners and operators are required to identify facilities critical to operating the interconnection, and have been investing in the physical security of their critical infrastructure by purchasing additional spare large power transformers (LPTs) and other large equipment, participating in sharing programs for LPTs, implementing security and perimeter fences, cameras, sensors and other technologies. Just recently Duke Energy Corp. formally announced it will spend $13 billion to strengthen the grid against power outages and cyberthreats with an emphasis on physical as well as cyber security.

In addition to the investments being made by industry, there are other technologies that may be helpful for physical protection of the electric infrastructure. Through DOE's Grid Modernization Initiative, low-cost sensor technologies are being developed to monitor multiple parameters within a "sensor suite" as highlighted in our answer to Senator Murkowski's question #1 and portrayed in the accompanying figure. These monitors can detect the presence of certain Unmanned Aerial System (UAS) devices, cellphone signals, and many other parameters that can then trigger an operator to further evaluate the presence with IR imaging and other cameras. Additional technologies are being developed at National Laboratories that can help with infrastructure protection in the event of a successful physical attack, such as low-cost power flow control systems that can direct electric flow under abnormal conditions.

ORNL has also been involved in scoping a separate network supporting various communications enclaves that could serve as an EMP "day after" hardened link for connected utilities, thereby allowing some level of secure and resilient communications between the utilities.

Statement for the Record by the

AMERICAN PUBLIC POWER ASSOCIATION (APPA),
EDISON ELECTRIC INSTIUTE (EEI), and the
NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION (NRECA)
Submitted to the
Senate Energy & Natural Resources Committee's Subcommittee on Energy
For the March 28, 2017, Hearing to
"Examine the Cybersecurity Threats to the U.S. Electric Grid and Technology Advancements to Minimize Such Threats and to Receive Testimony on S.79, the Securing Energy Infrastructure Act"

The American Public Power Association (APPA), Edison Electric Institute (EEI) and the National Rural Electric Cooperative Association (NRECA) appreciate the opportunity to submit a statement for the record for the Senate Energy & Natural Resources Committee's Subcommittee on Energy's hearing to "examine the cybersecurity threats to the U.S. electric grid and technology advancements to minimize such threats and to receive testimony on S.79, the Securing Energy Infrastructure Act." APPA, EEI, and NRECA support and agree with the testimony of Ben Fowke with Xcel Energy.

Protections Designed to Guard Against Energy Disruptions
The electric utility industry 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 a mandatory and enforceable federal regulatory regime in place for cybersecurity. Congress approved the process for mandatory and enforceable reliability standards 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 cybersecurity standards that apply across the North American grid (including 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, EEI, NRECA and our member owners and operators, as well as other utilities, are active participants in the NERC Critical Infrastructure Protection (CIP) standards drafting process on cybersecurity and physical security. As attacks on critical electric infrastructure are ever-changing, so too are 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
Industry 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, we strongly supported passage of the Cybersecurity Act of 2015, which was incorporated as Division N of P.L. 114-133, the Consolidated Appropriations Act, 2016. The Act provides policies and procedures for sharing cybersecurity threat information between the federal government and private entities (which includes electric utilities) as well as sharing between private entities while providing limited liability protection for these activities if conducted in accordance with the Act.

In addition to the Cybersecurity Act of 2015, we 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 clarified 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 required 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 also established sanctions for the unauthorized disclosure of shared information. It is critical to operational security that the industry is confident that clearly sensitive information about critical infrastructure that might provoke new threats or endanger the safety and well-being of the North American public or the integrity of the electric power grid not be publicized.

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 NERC, FERC, the Department of Homeland Security (DHS), and Department of Energy (DOE) 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.

Recently, ESCC leadership met with DOE Secretary Rick Perry, Department of Homeland Security leadership, and White House National Security Council staff to discuss grid security and the vital role the public-private partnership plays in it. We will continue to work to maintain and grow the valuable relationship between the council and senior administration leadership throughout the transition.

"Defense-in-Depth" and 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 of the time 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 "all hazard" threats 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, 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 cybersecurity 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 electric utilities, allowing them to test their readiness and preparedness for both cyber and physical attacks. Industry is currently in the process of preparing for Grid Ex IV in 2017.

S.79, the Securing Energy Infrastructure Act

S.79, 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, intelligence community, and electric utility industry, among others. We believe that the goals and intentions of this legislation are important and worthwhile and appreciate the interest of the legislative sponsors in this critical issue. The electric power industry's defense-in-depth approach allows for flexibility to incorporate technology advancements and we would like to stress 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.

Conclusion

APPA, EEI, and NRECA appreciate the opportunity to offer these comments to the Subcommittee as it looks into the critical issue of protecting the reliability of our nation's electric grid. Protecting the nation's electric power grid and ensuring a supply of safe, reliable, and affordable electricity is a top priority for the electric power industry.

Written Testimony of Acting 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

March 28, 2017

Chairman Gardner 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. 79, the Securing Energy Infrastructure Act. DOE supports the goals of S. 79, 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 well-being of our citizens depend on the reliable delivery of electricity. I know the Secretary is personally engaged in the cybersecurity issues facing the energy sector. Under his leadership, the Department's role in cybersecurity is a very high priority. 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 and secure 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 physical security events, natural and man-made disasters, and cybersecurity breaches.

Over the past decade, the Nation's energy infrastructure has become a major target of cyberattacks. The frequency, scale, and sophistication of cyber threats have increased and attacks have become easier to launch. Cyber incidents have the potential to interrupt energy services, damage highly specialized equipment, and threaten human health and safety. As a result, energy cybersecurity and resilience has emerged as one of the Nation's most important security challenges and fostering partnerships with public and private stakeholders will be of utmost importance in this work.

Importance of Cybersecurity for Energy Systems

Initial thoughts of cybersecurity often turn to computer servers and desktops, information technology (IT). Hackers target computing technology and business applications to cause disruptions – obtaining access to email accounts and personal information, data exfiltration to be released to the world at large. The energy sector is not immune to such attacks.

In the 2012 Shamoon attack, weaponized malware hit 15 state bodies and private companies in Saudi Arabia, wiping more than 35,000 hard drives of Saudi Aramco, from which the company took more than two weeks to recover. And again in January of this year, Shamoon 2 hit three state agencies and four private sector companies in Saudi Arabia, leaving them offline for at least 48 hours.

These cyberattacks affect not only business systems, but can also target the operating technology of energy delivery systems and other critical infrastructure as well. Electric utilities, oil and natural gas providers, hydro and nuclear facilities, along with financial, water, communications, transportation, and healthcare sectors are prime targets for cyber-attacks. The disruption of any one of these is not only inherently problematic, it also hampers the ability to respond to any type of emergency event.

In December 2015, the first known successful cyber-attack on a power grid took place in Ukraine. Over 225,000 residents were left without power for several hours in the coordinated attack, and a second attack occurred in December 2016 that left portions of Kiev without electricity. Domestically, the 2013 cyber-attack on the Bowman Dam in Rye, New York illustrated the multitude of targets available to and being surveilled by hackers.

The Ecosystem of Resilience

To address these challenges, it is critical for us 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, 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. The DOE National Laboratories have been the keystone in many endeavors to address new and existing cybersecurity concerns.

Importance of Partnerships

The U.S. Department of Energy has collaborated with the energy sector for nearly two decades in voluntary public-private partnerships that engage energy owners and operators at all levels — technical, operational, and executive, along with state and local governments—to identify and mitigate physical and cyber risks to energy systems.

These partnerships are built on a foundation of earned trust that promotes the mutual exchange of information and resources to improve the security and resilience of critical energy infrastructures. These relationships acknowledge the special security challenges of energy delivery systems and leverage the distinct technical expertise within industry and government to develop solutions.

The security and integrity of energy infrastructure is both a state and Federal government concern because energy underpins the operations of every other type of critical infrastructure; the economy; and public health and safety. The owners and operators of energy infrastructure, however, have the primary responsibility for the full spectrum of cybersecurity risk management:

identify assets, protect critical systems, detect incidents, respond to incidents, and recover to normal operations.

The first responder when the lights go out or gasoline stops flowing in the pipelines is not immediately the state or Federal Government; rather, it is industry. This is why public-private partnerships regarding cybersecurity are paramount—they recognize the distinct roles and capabilities of industry and government in managing our critical energy infrastructure risks.

Two of those partnerships are the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council, extremely strong partnerships in which DOE-OE is engaged. Each serves as a primary conduit between industry and the government to prepare for, and respond to, national-level disasters or threats to critical infrastructure. Through these relationships, cybersecurity issues can be addressed more completely and with multiple stakeholder input.

DOE Authority in Cybersecurity

DOE's role in energy sector cybersecurity is established in statute and executive action. In 2015, through the Fixing America's Surface Transportation Act (FAST Act), Congress assigned DOE as the lead Sector-Specific Agency (SSA) for cybersecurity for the energy sector, building upon previous Presidential Policy Directives (PPD). PPD-41 issued in July 2016, further clarified the role of DOE as a SSA during a significant cyber incident.

The FAST Act also gave the Secretary of Energy new authority, upon declaration of a Grid Security Emergency by the President, to issue emergency orders to protect or restore critical electric infrastructure or defense critical electric infrastructure. This authority allows DOE to respond as needed to the threat of cyber and physical attacks on the grid. DOE is developing a proposed rule of procedure regarding this new authority.

While the private sector is responsible for all aspects of cybersecurity risk management of their energy systems, DOE and the Federal government play critical roles in supporting industry functions in several ways: providing partnership mechanisms that support collaboration and trust; developing supportive policies that encourage voluntary cybersecurity in the energy sector; developing tools and capabilities to conduct risk analysis; leveraging government capabilities to gather intelligence on threats and vulnerabilities, and share actionable intelligence with energy owners and operators in a timely manner; supporting energy sector incident coordination and response; facilitating the development of cybersecurity standards; and, promoting and supporting innovation and R&D for next-generation physical-cyber systems.

DOE's Research and Development Activities in Cybersecurity and Resilience through the National Laboratories

Intentional, malicious challenges to our energy systems are on the rise and we are seeing threats continually increase in number and sophistication. This evolution has profound impacts on the energy sector.

Cybersecurity for energy control systems is much different than typical IT systems. Power systems must operate continuously with high reliability and availability. Upgrades and patches can be difficult and time consuming, with components dispersed over wide geographic regions. Further, many assets are in publicly accessible areas where they can be subject to physical tampering. Real time operations are imperative and latency is unacceptable for many applications. Immediate emergency response capability is mandatory and active scanning of the network can be difficult. As a result, our National Laboratories conduct cybersecurity R&D taking into account these systemic characteristics.

DOE-OE's Cybersecurity for Energy Delivery Systems (CEDS) R&D program aligns activities with Federal and private sector priorities, envisioning resilient energy delivery control systems designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

The CEDS R&D program is designed to assist the energy sector asset owners by developing cybersecurity solutions for energy delivery systems through a focused research and development effort. DOE-OE co-funds projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems. These research partnerships are helping to detect, prevent, and mitigate the consequences of a cyber-incident for our present and future energy delivery systems.

Since 2010, DOE-OE has invested more than $210 million in cybersecurity research, development, and demonstration projects that are led by industry, universities, and the National Laboratories. These investments have resulted in more than 35 new tools and technologies that are now being used to further advance the resilience of the Nation's energy delivery systems.

Through all of these R&D efforts, our National Laboratories have been – and continue to be – heavily engaged in their own efforts and in partnerships with academia and industry stakeholders. The following are examples of the types of cybersecurity advancements currently pursued at our National Laboratories, building off of successful cybersecurity tools and technologies already developed:

- Argonne National Laboratory is currently working on a resilient self-healing cybersecurity framework for the power grid that will leverage Wide-Area Monitoring, Protection, and Control to prevent and mitigate cyber-attacks. The project will develop tools to prevent and mitigate cyber-attacks and enhance the resilience of the bulk power system.

- Argonne is also working on a cloud and outsourcing security framework for power grid applications as well as cybersecurity for distributed energy resources (DER). This project will help ensure that implementation of cloud-based architecture and DER in the energy sector are deployed with security built-in to maintain resilience during cyber-attacks.

- An online tool being developed by Brookhaven National Laboratory will help utilities to detect, mitigate, and evaluate the potential impact of various cyberattack scenarios to reduce the risk that malicious compromise of essential forecasting data used for grid scheduling and operation might result in disruption of energy delivery.

- The Validation and Measuring Automated Response Project led by the Idaho National Laboratory is providing a cyber-incident response comparison capability and enabling industry to work towards an automated response capability to a cyber-incident and measuring the efficacy of automated response to drive future improvements.

- Lawrence Berkeley National Laboratory has an effort underway utilizing real-time micro-synchrophasor measurements and other telemetry in the distribution system to enhance identification and detection of current and future cybersecurity vulnerabilities in the power distribution grid to provide a more reliable, robust, scalable, and cost-effective means of detecting cyber-attack scenarios compared to traditional approaches.

- Pacific Northwest National Laboratory is developing visualizations that power system operators and/or cybersecurity professionals can use to make fast, accurate assessments of situations, enabling them to maintain situation awareness during unfolding events. The visualization tool will reduce the burden on the operators and enable them to make faster decisions and maintain cybersecurity situational awareness.

- Pacific Northwest National Laboratory is also working on a project evaluating existing Live Analysis monitoring and detection tools for energy delivery systems use. The research seeks to develop a tool that could provide evidence of anomalous cyber behavior on a live energy delivery system without interrupting energy delivery.

- The Artificial Diversity and Defense Security (ADDSec) project at Sandia National Laboratory is developing defensive technologies that randomly and automatically reconfigure energy delivery operational network parameters moment-by-moment to impede reconnaissance and cyber-attack planning. ADDSec will increase the security of both legacy and modern energy delivery systems by converting these traditionally static systems into moving targets.

- "Sophia" is a tool researched and developed by the Idaho National Laboratory (INL) that enhances continuous situational awareness of energy delivery control system communications and helps detect potential cybersecurity concerns. The technology helps strengthen the cybersecurity of our Nation's energy infrastructure today and of note is the fact INL successfully transitioned this technology to commercial use through a licensing agreement.

- Similarly, Oak Ridge National Laboratory licensed the developed "Hyperion" software technology. This software can quickly recognize malicious code even if the specific program has not been previously identified as a threat and before it has a chance to execute.

- Also in the process of transitioning to commercialization is Sandia National Laboratory's "CodeSeal." CodeSeal is a cryptographically secure code obfuscation technology that prevents reverse engineering, or malicious modification of energy delivery system code, even if that code is executed on a compromised system.

S. 79

The U.S. Department of Energy is tremendously proud of the role our National Laboratories have played in the advancement of cybersecurity technologies for our Nation's energy infrastructure. We also appreciate the opportunity to provide technical assistance on S. 79. It appears that the intent of the legislation is to strengthen our cybersecurity posture by directing the National Laboratories to undertake a study of the systems most critical to national security and to the grid.

In considering the legislation, DOE notes that many energy sector entities already conduct such assessments to comply with mandatory Critical Infrastructure Protection standards set by the Federal Energy Regulatory Commission and the North American Electric Reliability Corporation 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.

Conclusion

Cyber threats to the energy sector 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 the Nation's energy infrastructure through increased resilience and flexibility.

One of the cornerstones to this ecosystem of resilience is the DOE National Laboratories and the significant contributions they provide through their cybersecurity technology advancements. Building an ecosystem of resilience is—by definition—a shared endeavor, and keeping a focus on partnerships remains an imperative. DOE will continue its years of work fostering these relationships and investing in technologies to enhance resilience and security, ensuring the electric power grid continues to be able to withstand and recover quickly from disasters and attacks.