AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 115–489

ADVANCED CYBER TECHNOLOGIES THAT COULD BE USED TO HELP PROTECT ELECTRIC GRIDS AND OTHER ENERGY INFRASTRUCTURE FROM CYBERATTACKS

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

OCTOBER 26, 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

27–434 WASHINGTON : 2019

COMMITTEE ON ENERGY AND NATURAL RESOURCES

LISA MURKOWSKI, Alaska, *Chairman*

JOHN BARRASSO, Wyoming
JAMES E. RISCH, Idaho
MIKE LEE, Utah
JEFF FLAKE, Arizona
STEVE DAINES, Montana
CORY GARDNER, Colorado
LAMAR ALEXANDER, Tennessee
JOHN HOEVEN, North Dakota
BILL CASSIDY, Louisiana
ROB PORTMAN, Ohio
LUTHER STRANGE, Alabama

MARIA CANTWELL, Washington
RON WYDEN, Oregon
BERNARD SANDERS, Vermont
DEBBIE STABENOW, Michigan
AL FRANKEN, Minnesota
JOE MANCHIN III, West Virginia
MARTIN HEINRICH, New Mexico
MAZIE K. HIRONO, Hawaii
ANGUS S. KING, JR., Maine
TAMMY DUCKWORTH, Illinois
CATHERINE CORTEZ MASTO, Nevada

BRIAN HUGHES, *Staff Director*
PATRICK J. MCCORMICK III, *Chief Counsel*
ISAAC EDWARDS, *Senior Counsel*
ANGELA BECKER-DIPPMANN, *Democratic Staff Director*
SAM E. FOWLER, *Democratic Chief Counsel*
DAVID GILLERS, *Democratic Senior Counsel*

CONTENTS

OPENING STATEMENTS

	Page
Murkowski, Hon. Lisa, Chairman and a U.S. Senator from Alaska	1
Cantwell, Hon. Maria, Ranking Member and a U.S. Senator from Washington	2

WITNESSES

Imhoff, Carl, Manager, Electricity Market Sector, Pacific Northwest National Laboratory	5
Raines, Dr. Richard, Director of Electrical and Electronics Systems Research, Oak Ridge National Laboratory	13
Tudor, Zachary D., Associate Laboratory Director, National and Homeland Security, Idaho National Laboratory	25
Earl, Dr. Duncan, President & Chief Technology Officer, Qubitekk, Inc.	36
Riedel, Daniel, CEO and Founder, New Context Services, Inc.	40

ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

Cantwell, Hon. Maria:	
Opening Statement	2
Earl, Dr. Duncan:	
Opening Statement	36
Written Testimony	38
Responses to Questions for the Record	75
Imhoff, Carl:	
Opening Statement	5
Written Testimony	7
Responses to Questions for the Record	66
Murkowski, Hon. Lisa:	
Opening Statement	1
Raines, Dr. Richard:	
Opening Statement	13
Written Testimony	15
Response to Question for the Record	70
Riedel, Daniel:	
Opening Statement	40
Written Testimony	42
Tenable, Inc. and Siemens Energy:	
Statement for the Record	77
Tudor, Zachary D.:	
Opening Statement	25
Written Testimony	28
Responses to Questions for the Record	72

ADVANCED CYBER TECHNOLOGIES THAT COULD BE USED TO HELP PROTECT ELECTRIC GRIDS AND OTHER ENERGY INFRASTRUCTURE FROM CYBERATTACKS

THURSDAY, OCTOBER 26, 2017

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

The Committee met, pursuant to notice, at 10:01 a.m. in Room SD–366, Dirksen Senate Office Building, Hon. Lisa Murkowski, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. LISA MURKOWSKI, U.S. SENATOR FROM ALASKA

The CHAIRMAN. Good morning, everyone. The Committee will come to order. I apologize we are a little bit later starting than I had hoped.

Over the years, we have conducted a number of hearings designed to examine the vulnerabilities of our nation's electric grid system. In this Congress, we have held a series of hearings focused on cybersecurity, electromagnetic pulse, and grid security issues at both the full and the subcommittee levels.

During today's hearing, we will add to that, by looking at advanced and emerging cyber technologies and processes that are being developed in our national labs and in the private sector. These are technological improvements and sometimes breakthroughs, that could be used to protect the grid, as well as other critical energy infrastructure, from future cyberattacks.

I have mentioned, certainly many times in this Committee, but outside of the Committee as well, that around the country sometimes we get the sense that folks believe in this "immaculate conception" theory of energy, that it just happens. We all recognize, I think, that there is a lot more to this than that.

A related question is, what happens when the lights don't turn on? When you flip that switch and you just expect it to happen, and then they do not turn on. What happens when electricity is out for an extended period of time? And we are certainly seeing that in Puerto Rico and the U.S. Virgin Islands right now, the real-world impact of an extended power outage.

Just as we can harden our energy infrastructure to protect it from natural disasters, we must also look to ways to harden the grid from constantly evolving cyber intrusions as well. It seems like every day now we hear about an attempted hack or actual breach

that has taken place, and the list is long and getting longer. OPM, Ukraine's power grid, the WannaCry ransomware, Equifax, Anthem, Home Depot, Target, the list keeps growing and growing. Just last Friday, the Department of Homeland Security issued a public alert of an ongoing hacking threat to the U.S. energy systems.

In the midst of all of this, we have to continually look for ways to eliminate, diminish, or mitigate our vulnerabilities. So whether it is the application of quantum encryption, artificial intelligence, or moving control of grid infrastructure off of the public internet, the witnesses we have today will help provide our Committee with insights into how we can protect our national energy infrastructure now and into the future.

I mentioned quantum encryption, and I would like to note a recent article by McClatchy about the advances that China has made on this topic. Earlier this year China announced that a satellite and ground station 745 miles apart had communicated through quantum particles. Last month a video conference between China and Austria, a distance of about 4,600 miles, was held via China's quantum satellite. They have established a 1,200-mile quantum link between Shanghai and Beijing and announced that they will build a $10 billion quantum research facility. According to that article, some scientists believe that with the amount of resources China is putting into the field, a quantum computer may be built in a decade or less. Whether or not these claims are accurate, I think, remains to be seen, but it is clear that significant research is underway around the world in the cyber realm.

I want to thank our witnesses for joining us today. I look forward to learning about the efforts that you have been involved with to combat and deal with this threat, particularly on the work that you are doing to keep our electric grid and our energy infrastructure safe and reliable. So thank you for joining us.

I now turn to Senator Cantwell for her comments. And I want to thank you, Senator Cantwell, because you have been dogged and persistent when it comes to the issue of cyber and the cyber threats, particularly as they relate to our energy grids.

STATEMENT OF HON. MARIA CANTWELL,
U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Well, thank you, Madam Chair, and thanks for scheduling this important hearing so we can continue the discussion about what technologies we need to protect our electric grid and make sure that our whole energy infrastructure is protected from cyberattacks.

I want to say at the outset, I spent much of this summer working on this issue and spent a great deal of time at our national labs with Secretary Perry focusing on some of our cybersecurity solutions. I hope that he understands the pressing need here and will restore the DOE's crippling cybersecurity budget that was proposed by the Administration. It is very important that we continue to have the resources as a nation to fight and to protect key energy infrastructure.

I am dismayed that instead of focusing on cybersecurity as one of the key issues of resiliency, he is instead trying to get a com-

mand economy approach with FERC by trying to change market-based rate prices for consumers and instead trying to push a rule that would drive coal into the marketplace and raise rates on consumers. I think that FERC operates best when it operates on market rules.

I am also requesting this morning, Madam Chair, in light of yesterday or two days ago's amazing news about the huge increase in park fees that we have a hearing on this in the future. Many of my constituents woke up to, literally, shock over the fact that these exorbitant rates would be charged in our park system. I hope that we can have some input on this and show that our constituents are extremely concerned about it. For us in the Northwest, our outdoor economy is a big juggernaut. I know it is in your state as well.

But anyway, thank you for having this hearing and thank you to the witnesses for being here. It is such a critical issue and getting your input is very important.

I would also like to especially welcome Mr. Carl Imhoff, who is testifying on behalf of the Pacific Northwest National Laboratory (PNNL). Again, thank you for hosting us and the Secretary earlier this year and for all the impressive work that you do.

Cybersecurity is the one issue that keeps me up at night worrying about how foreign entities and actors might attack us as the next provocation in a national/international effort. We used to think of it as a plane that might fly into airspace or a sub that might cross international waters, and now what we have to worry about is provocations from actual grid attacks. If we don't make the necessary investments to prevent and defend against these impacts, our enemies could succeed in causing widespread blackouts or devastating the economy or threatening to bring millions of Americans to the point of without power being in great disarray.

As I referenced earlier, the Trump Administration proposed budget cuts to the cyber programs at DOE and put our critical infrastructure at risk. I have conveyed those concerns to the Administration in two letters, and as I said, spent a lot of time this summer hoping that they would see the impacts here to our budget and what they would do.

Since our Committee's last cybersecurity hearing when we discussed the Ukraine outages of 2015 and 2016, we have witnessed numerous large-scale cyberattacks as the risks continue to grow. In July, the Washington Post reported that the Russian government hackers were behind cyber intrusions into U.S. nuclear power plant business systems. In September, it was revealed that the hackers accessed the personal information of 143 million Americans through the data breach of Equifax. And just this week, the Department of Homeland Security issued a report about ongoing cyber threats to nuclear, water, and energy sectors that appear to reference the July incidents that I just mentioned.

With each day of cybersecurity threats to the grid and the multiple efforts that are underway, it is important that we continue to combat effectively our security risk through innovation. We need to take action.

The good news is our national labs are ready to play a key role in bolstering our cybersecurity, and they do so in close collaboration with the private sector. The PNNL cyber firewall blocks 24

million suspected internet communications, 25,000 of which are confirmed cyberattacks. That is what they do each day, so I have no doubt that they know how to help protect our country and our important missions.

Our witnesses today will demonstrate the breakthroughs that result from these productive public-private partnerships and why they need to continue. In that vein, I am calling on an increase in collaboration between the government, private sector, utilities, military, and academia. I know we are going to, in our state, try to continue the discussion at the University of Washington Bothell in a symposium on energy cybersecurity workforce.

I have also, on the Commerce Committee, attended some of the hearings that that Committee has had on cyber workforce. And we know from our DOE Quadrennial Energy Review, this is exactly what the previous Secretary said we needed to do, was to help build the cyber workforce for tomorrow. Hopefully this symposium will bring together critical partners to leverage the knowledge, expertise, and experience of all aspects of the challenge that we face.

It is clear to me that cyber solutions will require us to leverage the world class expertise of our labs, the private sector, and all of us working together. That is why I hope that Secretary Perry and the President will reverse their harmful 32 percent cut to the Department of Energy's cybersecurity budget without further delay and hopefully help us make the investments we need for the future.

Thank you.

The CHAIRMAN. Thank you, Senator Cantwell.

Know that I join you in your concern with the recent announcement from Park Service about the fees. So that is something that we will look to.

I welcome you to the Committee this morning. Thank you for giving us your time.

I will introduce each of you and give you an opportunity to present your opening statements for approximately five minutes or so. Know that your full statements will be included as part of the record. After each of you have presented, we will have an opportunity to ask questions of you.

We will lead off with Mr. Carl Imhoff, who is the Director for the Electricity Market Sector at Pacific Northwest National Laboratory. Welcome. Dr. Richard Raines is the Director for Electrical and Electronic Systems Research Division at Oak Ridge National Laboratory. We have another national lab expert with us this morning, Mr. Zachary Tudor, who is the Associate Laboratory Director of National and Homeland Security at Idaho National Laboratory. Dr. Duncan Earl is with us. He is the President and Chief Technology Officer for Qubitekk, Incorporated. And the last member of the panel this morning is Mr. Daniel Riedel, who is the CEO of New Context Services, Inc. We are delighted to have each of you.

Mr. Imhoff, if you would please lead off, thank you.

STATEMENT OF CARL IMHOFF, MANAGER, ELECTRICITY MARKET SECTOR, PACIFIC NORTHWEST NATIONAL LABORATORY

Mr. IMHOFF. Thank you, Chairman Murkowski, Ranking Member Cantwell, and members of the Committee for the opportunity to join this hearing today.

My name is Carl Imhoff, and I lead the grid research program at DOE's Pacific Northwest National Laboratory in Washington State. For more than two decades PNNL has supported system resilience, reliability, and innovation for DOE and utilities across the nation. I also chair DOE's Grid Modernization Laboratory Consortium, a team of 12 national laboratories, including Oak Ridge and INL, that supports DOE's grid modernization initiative, along with over 100 partners from academia and industry.

Today I'd like to offer two points regarding advanced technology for improved cyber resilience of the nation's power system.

Point one. Cyber risk information sharing between industry and DOE has significantly improved our national grid cyber readiness. The public-private effort must continue to advance in scope, speed, and industry inclusion to deliver full situational awareness of both operational control systems as well as utility enterprise networks.

Point two. Beyond situational awareness, the fundamental science and technology offer important opportunities to deliver defensive tools that span the growing Internet of Things challenges at both the grid edge as well as core grid operations. And in this area, I'll offer three examples.

Looking first at improving grid cyber situational awareness, PNNL and DOE developed and deployed the Cybersecurity Risk Information Sharing Program, or CRISP, first for DOE assets across the U.S. in the early 2000s. This concept was successfully tested on utility activities and transitioned to industry leadership via NERC over the past few years with industry investing in infrastructure and DOE funding the intelligence evaluation. This voluntary program identifies cyber threats and shares that information with utilities that collectively generate over 75 percent of the electricity of the United States. This effort continues to expand coverage and improve the speed, accuracy and affordability of situational awareness tools.

Going forward, PNNL is extending cyber situational awareness to better address grid operational control systems or OT and other interdependent infrastructures such as fuel delivery in light, natural gas pipelines, and communications. We believe that the nation must develop an integrated real-time view of the cyber risk spanning the IT and OT elements of the power system. NERC standards already require significant sense of the OT environment. PNNL is applying advanced real-time analytics to these OT data streams leveraging the fundamental science of high performance computing, statistics and a re-emerging field of deep learning. Deep learning refers to advances in artificial intelligence concepts from the '90s that are delivered on a profoundly improved, high performance computing platform. That's the big delta since the '90s. And they leverage the ultra large data sets that are growing and emerging in the power system as well.

These new tools will uncover relationships and trends that indicate cyber risk or control system anomalies resulting in better, faster operational decisions and automated machine-to-machine exchanges.

Beyond improved situational awareness, the nation must also develop inherently resilient paradigms for networks, open data, and system controls.

Adaptive networks are important because the emerging grid is substantially more dependent upon communications today than it was even ten years ago.

PNNL recently teamed with Schweitzer Engineering in Washington State to develop a product using a new concept called software defined networks to enable reconfiguration of communication networks through software commands. These networks provide an additional adaptive defense layer for the grid.

Data resilience concepts are important because of the growth in e-commerce and new utility market constructs. The challenge is how to protect data in open environments. One example is blockchain, the technology the Bitcoin uses to secure transactions. Resilient data concepts will enable secure use of distributed power generation and energy storage systems and help secure emerging market constructs like transactive energy.

A third technology innovation is adaptive control systems which adjust to real time based upon system conditions. Adaptive controls can provide a more level cyber playing field by adjusting on the fly to confuse, obfuscate, and mislead adversaries as they attack the system.

Cyber technology innovations are absolutely essential, but they're not sufficient to deliver a national cyber readiness posture. Small and midsized grid operators must learn and implement fundamental best practices in cyber applications and regulators and utilities must have new valuation tools and data sets to evaluate cyber technology investments and provide the regulatory incentives essential to delivering these improved technology assets.

So, in conclusion, industry and DOE cyber sharing efforts have significantly advanced our cyber situational awareness and the next challenge is to integrate control system situational awareness to achieve full awareness across IT and OT systems. And in parallel, we need to leverage high performance computing, deep learning and new control theory to develop inherently resilient systems and system designs for networks, data and grid control systems.

Thank you.

[The prepared statement of Mr. Imhoff follows:]

Statement of Carl Imhoff
Manager, Electricity Market Sector
Pacific Northwest National Laboratory

Before the
United States Senate
Committee on Energy and Natural Resources

October 26, 2017

Good morning. Thank you, Chairman Murkowski, Ranking Member Cantwell, and Members of the Committee. I appreciate the opportunity to appear before you today to discuss advanced cyber technologies to protect the electric grid and other energy infrastructure from cyber-attacks, and issues and opportunities in this area.

My name is Carl Imhoff, and I lead the Grid Research Program at the Pacific Northwest National Laboratory (PNNL), a U.S. Department of Energy (DOE) national laboratory located in Richland, Washington. I also serve as the Chair of DOE's Grid Modernization Laboratory Consortium, a team of national labs that, along with industry, industry groups such as the Gridwise Alliance and the Electric Power Research Institute, and university partners, supports the Department's Grid Modernization Initiative. The consortium members include PNNL, the National Renewable Energy Laboratory, Argonne National Laboratory, Brookhaven National Laboratory, Idaho National Laboratory, Lawrence Berkeley National Laboratory, Lawrence Livermore National Laboratory, Los Alamos National Laboratory, the National Accelerator Laboratory at Stanford, National Energy Technology Laboratory, Oak Ridge National Laboratory, Sandia National Laboratories, and Savannah River National Laboratory.

I will address two main points today:

1. PNNL and industry, via the North American Electric Reliability Corporation (NERC) Electricity Information Sharing and Analysis Center (E-ISAC), have made important progress in establishing information sharing capabilities for grid business information technology (IT) infrastructures, which provides cyber risk situational awareness for utilities and covers 75 percent of U.S. electricity generation. This effort will continue to broaden grid situational awareness for both the operational technology (OT) control systems of utilities in combination with IT systems, ultimately delivering enhanced, complete cyber situational awareness for the power system.

2. Fundamental science and technology offer important opportunities to complement cybersecurity situational awareness with improved defensive tools spanning the growing challenges at both the grid edge and core grid operations.

Background

For more than two decades, PNNL has supported power system reliability, resilience and innovation for Washington State, the Pacific Northwest, and the nation. During this period, the laboratory has:

1. Led DOE-industry collaborations in developing and deploying synchrophasor technology to help avoid blackouts. Phasor measurement unit networks are designed to enhance situational awareness of wide area systems. This new grid tool has demonstrated value by detecting impending system control and equipment faults for system operators, thus avoiding major outages. California estimates $360 million in annual savings to customers due to avoided outages, plus $90 million in annual savings in improved utilization of existing generation and delivery systems. This high performance monitoring system provides the basis for a new tool, developed in partnership between the Electric Reliability Council of Texas (ERCOT) and DOE, to better analyze complex blackout scenarios to that lead to improved design of resilient grid upgrades that resist cyber and other threats.

2. Gained significant experience leading effective public-private partnerships. For example, PNNL led a collaboration with utilities and vendors to develop and demonstrate transactive control concepts on the Olympic Peninsula in Washington State and for the Pacific Northwest Smart Grid Demonstration project – the largest of its kind – to validate smart grid benefits and new control approaches that engage demand and distributed resources at scale. Example outcomes include Avista Corporation implementing distribution automation and smart metering pilots that delivered a 10-percent reduction in customer outages, reduced consumer outage durations by 21 percent, and resulted in 1.5 million avoided outage minutes between April 2015 and April 2016.

3. Innovated and implemented new, novel predictive data analysis. PNNL delivered the first applications of high performance computing to grid tools such as interconnection-scale contingency analysis, reducing run times from days to under two minutes. PNNL also applied high performance computing and phasor measurement unit data to deliver the first real-time dynamic state estimation to open the door to the future world of predictive grid tools. This parallelized state estimator tool enabled PNNL to deliver assessments of system risk at the interconnection scale on the Western Interconnection in less than two minutes versus the traditional 24 hours. This provides operators with more powerful tools to mitigate the risk of potential cyber-attacks and other risks. Moving from reactive to predictive data-driven analysis methods is essential to effectively managing cybersecurity challenges on the grid.

4. Designed and implemented meaningful national exercises that address critical electrical grid resiliency and cybersecurity challenges. PNNL assisted NERC and DOE with design and implementation of a series of national GridEx exercises designed to link industry with government and law enforcement agencies to conduct cyber-attack exercises.

GridEx III, held in November 2015, engaged 364 organizations and more than 4,000 participants in scenarios designed and operated with support from PNNL. GridEx IV will be held in mid-November, with additional support provided by PNNL.

These examples illustrate the high return on investment possible when combining advanced technology innovation designed to improve cybersecurity with public-private validation and deployment.

Lastly, the DOE Grid Modernization Initiative is an important source of innovation for national efforts to modernize energy infrastructure. Improved grid resilience and security for cybersecurity is a major objective of the overall effort. The Initiative is a DOE-wide effort across multiple program offices to accelerate the development of technology, modeling analysis, tools, and frameworks to enable grid modernization adoption. As a key component of this Initiative, the Grid Modernization Laboratory Consortium – co-led by PNNL and the National Renewable Energy Laboratory – is working closely with partners in industry, academia, and cities and states to deliver new concepts, tools, platforms, and technologies to better measure, analyze, predict, and control the grid of the future – resulting in improved resilience, reliability, and productivity. Public-private collaboration in field validation accelerates the development of lessons learned and data that support states and utilities to develop business cases for their grid modernization efforts.

Current and Emerging Advanced Grid Cyber Security Technologies

Cyber Situational Awareness: In order to monitor and effectively manage the security and resiliency of the grid, PNNL and DOE developed and deployed the Cyber Risk Information Sharing Program (CRISP). This voluntary situational awareness program identifies cyber threats to utilities and shares that information with utilities, which collectively generate over 75 percent of the nation's electricity. Today, PNNL works with the NERC E-ISAC and DOE to ensure rapid exchange of information across industry and government entities to provide timely alerts and response to cybersecurity risks posed to power industry infrastructure. This effort continues to expand coverage and improve the speed and accuracy of situational awareness of threats for the industry. In addition to expanding the system to include additional utilities, PNNL is developing advanced analytics that can handle terabytes of data daily.

PNNL is now extending cyber situational awareness to increase attention on the grid control systems internal to the utilities, also called operational technologies (OT), and the interdependent infrastructures such as fuel delivery (e.g. natural gas pipelines) and communications. We believe that the nation must develop an integrated, real-time view of cyber risk across the IT and OT elements of the power system to significantly improve our cyber resilience.

NERC standards already require significant sensing of the OT environment to ensure NERC Critical Infrastructure Plan (CIP) compliance. As such, PNNL is applying science and advanced technology tools to enhance the analytics of these data streams to deliver cyber situational awareness for these grid control systems. These analytics depend on the fundamental science of

high performance computing, statistics, and a reemerging field of "deep learning." Deep learning refers to advances on the artificial intelligence concepts of the 1990s that are delivered on new high performance computing platforms and leverage the ultra large data sets that are emerging in the power system. These ultra large data sets exist on the IT and OT sides of the power system. They are driven by the two billion intelligent devices at the grid edge today, which are expected to grow to 20 billion by 2025; the 64 million smart meters installed over the past decade; and the cutting-edge synchrophasor monitor network of 2,500 sensors across North America delivering samples at a rate of 60 samples per second. Collectively, power system operators are engaging massive-scale data sets that offer significant opportunity to improve power system cyber situational awareness.

PNNL and others in the national lab, industry and academic communities are applying deep learning concepts to these data sets to extract relationships and trends that have meaning to issues such as cyber risk or control system anomalies, which can be indicators of cyber-attack. These results can deliver value in two ways:

1. They provide power system operators and/or planners with insights that inform better decision making in the dispatch of generation and secure operation of the power system.

2. Automated "machine to machine" exchanges enable the power system protection and control systems to recognize problems faster and respond safely. The "machine-to-machine" topic is one of the high priorities set by the Electricity Subsector Coordinating Council for public-private research and development (R&D) advancement.

Ultimately, this course of advanced R&D effort by PNNL and the broader community will help detect cyber and other risks faster and support the design of new systems that are inherently more resilient to cyber and other threats.

Advanced Science and Technology Research: To complement the improvements in situational awareness of IT and OT systems, PNNL is also applying advanced science and technology cyber resilience concepts in pursuit of new power system paradigms that are inherently resilient and adaptive. Elements of this research include:

- **Adaptive Networks:** The emerging modern grid is substantially more dependent upon communications networks, both in terms of capacity and performance as well as reliability. PNNL recently teamed with Schweitzer Engineering in Pullman, Washington to develop and deploy a product using a new concept called "software defined networks" to enable the reconfiguration of communication networks through software commands. Software defined networks provide an additional, adaptive defense layer. This new "software" layer of a computer network allows the network to change segmentation and to quarantine parts of the network dynamically. This means an adversary would need to break through an additional layer of technology, one that can change. This project resulted in a commercial product that achieved exceptional market presence in a very

short time.

- **Data resilience:** Growth in e-commerce innovation and the consideration of new utility market constructs to better engage consumer interests in new services have resulted in new approaches to protecting data in open environments. One example is blockchain, the technology that Bitcoin uses to secure transactions. Blockchain is a method for recording transactions in a shared, encrypted ledger without the need for a central repository, which is significant because centralized data is a compelling target for cyber attackers. By spreading the data around in multiple places, it is much harder to attack, modify or manipulate. With regard to the grid, blockchain could be a part of grid modernization efforts, encourage distributed power generation and storage systems, and help secure emerging market constructs. PNNL is currently working with DOE and industry partners to determine the optimal use of such resilient data concepts as blockchain in emerging market constructs such as transactive energy.

- **Adaptive control systems:** A third technology innovation is the transition from fixed to adaptive control and protection systems which adjust in real-time based upon system conditions at that moment. Adaptive control systems can provide a more level cyber playing field by adjusting on the fly to confuse, obfuscate, and mislead adversaries as they work their way through a system, increasing the effort and knowledge needed to get through defenses, while also giving a better chance for detection and deployment of solutions to be effective. PNNL is developing advanced distributed and hybrid control theory and concepts that make the power system and key parts thereof, such as building control systems, more adaptive and resilient to cyber-attack. The Grid Modernization Laboratory Consortium also is conducting advanced control research that leverages fundamental mathematics and advance network theory to accommodate more distributed energy resources that can support power system resilience.

These are three examples of advanced technologies that will enable new paradigms of power system design to actively defend against cyber-attack and other risks facing the modern grid.

Cyber "Best Practices" and Valuation an Important Part of National Cyber Readiness

Science and technology efforts are critical to protect the electric grid and energy infrastructure from cyber-attack, but cannot alone achieve the end state goal. Grid operators must learn and implement basic "cyber hygiene" measures – practices and routines that can be undertaken regularly (or avoided) to keep utility systems in good shape. While large utilities are actively pursuing cybersecurity strategies to meet industry requirements, small and mid-sized utilities don't have to meet those requirements and can view cyber defense as an expensive and complex undertaking. DOE is working with the American Public Power Association and the National Rural Electric Cooperative Association to help small and mid-sized utility managers improve their cybersecurity readiness.

Additionally, utilities at all levels – consumer-owned, investor-owned, municipalities – must have the capacity to understand the value of alternatives to improve their cybersecurity, system resilience and performance. State regulators need the same tools and data sets with which to evaluate cybersecurity and modernization plans and provide the regulatory incentives to achieve prudent efforts that delivers affordable resilience improvements to product offerings that enable modernization at scale. Finally, vendors must be able to define market opportunities to ensure rapid innovation in their product offerings. The Grid Modernization Laboratory Consortium portfolio includes research projects to develop a framework for valuation of the new grid technologies and concepts, including for cybersecurity, so that government and industry stakeholders can work together to assess the benefits and costs of security and resilience improvement strategies. This partnership between DOE, states, and industry is an important collaboration in charting a timely path to a more secure, resilient U.S. power system.

Conclusion

Industry and DOE have partnered to significantly advance the cyber situational awareness of the utility business and internet-facing computer networks over the past few years. The next step in the journey is to integrate these capabilities with enhanced situational awareness of control systems, providing both operators and automated protection systems the capacity to significantly enhance cyber awareness, security and resilience across utility IT and OT systems.

In parallel to "better defending" the current system, we must to continue to leverage the foundational science and technology tools of high performance computation, analytics, deep learning and control theory to develop more resilient system designs for networks, data and grid control systems. These will enable the power system to resist inevitable attacks, better defend against cyber and other hazards, and ultimately recover more quickly.

The DOE investments in fundamental science, applied technology and public-private field validation partnerships are foundational elements of an effective, integrated national cyber readiness strategy and capacity for the U.S. electric power system and its related infrastructures. I appreciate the opportunity to discuss this important issue with you today, and I am happy to answer your questions. Thank you.

The CHAIRMAN. Thank you, Mr. Imhoff.

Dr. Raines, welcome.

STATEMENT OF DR. RICHARD RAINES, DIRECTOR OF ELECTRICAL AND ELECTRONICS SYSTEMS RESEARCH, OAK RIDGE NATIONAL LABORATORY

Dr. RAINES. Good morning, Chair Murkowski, Ranking Member Cantwell and members of the Committee. Thank you for the opportunity to appear before you today with this distinguished panel.

I'm Dr. Rick Raines, Director of Electrical and Electronics Systems Research at the Department of Energy's Oak Ridge National Laboratory (ORNL). I previously served as the Director of Cybersecurity Data Analytics at ORNL which was followed by a military and federal service career where I founded and directed the Air Force Cyberspace Technical Center of Excellence at the Air Force Institute of Technology.

The Department of Energy's national laboratory system has a long history of providing solutions to the nation's hardest problems. Our structure and operations encourage partnerships with industry and other institutions to solve big science challenges. Cybersecurity of our critical energy infrastructure is a national challenge demanding national focus.

Today, I want to address the importance of securing a resilient, electrical grid and discuss some of the technological breakthroughs we're developing at ORNL to harden the grid defenses.

As you're well aware, our electric grid is a vital national asset. It is also a system that's becoming increasingly vulnerable to cyber intrusions, due in large part to its increased connectivity with the public internet.

As industry has embraced these technological and cost-effective advances, operational risks have increased. Energy sector devices and systems are experiencing increased exposure to savvy and nefarious cyber actors. As a result, we're in a highly dynamic cycle of developing cybersecurity measures and capabilities to address these rapidly emerging threats.

Our challenge is to produce solutions to better protect energy sector communications and controls while continuing to make the grid smarter and to better able recover when problems do arise, including the devastating effects of Hurricanes Harvey, Irma and Maria.

At Oak Ridge our scientists and engineers are engaged in research to defend and modernize the grid, including real-time monitoring and sensing of the grid state and new technologies to control and better utilize distributed power resources such as community microgrids. We have developed cybersecurity technologies that can detect intrusions, such as malicious software code, advanced persistent threats, and real-time cyber awareness tools to detect anomalies and network communication traffic.

Among our cybersecurity work is a concept called Dark Net. The Dark Net vision is to shield the nation's electric grid from hostile cyber intrusions while advancing the state of the art and anticipating and mitigating threats. The Dark Net, in its most simple terms, is a way to get the communications and control of the electric grid off the public internet. Moving these functions onto a private system could be accomplished using existing and underutilized

optical fiber, commonly known as dark fiber. It's estimated over 100,000 miles of optical fibers exist within the U.S. Bundling with multiple fibers, communication techniques can easily increase its capacity tenfold.

I'd like to be clear that the Dark Net is not just about moving the grid's command and control functions off the public internet, nor is it just about the unused fiber that we have, but it's about creating and leveraging a holistic tool kit of capabilities to make it harder for an adversary to exploit our systems.

Working with our private and public partners we envision Dark Net as a highly secure, resilient, and redundant communication sensing and technical assistance solution supporting all elements of the electric enterprise and its supply chain. Our goal is to develop methods so that these attacks are automatically detected, isolated, and defended, achieving a self-aware, self-healing network. We believe the Dark Net project can provide cost-effective, secure solutions to include the use of new and existing dark fiber and advanced communications and cybersecurity technologies; working with industry to create living laboratories where we'll test security functionality and resiliency; implementing new technologies in tool kit form and operational security approaches to protect against grid and cyber threats; and lastly, enhancing grid state monitoring with advanced sensing, measurement, and situational awareness. The grid must evolve to address a variety of challenges such as cyberattack, severe weather, a changing mix of power generation types, the growth of interconnected smart devices, and the aging of our energy infrastructure. We envision Dark Net as a key component in the evolution toward a secure national energy asset.

In conclusion, Oak Ridge National Laboratory and the other DOE national labs stand ready to work with public and private partners to develop and employ innovative technical solutions to protect the nation's electric grid.

Thank you again for the opportunity to provide this briefing. I welcome your questions.

[The prepared statement of Dr. Raines follows:]

Cyber Technology and Energy Infrastructure

Statement of Richard Raines, Ph.D.
Director of Electrical and Electronics Systems Research
Oak Ridge National Laboratory

Before the
Committee on Energy and Natural Resources
U.S. Senate
October 26, 2017

Thank you, Chairman Murkowski, Ranking Member Cantwell, and Members of the Committee. I am Dr. Richard Raines, Director of the Electrical and Electronics Systems Research Division at the U.S. Department of Energy's Oak Ridge National Laboratory (ORNL) in Oak Ridge, Tennessee. It is an honor to participate in this hearing with this distinguished panel today.

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, fossil energy, solar photovoltaics, 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, its critical infrastructure, and the world a safer place.

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 (fourth most powerful 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. The latest frontier in materials research is at the nanoscale—designing materials atom by atom —and we leverage ORNL assets such as Titan and the Center for Nanophase Materials Science for breakthrough materials research;

- 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 director of electrical and electronics systems research and as the lead for energy system cybersecurity at a national laboratory with an intense focus on solving compelling national problems in energy and security.

GRID VULNERABILITY: A GROWING THREAT

The nation's electrical grid is a vital resource upon which our economy and our citizens' daily lives depend. It is also a system that is highly vulnerable to cyber intrusions as more and more utility controls and "smart" technologies rely on public internet connections. These advanced technologies give operators better control and make the grid more efficient and resilient. But they come at a price: the potential exposure of devices and systems to very savvy computer specialists whose intent may be nefarious. As such, cybersecurity measures and capabilities must be constantly improved to address these rapidly emerging threats as we modernize grid infrastructure.

The electrical grid is an interconnected network of power, communication and control systems that requires vigilance in cybersecurity that is shared by all associated partners. All must operate with the recognition that vulnerabilities will be discovered and exploited by adversarial actors. Energy owners and operators have the primary responsibility to protect their systems from failure. The federal government is responsible for ensuring national and economic security, and the health and safety of American citizens and communities. It is in everyone's interest that we engage in a closely coordinated defense of our energy networks, to reduce the types of physical and cyberattacks that could trigger a large-scale and prolonged energy disruption with direct bearing on our strength as a nation.

Operational technologies, such as electric power grids, offer realizable targets for the midrange to sophisticated actor. The grid has emerged as a viable target for exploitation for many reasons, including simple control logic and operations, and globally produced sensors, but largely due to growing interconnectivity with the internet. Attackers exploit systems that lack current software configurations or unsuspecting operators who may not have been trained to avoid attacks such as

phishing. The intrusions can inflict damage on physical infrastructure by infiltrating the digital systems that control assets—damaging equipment and disrupting vital services even without a physical attack. As witnessed in the Ukraine in 2015 and again in 2016, the cyber threat is real and damaging.

In the Ukrainian cyberattacks, the adversary exploited the human component of the system's operations to gain access and escalate privileges for total control of the targeted system. Additionally, the attackers circumvented reporting mechanisms that were designed to alert system monitors of abnormal behavior. These actions resulted in power losses to more than 225,000 customers over a period of a few hours. While power was restored to consumers relatively quickly, the overall implications of this attack were not known for weeks. A key takeaway from these attacks was the reactive nature of the system operator responses. Forensic analysis revealed that little to no protective mechanisms were in place to preclude the attack from occurring—all efforts were restorative in nature.

Fast-forwarding to May of this year, the President recognized the growing cyber threat to U.S. critical assets and sought new assessments under an executive order[1] on strengthening the cybersecurity of federal networks and critical infrastructure.

Furthermore, in an August report[2] released by the President's National Infrastructure Advisory Council (NIAC), senior executives from industry and state and local governments stated that national leadership, in close collaboration with industry, is essential to support cybersecurity of high-risk assets. The report listed 11 recommended actions that the federal government and the private sector can take to defend critical private systems from aggressive cyberattacks including "…establishing separate, secure communications networks specifically designated for the most critical cyber networks…."

Our challenge in the United States is to implement cyber solutions to better protect energy sector communications and controls, while continuing to make the grid "smarter" and more resilient when problems do arise, including the challenges of severe weather events such as we recently saw with Hurricanes Harvey, Irma, and Maria.

It is a task made difficult by the grid's existing operational requirements and complex interconnectivity. The electric grid is a 24/7/365 operating system. The United States' strategic and societal interests rely on the grid's continuous, real-time, and reliable operation, which underpins the social fabric of this country. This operational tempo makes grid research, development, and the deployment of solutions a difficult challenge for industry to address alone.

This is where the DOE's national laboratories provide essential national research. The National Laboratory System is uniquely positioned to address cybersecurity challenges through technology breakthroughs in partnership with the private sector. At ORNL, expertise and capabilities in high-performance computing, data and graph analytics, discrete mathematics,

---

[1] http://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[2] http://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf

power systems and engineering, embedded systems and wireless technologies, sensors and controls provide solutions and breakthroughs for detecting and deterring cyberattacks.

ORNL EXPERIENCE: TECHNOLOGICAL SOLUTIONS

ORNL brings capabilities and expertise to both 1) protect the electric grid from cyberattack, and 2) modernize grid infrastructure and increase its ability to respond quickly to disruption.

Our scientists and engineers are engaged in several areas of research designed to increase both grid cybersecurity and resilience, or the system's ability to quickly rebound from disruption. Modernizing grid infrastructure and making it more resilient is essential to grid security.

ORNL has developed numerous technologies for cybersecurity. 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).

Additional ORNL-developed cyber-physical tools and capabilities include:

- GridEye sensors located across the U.S. for real-time monitoring of the power grid;
- EAGLE-I, a visualization and analysis system designed to predict possible energy system outages as well as help first-responders rapidly locate outages when they occur;
- Oak Ridge Cyber Analytics (ORCA), a real-time cybersecurity platform for detecting advanced persistent threats and zero-day exploits;
- Situ**,** a real-time cyber situational awareness tool capable of determining anomalies in network-related traffic; and
- Timing Authentication Secured by Quantum Correlations (TASQC**),** a ground-based timing capability for secure communications.

As announced in September 2017 by DOE's Office of Electricity Delivery and Energy Reliability, ORNL is taking on several additional projects for grid resilience and cybersecurity.

As part of DOE's Grid Modernization Laboratory Consortium (GMLC), which leverages the capabilities and expertise of all 17 national laboratories, ORNL will be involved in two **resilient distribution systems** projects:

- Integration of responsive residential loads into distribution management systems. This project aims to provide electric utilities with software and hardware that make possible demand-side management of residential loads to improve grid resiliency.

- Increasing distribution system resiliency using flexible distributed energy resources and microgrid assets enabled by OpenFMB, or Open Field Message Bus. OpenFMB is a

framework that allows generation assets to communicate with each other for better system flexibility, rather than being controlled by a single system.

Both projects address ways to enhance electricity distribution systems, including microgrids – localized grids that can disconnect from the traditional grid and operate autonomously, a capability that helps to mitigate disturbances and strengthen grid resilience.

Under DOE's **cybersecurity for energy delivery systems** research area, ORNL will be involved in five projects:

- *DarkNet*. A project to get the electric grid off the public internet. The project will define requirements for a secure energy delivery control system network that is independent of the public internet and uses existing but currently unused optical fiber, known as "dark fiber." The NIAC report referenced above, for instance, lists the creation of a separate, secure communications network specifically designated for critical infrastructure as its number one recommendation. The DarkNet concept is discussed in more detail below.
- *Quantum physics-secured communications for the energy sector* (referencing our national security needs to outpace Chinese advances demonstrated in orbiting satellite systems http://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance). Development of a quantum-rooted grid security framework in which information is carried in quantum states of light, so that any attempt to read that information is revealed in real-time, detectable changes to the quantum states.
- *Quantum key distribution for the energy sector*. Trusted node relays and networks. Research, design, and prototype of a quantum secure communication operational network, including trustworthy relays to extend distance and decrease cost for critical energy infrastructure.
- *Malware operational mitigation.* Working with energy sector partners to coordinate utility system malware detection and analysis and provide real-time validation of vulnerabilities to system operators.
- *Energy delivery systems with verifiable trustworthiness.* Providing a tool to verify the integrity of firmware used in energy delivery system devices, without taking the equipment offline.

These projects continue ORNL's long history of working with public and private partners to achieve the energy sector's vision of resilient energy delivery systems that are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

In addressing the area of grid security, ORNL is mindful that the nation's privately-owned electricity assets present a unique challenge, and we are leveraging our long history of working closely with private sector partners to develop effective research.

ORNL is working with utility companies such as the Chattanooga Electric Power Board (EPB) and Southern Company to help design, assess and install microgrids. Companies are trying to

understand the value proposition of these technologies for improved grid resiliency. With ORNL's assistance, EPB is evaluating the idea of "dynamic microgrids" where sections of the distribution system—potentially with distributed energy resources—can be sectionalized into independent microgrids to determine if this will improve grid resiliency. ORNL's research with EPB is a prime example of how a close working relationship with industry can deepen our understanding of these challenges and produce workable solutions. The EPB system has been a successful "living laboratory" for advanced sensors and other technology developed by ORNL to make the grid more secure and resilient.

We are also working with Southern Company to test new microgrid technology that provides local control of resources like solar power and energy storage sited in a "connected neighborhood" and then seamlessly integrated into the larger power grid.

Most recently, ORNL has considered how its scientific expertise may be leveraged to help an area in which the local power grid is essentially being rebuilt from the ground up. Puerto Rico was devastated by Hurricane Maria last month. The island's critical infrastructure, including its power transmission and distribution grid serving more than 1.4 million customers, was nearly demolished by the powerful storm. As the relief and recovery effort continues, we are mindful that many of the solutions developed for grid resilience could be purposely built into a completely new, robust system for Puerto Rico.

Through distributed energy resources, for instance, the Puerto Rico Electric Power Authority could benefit from microgrids, with more power generation spread throughout its territory, sited locally in neighborhoods and communities and providing greater flexibility when the larger grid is disrupted.

Complementary opportunities exist to support the development of a more secure and resilient Puerto Rican infrastructure, which will ultimately lead to better quality of life for its residents and reliable electricity to support its businesses.

THE DARKNET CONCEPT

As part of DarkNet, ORNL is investigating ways to move electric grid controls and communications away from the public internet and onto secure networks. The goal of DarkNet is to develop and implement, in conjunction with private and public partners, a highly secure, resilient, and redundant communications, sensing, and technical assistance solution supporting all elements of the electricity enterprise and its supply chain. The vision is to shield the nation's electric grid from hostile cyber penetrations while also advancing the state-of-the-art in anticipatory threat mitigation. DarkNet will design and build an isolated, secure communications network to protect and transport the nation's most sensitive critical infrastructure data—beginning with the electric grid.

Under DarkNet, ORNL and its partners, will investigate ways to take advantage of underutilized fiber optic capacity already on utility systems across the country but not accessible to the

internet. This approach can be used to move grid command and control functions onto private, isolated networks using "dark" or unlit fiber.

ORNL scientists and engineers are evaluating the over-capacity of fiber deployed in the past two decades and determining whether it offers a platform for a new communications and control architecture with innovative cyber-physical security measures. With advanced sensor technologies that monitor the grid for any disturbances that indicate intrusion, ORNL will develop methods that automatically detect, isolate, and defend against these attacks—with the goal of a self-aware, self-healing network. Utilizing ORNL's unique high-performance computing platforms and energy testbeds, anticipatory threat modeling and analysis will aid the development of capabilities to rapidly identify emerging threats, gain awareness of the potential threat's capabilities, and dynamically posture resources (sensors and mitigation devices) to minimize, if not eliminate, the threat and disruptive consequences.

DarkNet's key differentiator from previous cybersecurity solutions lies in its holistic approach to 1) use existing resources (i.e., unlit fiber) for separation from an inherently unsecureable infrastructure (the internet); and 2) develop and rapidly deploy new and innovative foundational security capabilities.

Key DarkNet objectives include:

- Enhancing infrastructure (new and existing dark fiber) as a cost-effective protective measure, using advanced communications and cybersecurity technologies;
- Leveraging emerging communications security protocols that establish protected links across the grid;
- Working with industry to create living laboratories to test security functionality and resilience—partnering with utilities and suppliers for proof of concept;
- Implementing new technologies in toolkit form and operational security approaches to protect against cyber and insider threats;
- Enhancing grid state monitoring with advanced sensing, measurements, escalating alert and situational awareness; and
- Using the existing buried infrastructure (dark fiber) as a cost-effective protective measure, leveraging advanced communications (ultra-fast 5G-LTE networks, satellite communications, and private wireless networks) and cybersecurity technologies suitable for expanding smart grid requirements.

DarkNet will evolve from an implementation framework already under development to a series of integrated research, development, test, and evaluation projects that will have the potential to yield near- and far-term cybersecurity solutions.

In conclusion, if the DarkNet concept is funded and implemented, it will enable national continuity of operations, rapid restoration, and cost-effective protective measures to thwart damage from cyberattacks, operational and physical threats, and natural disasters. Security and

resilience enhancements are not about bolting on a costly, cumbersome exoskeleton. As a nation, we must infuse the grid's operational DNA with capabilities that make it immune to attack and degradation.

CLOSING REMARKS

Whether the threat is natural or manmade, intentional or not, a secure, resilient electrical grid with hardened defenses is essential to the security of our nation. The grid's critical systems must evolve to address a variety of challenges such as cyberattack, severe weather, a changing mix of power generation types, the growth of interconnected smart devices, and the aging of electricity infrastructure.

Sometimes called the world's largest machine, a reliable, secure electric grid is foundational to U.S. competitiveness, economic vitality, and our very way of life. ORNL and the other DOE national laboratories stand ready to work with industry and other institutions to develop and employ innovative technical solutions to protect the nation's power grid. Thank you again for the opportunity to provide this briefing. I welcome your questions on this important topic.

APPENDIX

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

The National Laboratory System is well-suited to exploring and developing technological solutions for protecting the energy grid. Partnerships with government, industry and academia are 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)**, 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**, a comprehensive, real-time energy monitoring dashboard developed by DOE/OE for integration with VERDE
  - **Oak Ridge Cyber Analytics (ORCA)**, a real-time cybersecurity platform for detecting advanced persistent threats and 0-day exploits
  - **Situ**, 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**, 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**, technology being developed by ORNL in partnership with General Electric Research to exploit 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 Institute
  - Two-year effort to determine cybersecurity R&D gaps and develop way-ahead strategy

National Electric Grid 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

The CHAIRMAN. Thank you, Dr. Raines.

Mr. Tudor, welcome. I know that Senator Risch wanted to make a comment before you spoke.

Senator RISCH. Well thank you.

Zach, welcome to the Committee. You are in for a real treat here.

I have gotten to know Mr. Tudor in his capacity as Associate Lab Director at the Idaho National Laboratory. He is responsible for the lab's national and homeland security mission and that includes nuclear non-proliferation, critical infrastructure protection, obviously, very important to this hearing and defense systems missions. He has an incredibly impressive resume which I am not going to go into here, but he is the right man for the job in Idaho. We are glad to have him, and he is the right person for this hearing which you are going to see in a moment. So, welcome, Zach.

The CHAIRMAN. Thank you, Senator Risch.

Mr. Tudor, welcome.

STATEMENT OF ZACHARY D. TUDOR, ASSOCIATE LABORATORY DIRECTOR, NATIONAL AND HOMELAND SECURITY, IDAHO NATIONAL LABORATORY

Mr. TUDOR. Thanks.

Chairman Murkowski, Ranking Member Cantwell and distinguished members of the Committee, thank you for holding this hearing and inviting Idaho National Laboratory's (INL) testimony on advanced technologies to protect the U.S. power grid and other energy infrastructure from cyberattack. I appreciate the opportunity to address this Committee and express my utmost respect and gratitude for your leadership and continued interest in this topic.

I also want to acknowledge my peers and partners from industry and national labs who will share their examples of innovation, unique capabilities and technology breakthroughs in areas such as situational awareness, quantum computing, sensors, automation, modeling and simulation and visualization.

The cyberattacks on the Ukraine power grid demonstrated how quickly these events can move and impact a wide variety of interdependent systems across the region. In the U.S. high profile events like Nuclear 17 and Palmetto Fusion illustrate why utilities and regulators are concerned with increasing burdens due to more sophisticated and frequent cyber events. Industry must have advanced capabilities and cyber skills not only to detect but also to respond to these events before there is an unacceptable impact.

Protection of the grid and energy infrastructure from cyberattack is one of the nation's most difficult technical and operational challenges and requires the national laboratory's capabilities.

INL enables research and development of cybersecurity solutions to understand and manage the multifaceted interdependencies between the grid and other critical infrastructure, detect and respond within compressed timelines to prevent highly impactful consequences and develop top tiered defenders to mitigate sophisticated threat actors. As part of our national laboratory leadership role in addressing this national challenge, INL advocates that effective grid and energy infrastructure protection is achieved, not only

with advanced technology, but also requires innovative engineering approaches in a deep pool of top tiered cyber defenders.

As such, the development of technology process and people are priorities within INL's strategic initiative, the Cybercore Integration Center. This initiative is envisioned to create and align national science and engineering resources, technical expertise, and collaborative partnerships to focus on scalable and sustainable control system cybersecurity solutions—solutions that protect the U.S. grid, other critical infrastructure, and also military systems.

In response to your request for INL's participation in this hearing, I provide several examples in the written testimony of INL's progress in developing advanced technology solutions, advanced engineering processes, and the development of that top tier workforce. For brevity, I will quickly summarize four examples.

In collaboration with the partners of the California Energy Systems for the 21st Century (CES-21), an innovative concept from machine-to-machine automated threat responses is being developed. When this research proves successful, utilities, and not only California utilities, will have access to automated threat and exploit prioritization capabilities that will reduce the time for discovery and recovery from illicit behavior resulting in increased resiliency of the electric grid.

The INL Autonomic Intelligent Cyber Sensor will enable system owners to more easily design, implement, and monitor cyber secured control system networks. The goal of this technology is to automate network information, deploy deceptive virtual hosts, kind of virtual and dynamic honeypots, and identify threats on network traffic with very high accuracy.

These two advanced technology examples represent opportunities to gain benefits of machine-to-machine speed in responding to cyber intrusion or attack. The next examples emphasize an engineering approach and workforce development strategy for grid protection.

Recognizing that just chasing vulnerabilities has not been sufficient. Our Consequence-driven, Cyber-informed Engineering, or CCE, is a transformational engineering process methodology that fully leverages an organization's deep engineering expertise and their intimate knowledge of their own systems and processes. This enables the organization to eliminate and manage the cyber risks that could result but in the greatest consequence.

A pilot study was completed with a major U.S. electric power utility to determine the potential value of CCE to assist utilities with reducing cyber risks by implementing cyber-informed engineering solutions while engineering out vulnerabilities and attack pathways that detect those severe consequences.

Following the Ukraine attack, INL researchers used their experience gained while investigating the event to convert the lessons learned into a training course for utilities. The Ukraine event in a box devices fit on a desktop and are designed to challenge course participants to cyber defend the equipment that they routinely encounter.

In summarizing, the described examples highlight Cybercore's holistic research and development strategy for control system cybersecurity innovation.

I do want to re-emphasize that solutions to protect the grid and energy infrastructure are realized through deployment of advanced technologies, implementation of enhanced engineering and operational processes, and the development of highly-skilled and well-informed workforce.

I thank the Committee members for this opportunity to share our strategy and examples of the progress in protecting the grid and energy infrastructure, and I welcome your questions.

[The prepared statement of Mr. Tudor follows:]

STATEMENT OF
MR. ZACHARY D. TUDOR, ASSOCIATE LABORATORY DIRECTOR
NATIONAL & HOMELAND SECURITY

IDAHO NATIONAL LABORATORY

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON ENERGY AND NATURAL RESOURCES

OCTOBER 26, 2017

Mr. Zachary D. Tudor, Associate Laboratory Director, Idaho National Laboratory National and Homeland Security Directorate

U.S. Senate Hearing to receive testimony on advanced cyber technologies that could be used to help protect electric grids and other energy infrastructure from cyberattacks.

Chairman Murkowski, Ranking Member Cantwell, and distinguished members of the Committee, thank you for holding this hearing and inviting Idaho National Laboratory's testimony on advanced technologies to protect the U.S. power grid and energy infrastructure from cyberattack. I appreciate the opportunity to address this Committee and express my utmost respect and gratitude for your leadership and continued interest in this topic.

I request that my written testimony be made part of the record.

I am the associate laboratory director for National and Homeland Security at Idaho National Laboratory, also known as INL. INL is responsible to the Department of Energy (DOE) to create, cultivate, and deliver future technology solutions that enable the realization of this nation's strategy for secure energy production and delivery. INL's role within the DOE laboratory complex provides great opportunities for influencing and executing an extensive government and industry portfolio of research, development and demonstration programs that address the cyber threats to the stability, reliability, and resilience of the nation's energy infrastructure. Also, with my role as a member on the Board of Directors of $(ISC)^2$ – the International Information Systems Security Certification Consortium – I have the opportunity to influence the strategy, governance, and oversight of certification for information security professionals around the world – some of whom are protecting the information and control system networks within our electric infrastructure.

The cyberattacks in 2015 and 2016 on the Ukraine power grid demonstrated that attacks on energy infrastructure can move very quickly and impact a wide variety of interdependent systems across a region. With recent high-profile events like Nuclear 17 and Palmetto Fusion within the U.S., it is obvious why utilities and regulators are concerned with increasing burdens caused by more sophisticated and frequent cyber events – during which they must have capabilities and skills to detect and respond to an attack before it causes an unacceptable impact. Due to the multifaceted interdependencies of the grid with other critical infrastructure, the breadth of technologies and systems that make up our energy infrastructure, and the speed and sophistication of a cyberattack, protection of the grid and energy infrastructure from cyberattack is one of our most complex technical and operational challenges. To increase confidence in our ability to protect the grid and energy infrastructure, the U.S. must continue to pursue research and development, demonstration at scale, and deployment of solutions from all sources of innovation, including industry, universities, and national laboratories. *These solutions will be realized through deployment of advanced technologies, implementation of enhanced engineering and operational processes, and development of a highly skilled and well-informed workforce.*

The U.S. requires unique capabilities to solve the most complex technical research and development challenges. The nation owns and invests in the Department of Energy's national laboratories to provide expertise and unique research and development capabilities to solve these difficult technical challenges. A recent example that illustrates our reliance on the Department of Energy and its national laboratories for protection of the grid and energy infrastructure is the March 14 letter from Senators Cantwell and Wyden to President Donald Trump urging the President to maintain the Department of Energy's leading role in defending our critical energy systems and networks as codified in the Fixing America's Surface Transportation Act (Public Law 114-94). Similarly, Senator King and co-sponsors Senators Risch, Heinrich, Collins, and Crapo drafted S. 79, the Securing Energy Infrastructure Act – legislation that emphasizes the development of a cyber-informed engineering strategy with the Department of Energy and national laboratories to defend energy infrastructure from vulnerabilities and exploits.

INL is the nation's lead nuclear energy national laboratory and is recognized as a national and international leader in control systems cybersecurity and grid resilience. INL advocates that effective grid and energy infrastructure protection will be achieved with not only advanced technology solutions, but with innovative engineering approaches, and a deep pool of top-tiered cyber defenders, scientists, and engineers. As such, INL is committed to and engaged in conducting the research, development, demonstration, and deployment of a broad range of holistic solutions that will have transformational and sustainable impact on the reliability and resilience of the grid and energy infrastructure. INL's commitment is showcased in an INL strategic initiative – the Cybercore Integration Center. The Cybercore Integration Center is focused on creating enduring national capabilities for control systems cybersecurity innovation with long-term objectives to:

- Transform the cyber-informed science and engineering within national research and innovation programs that solve the most complex cybersecurity challenges resulting from the convergence of cybersecurity with control systems, power, and wireless among critical infrastructure and national security systems.
- Develop multi-organizational partnerships to share research capabilities and real-time threat information on the most difficult national security challenges.
- Build the nationwide, multidisciplined expertise needed to sustain a superior control systems cyber workforce.

Successful implementation of the Cybercore Integration Center strategy includes partnerships and collaborations to leverage the researcher talent pool and unique research infrastructure within the national laboratories, industry, and universities. As an example, my national laboratory and industry peers who are participating in this hearing (i.e., Oak Ridge National Laboratory, Pacific Northwest National Laboratory, and New Context) provide many unique capabilities, including those that are making technology breakthroughs in situational awareness, sensors, automation, modeling, simulation, and visualization.

A critical factor in achieving grid and energy infrastructure protection and resilience is taking a balanced approach to projects for advanced technologies, engineering processes, and workforce development. A balanced portfolio includes near-term, urgent solutions that can be rapidly developed, tested, and deployed for industry use, and the long-term, complex advanced technologies that must transition through the scientific peer-review process and technology maturation levels before they can be deployed. Whether solutions are developed for the near term or long term, research for protection of the grid and energy infrastructure should be based on real-world operational requirements and cybersecurity gaps.

INL has unique insight into these real-world operational requirements, because on any given day, INL experts can be found in multiple locations across the U.S. working with industry to protect the grid and other critical infrastructure. Multidisciplinary teams of cybersecurity, control systems, wireless, power management, and threat analysis are deployed to work collaboratively with power utilities, industrial product vendors, or other infrastructure asset owners. These teams enable discovery and analysis of gaps, such as the need for tools that provide effective and immediate assistance for incident response and recovery. Other gaps may lead to better defined requirements for a long-term solution that would eliminate future vulnerabilities and threats. INL's experts also uncover requirements during threat analysis briefings, cyber exercises and cyber training when we identify needs for improvements in information sharing and skills development.

With this technical and operational insight into near-term and long-term technology requirements, INL's Cybercore Integration Center is positioned to implement a research and development strategy that encompasses a broad spectrum of solutions for grid and energy infrastructure security. This strategy emphasizes that there is no single silver bullet solution; rather, solutions must address technologies, processes, and people. Cybercore Integration Center's priorities are a holistic research and development strategy, which pursues advanced solutions that, when deployed, enable stakeholders to implement sustainable, cyber-informed decisions that harden infrastructure against the most sophisticated cyberattacks and the most unacceptable consequences.

Advanced Technologies: Examples of INL's progress in research and development of advanced technology solutions for grid and energy infrastructure protection and resilience are provided in the following bullets. These technologies emphasize opportunities to employ multiple technology disciplines (sensors, information and decision science, wireless, network architectures, etc.) to provide the benefits of machine-to-machine speed and automation in responding to cyber intrusion or attack.

- Automated threat response for industrial control systems can result in improved capabilities to prioritize threats and exploits, reduce the time to discover and recover from illicit behavior, and increase resiliency of the electric grid. In collaboration with Lawrence Livermore National Laboratory, New Context, and the other industry partners of the California Energy Systems for the 21st Century (CES-21) Program, INL is conducting research with machine-to-machine automated threat response (MMATR) concepts and technologies. One essential

concept within MMATR research is machine-readable Indicator and Remediation Language (IRL) generation. This concept will enable control system devices to have capabilities for early detection of abnormal behavior, and then with machine-speed, remediate an exploit before the exploit has an impact. This concept, as well as others for automated response capabilities are currently being tested on physical test beds consisting of actual utility grid controls and security equipment. INL's experimental infrastructure to test and demonstrate at-scale provides unique capabilities to measure and understand a new technology's performance through normal operations, equipment malfunctions, system degradations, and failure events.

- To address increasing demand for real-time cyber intrusion monitoring and immediate cyber event response, INL is pursuing a variety of autonomous technology solutions for protecting operational technology (OT) systems and networks (e.g., industrial control systems (ICS), programmable logic controls, supervisory control and data acquisition systems (SCADA), etc.). One of INL's innovations in cybersecurity automation includes the INL Autonomic Intelligent Cyber Sensor (AICS). AICS is an example of an OT tool that can be used to protect the grid and energy infrastructure by enabling system owners to more easily design, implement, and monitor cyber secure control system networks. AICS uses autonomic computing techniques and a service-oriented architecture to: a) automatically discover network entity information, b) automatically deploy deceptive virtual hosts (dynamic honeypots), and c) automatically identify anomalous network traffic with very high accuracy. The continued advancement of AICS towards deployment through DHS's Transition to Practice Program is an excellent example of maturing an INL Laboratory Directed Research and Development Program (LDRD) research project through the levels of technology readiness.

- The U.S. grid, energy infrastructure, and electric vehicles are evolving rapidly to rely more heavily upon wireless communication technologies. This increased reliance on wireless technology introduces the potential for vulnerable access points for malware intrusion into the electric grid and energy infrastructure. To explore potential wireless vulnerabilities and eliminate consequences from a wireless cyberattack, INL is performing wireless cyber research on a protection technology, WiFIRE, through our Laboratory Directed Research and Development (LDRD) Program. Researchers are making significant progress in the early stage research and proof-of-principle testing of a prototype for real-time monitoring of radiofrequency spectrum use and characterization of communication protocols. WiFIRE has the potential to serve as an early warning sensor for wireless-based cyber intrusion to assure the confidentiality, integrity, and availability of wireless communications. WiFIRE is being designed for the protection of approved for current and future radiofrequency spectrum allocations such as the allocations assigned for Smart Grid communications networks, electric vehicle wireless charging systems, and vehicle-to-vehicle (V2V) technologies. This technology also will have capabilities for next-generation wireless communication systems and the detection of illicit use of spectrum.

Advanced Engineering Processes and Operations: Examples of our progress in research and

development of cyber-informed engineering protections of the electric grid and energy infrastructure are provided in the following bullets. These advancements enable asset owners and the operational defenders of critical infrastructure to assess their systems and operations to optimize their operational technology cybersecurity posture within their current and future systems by engineering in cyber secure designs and barriers, and engineering out vulnerabilities and attack pathways.

- Many asset owners are burdened with the unsustainable, day-to-day responsibility of detecting and responding to an increasing load of cyber exploits on their information technology (IT) and operational technology (OT) networks. Hence, INL developed Consequence-driven, Cyber-informed Engineering (CCE) to assist asset owners in understanding the actions they can take that will have the most beneficial impact in reducing risk to assets, operations and services/products. CCE provides asset owners with a methodology to implement an effective and efficient cyber investment strategy that is based on sound engineering principles and credible threats. The CCE guided methodology leads an organization through the steps required to protect their most essential processes from the most capable cyber adversaries. CCE fully leverages an organization's deep engineering expertise, including intimate systems and process knowledge, to engineer out the cyber risk with greatest consequence. The unique value of CCE is achieved when stakeholders complete the four-phase process: a) identify the highest consequence events; b) conduct a system of systems breakdown to identify all digital components and systems within the target environment; c) perform an ICS Cyber Kill Chain analysis to identify likely attack vectors and end effects, including assessment of current threat actors' capabilities; and d) prevent the high consequence event through cyber-informed engineering mitigations that disrupt the kill-chain. INL recently completed the initial pilot study of this advanced engineering process with a major U.S. electric power utility through a Cooperative Research and Development Agreement (CRADA). The pilot study was completed to mature the methodology and determine the potential value of CCE to assist utilities with assessing vulnerabilities and implementing solutions to cyber threats. With the discoveries and lessons learned of this first CCE pilot, INL is evaluating pathways to increase exponentially the availability and use of CCE through publications, train-the-trainer courses, and industry licenses. CCE results were briefed to the Section 9 electric utility partners and key U.S. intelligence community representatives. Intelligence threat analysts are evaluating the pilot study's findings, recommended mitigations, and lessons learned to determine if there are opportunities to enhance future threat analyses to protect grid and energy infrastructure.

- In support of the Department of Energy Office of Electricity Delivery and Energy Reliability's (DOE-OE) efforts to enhance grid and energy infrastructure security, INL is participating in multiple research initiatives with utilities. The goal is to enhance the value of cyber threat information sharing, and to expand information sharing for protection of operational technology (OT) networks. These initiatives focus on new analytical tools and information sharing approaches for the grid and energy infrastructure operators to determine what to monitor, how to collect and process data, and how to share sensitive data while protecting privacy. The results from these pilots will inform the development of a repeatable, standard

approaches that the utilities across the entire electric grid enterprise can use for operational threat data sharing and analysis.

- The Controller Area Network Bus (CAN Bus) protocol integrates the controls for powertrain, battery charging, transmission, antilock braking, air bags, etc., for automobiles, air, rail and marine transportation. To advance secure use of the CAN Bus protocol for electric vehicle connections to the power grid, battery storage systems, and vehicle-to-vehicle (V2V) networks, INL researchers are performing research to improve the cybersecurity of CAN Bus hardware and software. Success with innovations in CAN Bus will significantly reduce the cybersecurity risks associated with the automated control systems within automobiles, heavy transportation vehicles, aviation systems, and large electric generators – particularly when these new protections remove risks inherent to vehicles connecting with the electric grid. INL researchers are transitioning CAN Bus innovations towards deployment as part of research supported by DOE's Grid Modernization Laboratory Consortium and DOE's Technology Commercialization Fund.

Advances in Workforce Development: INL experts seek novel approaches to improve the effectiveness of knowledge transfer and information sharing by developing novel immersive learning environment methods and tools. Within our program portfolios for DOE, Department of Homeland Security (DHS), and other federal organizations, INL experts are in high demand nationally and internationally to provide education and training to elevate cyber skills and provide cyber awareness through sharing real-world knowledge and experiences. Examples demonstrating the progress in advancing the Cybercore Integration Center's objective for developing highly skilled, multidisciplinary cyber defenders and researchers, include the following:

- In response to a DOE-OE request for INL to provide critical knowledge transfer to utility operators related to the Ukraine power grid cyberattack, INL researchers designed, developed, and prototyped unique hands-on training devices. These "Ukraine-Event-in-a-Box" devices are designed to challenge course participants to defend against cyberattack on the equipment these participants routinely encounter within their power generation systems and power distribution substations. INL is exploring opportunities to make these training systems readily available for university engineering laboratories and industrial control room simulators.

- As part of collaborative university research in control system cybersecurity with the University of Tulsa, INL researchers developed a specialized educational tool. The credit-card-sized board is used as a cyber-skill teaching and assessment tool. This board includes various environmental sensors, data storage, input mechanisms and screen display features to develop expertise in forensic analysis. To increase access to students, INL is evaluating the potential for open source release of the board's proprietary control software.

- INL and DHS provide the ICS-CERT ICS Cybersecurity (301) control systems technical level training course for industry, government, and university participants. For over a decade, this

first-of-its-kind course has provided over 4,000 participants with hands-on training to discover who and what is on the network, identify vulnerabilities, understand how those vulnerabilities may be exploited, and learn defensive and mitigation strategies. This course includes a Red Team/Blue Team exercise that takes place within an actual control systems environment, and continuously evolves to address new learning methods, evolving threats, and protections.

- INL is partnering with educational institutions across the state of Idaho to build a pipeline for the future control systems cybersecurity expertise. INL, in collaboration with Idaho's three research universities, conducted a Cybercore summer camp – a three-day camp that provided high school students with hands-on experience using various ethical hacking techniques and methods. INL also assisted the University of Idaho in creating a graduate certificate in Critical Infrastructure Protection. This new graduate certificate, available in fall 2017, will educate current and future technology management, engineering, and computer science students on the challenges of protecting U.S. critical infrastructure.

The examples described within this testimony are provided to emphasize INL's progress in developing and deploying advanced technology solutions and to emphasize the key principles of the INL Cybercore Integration Center's holistic research and development strategy for control system cybersecurity innovation. These principles emphasize solutions focused on the development of the technologies, processes, and people required to protect electric grids and other energy infrastructure from cyberattacks. The principles include: a) multiple advanced technology innovations are needed when we are threatened by a sophisticated cyber-threat actor; b) advanced technologies that focus on autonomous detection and mitigation will be more readily accepted when stakeholders benefit from reductions in the costs and labor of cybersecurity, and the solutions provide timely and effective detection and mitigation of cyberattacks; c) advanced engineering technologies should enable cyber-informed design of processes, operations, and systems that have engineered-in cyber protections and engineered-out cyber vulnerabilities; d) advanced solutions must support the building of a nationwide, multidisciplined control systems cybersecurity workforce; and e) effective solutions should be based upon peer-reviewed science, use sound engineering principles and standards, and be tested and validated at-scale. INL encourages collaborations and partnerships because advanced technology solutions will arise from all sources – industry, entrepreneurs, academia, government, and laboratories.

I thank the Committee's members for this opportunity to share our strategy and provide examples of the progress we are making in meeting the dynamic evolution and technical complexity in identifying and mitigating threats to the electric grids and energy infrastructure. Your strong support for discussions of the opportunities and benefits of long-term research and development will result in effective and sustainable solutions. The written examples of our progress along with continued technology development from many others will lead to the solutions needed to protect the U.S. power grid and energy infrastructure from cyberattack. You have my commitment that INL will continue to pursue the realization of DOE's and INL's mission and strategy to meet the national objectives for protection of the grid. Thank you.

The CHAIRMAN. Thank you, Mr. Tudor.

Dr. Earl, welcome.

STATEMENT OF DR. DUNCAN EARL, PRESIDENT & CHIEF TECHNOLOGY OFFICER, QUBITEKK, INC.

Dr. EARL. Thank you and good morning.

Madam Chair Murkowski, Ranking Member Cantwell, members of the Committee, I am Dr. Duncan Earl, President and Chief Technology Officer at Qubitekk. Thank you for inviting me to appear before you today to discuss the role quantum technology can play in protecting our electrical grid.

The U.S. electrical grid has operated for nearly 150 years without experiencing a large-scale, long-term blackout. This is a testament to the hard work of the men and women who maintain the grid as well as the many smart devices that we depend on to monitor and control it.

However, the grid has never faced a threat of the type and severity as it is experiencing today. Over 70,000 power substations throughout our country depend and rely on smart devices to maintain the delicate balance between energy generation and energy demand. Effective coordination between these devices is only possible when they share data that is accurate and uncompromised.

Unfortunately, as we have seen in other countries, the ability of hackers to infiltrate grid networks and corrupt these communications is real and growing. To prevent a devastating attack on our own nation's electrical grid, we must implement the best cybersecurity solutions possible to protect sensitive grid communications.

If you ask utilities today, "At this very moment, are your communication channels secure?" many will admit that they do not know. A new technology, quantum technology, can allow them to answer, "Yes."

Quantum technology enables communications that cannot be intercepted or altered. Any attempt to do so can be immediately detected and thwarted. Fundamentally different from past solutions based on mathematics and software, this new solution is rooted in physics and uses hardware to create a trusted channel that is secure today, tomorrow, and a thousand years from now.

Quantum technology uses the laws of quantum physics to generate secret keys that cannot be cracked. The keys are transmitted as light through optical fibers to devices in the field. Although quantum physics, with the demonstrations of teleportation and particles existing in parallel universes, can sound like science fiction, its application to grid security is real and near-term.

At Qubitekk, with funding from the Department of Energy Office of Electricity's Cybersecurity for Energy Delivery Systems, or CEDS, program, we are conducting preliminary tests of quantum technology with utilities in California and Tennessee. In 2018 and 2019, larger pilot testing within substations is planned. We are also working closely with our industry and national laboratory partners to develop protocols that allow traditional communication solutions to integrate with these new quantum systems.

To speed the adoption of this technology, though, will require government action. With government support, a nationwide quantum-protected network between our substations can be built, cre-

ating an impenetrable shield around our grid's communication channels. With increased funding to existing DOE programs, quantum-enhanced cybersecurity solutions can be developed to protect every substation in our country. Ultimately, as occurred with the Internet, early government investment in communication infrastructure and equipment will be needed.

Finally, Senators, let me suggest the most important reason yet why we must embrace and pursue quantum technology, and I'll echo what Senator Murkowski said. China has already developed and installed the foundations for a nationwide quantum network that leverages both fiber optic and satellite-based communications. Last month they demonstrated the first-ever quantum secured video call between China and the European Union. Earlier this month, they committed $10 billion to the creation of a massive new quantum information laboratory in Eastern China. Although much of the basic science in quantum technology was developed here in the United States, our hesitation in its implementation has left us far behind in the quantum race.

Quantum networks are just the beginning of the quantum revolution. Quantum technology will revolutionize cybersecurity, computers, artificial intelligence, chemistry, medicine, and ultimately, the world economy. Building a quantum-protected grid will not only strengthen America's security but will also create a sustainable first market for quantum technology here in the U.S. It represents a significant step toward challenging, and eventually overtaking, our counterparts in Asia and the European Union.

With that, I look forward to your questions on this technology.

[The prepared statement of Dr. Earl follows:]

Dr. Duncan Earl
President & Chief Technology Officer
Qubitekk, Inc.

Opening Statement to the Senate Energy and Natural Resources Committee Hearing - October 26, 2017

Madam Chairman Murkowski, Ranking Member Cantwell, Members of the Committee. I am Dr. Duncan Earl, President and Chief Technology Officer at Qubitekk. Thank you for inviting me to appear before you today to discuss the role quantum technology can play in protecting our nation's electrical grid.

The U.S. electrical grid has operated for nearly 150 years without experiencing a large-scale, long-term blackout. This is a testament to the hard work of the men and women who maintain the grid as well as the many smart devices that we depend on to monitor and control it.

However, the grid has never faced a threat of the type and severity as it is experiencing today. Over 70,000 power substations throughout our country rely on smart devices to maintain the delicate balance between energy generation and energy demand. Effective coordination between these devices is possible only when they share data that is accurate and uncompromised.

Unfortunately, as we have seen in other countries, the ability of hackers to infiltrate grid networks and corrupt these communications is real and growing. To prevent a devastating attack on our own nation's electric grid, we must implement the best cybersecurity solutions possible to protect sensitive grid communications.

If you ask utilities today, "At this very moment, are your communication channels secure?" many will admit that they do not know. A new technology - quantum technology – can allow them to answer, "Yes."

Quantum technology enables communications that cannot be intercepted or altered. Any attempt to do so can be immediately detected and thwarted. Fundamentally different from past solutions based on mathematics and software, this new solution is rooted in physics and uses hardware to create a trusted channel that is secure today, tomorrow, and a thousand years from now.

Quantum technology uses the laws of quantum physics to generate secret keys that cannot be cracked. The keys are transmitted as light through optical fibers to devices in the field. Although quantum physics, with its demonstrations of teleportation and particles existing in parallel universes, can sound like science fiction, its application to grid security is real and near-term.

At Qubitekk, with funding from the Department of Energy Office of Electricity's Cybersecurity for Energy Delivery Systems program, or CEDS program, we are conducting preliminary tests of quantum technology with utilities in California and Tennessee. In 2018 and 2019, larger pilot testing within substations is planned. We are also working closely with our industry and national

laboratory partners to develop protocols that allow traditional communication solutions to integrate with these new quantum systems.

To speed the adoption of this technology, though, will require government action. With government support, a nationwide quantum-protected network between substations can be built, creating an impenetrable shield around our grid's communication channels. With increased funding to existing DOE programs, quantum-enhanced cybersecurity solutions can be developed to protect every substation in our country. Ultimately, as occurred with the Internet, early government investment in communication infrastructure and equipment will be needed.

Finally, Senators, let me suggest the most important reason yet why we must embrace and pursue quantum technology. China has already developed and installed the foundations for a nationwide quantum network that leverages both fiber optic and satellite based communications. Last month they demonstrated the first-ever quantum secured video call between China and the European Union. Earlier this month, they committed $10 billion to the creation of a massive new quantum information laboratory in Eastern China. Although much of the basic science of quantum technology was developed here in the United States, our hesitation in its implementation has left us far behind in the quantum race.

Quantum networks are just the beginning of the quantum revolution. Quantum technology will revolutionize cybersecurity, computers, artificial intelligence, chemistry, medicine, and, ultimately, the world economy. Building a quantum-protected grid will not only strengthen America's security but will also create a sustainable first market for quantum technology here in the U.S. It represents a significant step toward challenging, and eventually overtaking, our counterparts in Asia and the European Union.

The CHAIRMAN. Thank you, Dr. Earl.
Mr. Riedel.

STATEMENT OF DANIEL RIEDEL, CEO AND FOUNDER, NEW CONTEXT SERVICES, INC.

Mr. RIEDEL. Good morning.

Chairman Murkowski, Ranking Member Cantwell and the other members of the Committee, it's an honor and privilege to testify. My name is Daniel Riedel. I'm the CEO and founder of New Context Services. New Context was founded in 2013 with a vision of keeping the connected world safe. Our mission is to use lean security to automate the orchestration, governance and protection of critical infrastructure.

New Context is working with Southern California Edison, Pacific Gas and Electric, and San Diego Gas and Electric, in a partnership with Idaho National Lab and Lawrence Livermore National Lab in advanced cybersecurity research for machine-to-machine threat detection and response referred to as California Energy Systems of the 21st Century. That work has resulted in our involvement in the STIX/TAXII and OpenC2 standards that are becoming the default for governmental agencies, enterprises, and information sharing communities to distribute threat intelligence. New Context also offers secure engineering services to many industrial and financial services firms.

There are five cyber-defense areas I will be discussing today: Identity, Trusted Data, Attributed Isolated Networks, Threat Detection & Sharing, and Automated Response & Remediation.

Twenty billion IoT devices will soon be connected to the internet to grow our economy. At the same time, Smart Grid technologies are being rolled out to the energy grid. Organizations such as General Electric, ABB, and Siemens are building new technologies to create efficiencies in our nation's demand for electricity.

Each of these technologies are going to add new vectors of attack while at the same time current attacks are increasing in number. Some of these attacks have physical consequences such as black energy in the Ukraine.

Over 80 percent of all attacks are the result of stolen credentials. Credentials are a weak link in cybersecurity. We must move to multi-factor, biometric, and continuous authentication for all individuals who interact with critical infrastructure.

For each human, device, or application that attaches to critical infrastructure, we must strengthen the validation for the authority to operate. Rolling out more advanced processes of attribution across the energy grid faces these challenges: current credential technology, current IT practices, legacy applications, and the age of the equipment. Within critical infrastructure networks we must trust the data that is used in the decision-making process. Blockchain frameworks can provide this trust. Cryptographic trusted data can be used for a variety of use cases in the energy grid.

Isolated networks are used effectively as a method of network separation. However, insider threats and malware can still operate within that network. To build an attributed isolated network, we have to look at every device on the network to ensure identity of the operator and the operational history of that device. With

stronger identity, we can strengthen legal evidence to more effectively prosecute malicious attacks.

The ability to identify and share threat data at machine speed helps prevent the spread and propagation of attacks. Early in our work with CES-21, New Context identified STIX to be the best format for sharing threat intel and remediation data. New Context has begun working with the STIX community and the energy industry to extend STIX for the grid. STIX is just the first step; we now need the ability to share threats and remediations automatically between organizations. Several information sharing organizations have begun, but we still heavily rely on human analysts. If there were a coordinated attack on the grid those analysts would not be able to respond. To continue to advance threat intel we need to use new technology such as artificial intelligence to speed up the response.

Discovering and sharing threats at machine speed is a huge step in the right direction, but the logical next step is an automated response remediation. The first hurdle in automated response is trust by third party. We will need to ensure that there is trust in remediation. Once we have been able to solve for that trust, then our utilities, national labs, and agencies can distribute the remediation to the energy grid. These remediations can be deployed with the utility networks allowing them to rapidly respond to attacks.

In summary, Identity, Trusted Data, Attributed Isolated Networks, Threat Detection & Sharing, and Automated Response & Remediation are technologies to focus on for advanced cyber defense. The battlefield continues to change, and we need to look at new ways of protecting our infrastructure.

Our adversaries are formidable, and the challenge to the organizations is the high cost of defending their assets while the cost to attack them is low. This is a hidden tax on our economy that will continue until we address the root cause instead of the symptoms.

Investing in these technologies will lower the cost to defend our infrastructure and raise the cost to attack our infrastructure. This will allow more innovation in our industry and allow us to build the appropriate framework to welcome these 20 billion devices.

Thank you for the opportunity to testify. I look forward to today's questions.

[The prepared statement of Mr. Riedel follows:]

NEW CONTEXT New Context Services, Inc
717 Market Street, Suite 200, San Francisco, CA 94103

Senate Committee on Energy and Natural Resources
Full Committee Hearing to Examine Cyber Technology and Energy Infrastructure
October 26, 2017

Chairperson Murkowski, ranking member Cantwell, and the other members of the committee, it's an honor and a privilege to testify before you today. My name is Daniel Riedel, and I'm the CEO and Founder of New Context Services. New Context was founded in 2013 with the vision of keeping the connected world safe. Our mission is to use Lean Security to automate the orchestration, governance, and protection of critical infrastructure.

For the past three years we have been working closely with Southern California Edison, Pacific Gas and Electric, and San Diego Gas and Electric, in partnership with Idaho National Lab and Lawrence Livermore National Lab, to assist in advanced cyber-security research for machine-to-machine threat detection and response within the energy industry. This project is referred to as California Energy Systems for the 21st Century. That work has resulted in our involvement in the STIX/TAXII and OpenC2 standards that are becoming the default for governmental agencies, enterprises, and information sharing communities (ISAOs & ISACs) to distribute cyber-threat intelligence rapidly.

Beyond working with utility companies, New Context offers secure engineering services to many industrial and financial service firms, to build and scale their infrastructures securely through our methodology, Lean Security.

There are five areas of advanced cyber-defense that I will be discussing in my testimony:

- Identity
  - Advancing authentication credentials by moving beyond static username and password, with just one other factor (commonly referred to as two-factor authentication) to multi-factor biometric and continuous authentication solutions.
- Trusted Data
  - Looking at advanced ways of using a cryptographic ledger to be able to secure and validate that data has not been manipulated. Additionally, cryptographic ledgers allow for the ability to assure data across multiple third party organizations and supply chains. This is popularly referred to as blockchain.
- Attributed Isolated Networks
  - Isolated networks have helped in protecting data, but they are still a hard outer shell, and many of the vulnerabilities that affect the public internet exist within those networks, from credential theft to malicious network activity. Advancing technologies and software to ensure that every actor is accounted for on that network creates a higher level of assurance that doesn't exist today.

- Threat Detection & Sharing
    - Machine speed threat detection and threat sharing, enables the ability to identify and respond to threats faster, and to share intelligence with other utilities, agencies, and organizations in near real time.
- Automated Response & Remediation
    - This is the ability for the grid to automatically take action to prevent potential devastating consequences to itself. Automated remediation is a key technology we are developing, it allows the grid to self heal in the event of well orchestrated cyber attack. If we are to continue to innovate and add new intelligent devices to the energy grid, we have to allow for automated response as the complexity will surpass the human ability to respond.

In the next few years, 20 billion IoT devices will be connected to the internet, and powered up to continue the support and grow of our economy and society. At the same time, Smart Grid technologies are being rolled out to utilities to modernize the energy grid. Organizations such as General Electric, ABB, Bosch and Siemens are building new ways of managing and responding to data, to create greater efficiencies as our nation's demand for power continues to grow dynamically.

Each of these technologies are going to add additional vectors of attack to an already complex environment. As the US modernizes its electrical infrastructure, we are also seeing an unprecedented number of cyber attacks that have been launched against organizations around the globe, including utilities. Those attacks have started to have physical consequences, as seen in the Black Energy attack on Ukraine's critical infrastructure.

Each of the five areas I will be discussing - Identity, Trusted Data, Attributed Isolated Networks, Threat Detection & Sharing, Automated Response & Remediation, all help build a stronger grid that allows for greater innovation and flexibility, while addressing more complex and sophisticated cyber attacks.

Identity

Over 80% of all cyber attacks are the result of stolen credentials. Credentials are one of the weakest links in cyber security today. We need to move to multi-factor, biometric, and continuous authentication for all individuals who interact within critical infrastructure. Current credentials and roles are still vulnerable to many types of phishing and spear fishing attacks, and two-factor authentication still has challenges. This level of authentication needs to extend beyond human authority to devices, applications, and systems.

For each human, device, or application that attaches to critical infrastructure, we will need to make sure to validate for identity, and authority to operate on that network. It is important to establish attribution early, by identifying the actors and devices, upon inception, to the network. Then we need to continually monitor those identities proactively, continually giving assurance. Based on early attribution we can establish identities before their actions, as opposed to discovering malicious activity, and then trying to establish attribution through forensics.

This is no easy feat to do and there are several factors to overcome. Rolling out a holistic process of attribution across the energy grid faces these challenges: current credential technology, current methodologies in IT, legacy applications, legacy devices, and the age of equipment.

Trusted Data

Within critical infrastructure networks, it is vital that we trust the data that is used in any decision making process. We protect that data today by running isolated networks, limiting interaction and control to devices. This is a good step, but we need to be looking at advanced threats that target the data, and manipulate its output, potentially causing devices and operators to make harmful decisions that have drastic consequences to the energy grid. These attacks could be made more powerful with automation, and the use of artificial intelligence to coordinate across many utilities at one time. To my knowledge no such attacks have taken place, but we should work to prepare against such a threat.

Building trusted data platforms means that we need to build in the ability to prove the data has not been altered at any point. Some research has pointed toward blockchain frameworks to prove this level of trust and certainty. This approach to building trusted data can be used for a variety of use cases within the energy grid. One such use case would be analytics used to make key decisions, or another use case such as supply chains where we need to guarantee there has been no altering of data between third parties.

Attributed Isolated Networks

Isolated networks are used relatively effectively today as a method of network separation, and security from threats on the open internet. However, insider threats and malware operate within the borders of the isolated network. This means we have to make sure that we build a chain of trust between all the devices and actions that happen on the network.

To build an attributed isolated network, we have to look at every device on that network and ensure that we know who is operating it, who is programming the software on it, and the entire history of the operation of that device. I would like to emphasize that we are always looking to get to the actual persons involved in the actions including the operators, and engineers. If we can move to world of whitelisting applications and devices based on our knowledge of it actions and history, including the applications residing on it, then we have assurance that we can find who is responsible for a given action. Once we have that actor we can then follow with legal recourse and evidence that allows us to prosecute malicious actors. We are a long way from having this level of transparency but this allows far greater assurance than we have today. It's not impossible to do this, it's just difficult but the outcome allows for a much more frictionless operational environment.

To build the history of operation trusted data technologies such as blockchain could allow us to be able to create cryptographic ledgers, that we can use to write the history of all the actions that are taken within a network, providing a much higher level of certainty for legal action against malicious behavior.

Threat Detection & Sharing

The ability to identify and share threat data at machine speed is another advanced strategy to respond within a time frame that prevents the spread and propagation of malicious attacks. Early in our work on CES-21, New Context identified Structured Threat Information Expression (or STIX, a structured language for describing cyber threat) to be the most applicable format for the energy industry. New Context has been working with the STIX open source group and the energy industry to make sure STIX is adaptable for the grids needs. STIX is backed by DHS and numerous commercial vendors.

STIX is just the first step; we now need to build the ability to rapidly share threats and remediations between organizations. Several information sharing organizations have taken initial steps to build out these capabilities, but most current practices still heavily rely on human analysts. If there were to be a coordinated attack on the grid, it is likely those analysts would not be able to respond to it in a timely fashion. To continue to advance threat intel we need to use new technologies such as artificial intelligence (AI) to help reduce the noise to human analysts and assist in making more rapid decisions.

Automated Response & Remediation

Discovering and sharing threats at machine speed is a huge step in the right direction, but the logical next step is to take automated actions against an overwhelming and rapid attack, we have to look at automated response. Automated response is a significant challenge for many reasons.

The first hurdle is how do we trust in the actions that are being recommended by a potential third party. We will need to ensure there is trust in the remediation about to be performed, which is why Identity, Trusted Data, and Trusted Networks are vital. Once we have been able to solve for trust, then our utilities, national labs, and agencies can distribute a remediation to the energy grid. These remediations can then be deployed within the utility networks, allowing them to be ready for anomalous behaviors and respond before potential instability in the network.

In summary, Identity, Trusted Data, Attributed Isolated Networks, Threat Detection & Sharing, and Automated Response & Remediation are technologies to focus on for advanced cyber defense. The battlefield continues to be changing, and we need to constantly look at new ways of protecting our infrastructure.

Our adversaries are formidable, and the challenge to most organizations is that the costs of defending their assets are high while the cost to attack is low. This is a hidden tax on our economy that will continue until we address the root cause instead of the symptoms.

Investing in these technologies will lower the cost to defend our infrastructure, and raise the cost to attack our infrastructure. In the end, it's an economic game and any investment into better more effective solutions that address the core problems of cyber security instead of the symptoms, will significantly lower the cost of defense. This will allow more innovation in our industry and allow us to build the appropriate framework to welcome these 20 billion devices and applications to operate on the energy grid safely.

Thank you for the opportunity to testify. I look forward to the questions for today's hearing.

The CHAIRMAN. Thank you, Mr. Riedel.

Thank you, all of you. Very interesting testimony, very important testimony. We just really appreciate it.

I think we look to some of the breakthroughs that are out there and these technologies that we hope will allow for that level of protection, but many, several, of you have spoken to the human factor. We recognize that most of the control systems today are separated from the public internet by a firewall or an air gap, but we can still see intrusions through human error, whether it's transferring data via a flash drive from a public network to a secure one or vice versa. So even with all of the advances that we have out there and the processes that you have mentioned, we are still in a situation where we have exposure to security breach.

Dr. Raines, you mentioned the Dark Net. How do we work to protect the Dark Net from this type of activity, the breach through the human factor?

And then I also want you, Dr. Earl, to speak a little bit—you mentioned the quantum technology that I had raised in my opening, and you have suggested that a quantum protected network will create an impenetrable shield around our grid's communication channels. But does that apply to the insider threats as well? I am interested in this aspect. Technology is great; sometimes it is the human factor that is our weakest link.

Dr. RAINES. Thank you, Senator, for that question.

Addressing, first of all, the human link, certainly it's going to be with us. And so, how do we take and do better education and training of people who have not been exposed, historically, to these types of things?

We have a lot of folks in the industry that are very good at operationally providing those capabilities and safety paramount. But when you start talking about cybersecurity, it's a little bit of a foreign issue in terms of some of the industry partners out there.

So, how do we take and raise this awareness so that, you know, they understand the threats that exist? Additionally, from a standpoint in making sure that the systems are patched, updated, these are mainly IT type systems that are being utilized. So there are steps that we can take from that standpoint to help out the industry.

With regards to the Dark Net concept that we're proposing here, moving the command and control communications away from the internet, at least, separates, as you mentioned before, air gapping, if you will. There are exploits that get across air gaps as we know, but having separate control and communication capabilities via these fibers, as was mentioned by Dr. Earl, will give us some enhanced capabilities to understand and immediately determine if there was any type of exploitation that may hit. So as long as we can take and have that separation that we don't connect back or add additional vectors for exploitation, we believe that there's going to be that added level of security that can occur by going to the separate, secure, if you will, dark fiber implementation and advanced communication capabilities as well, that we would implement, but——

The CHAIRMAN. Let me ask Dr. Earl to speak on the quantum technology side and the vulnerabilities there.

Dr. EARL. Yeah, absolutely.

So, quantum technology is a very powerful technology, but the grid is going to require many solutions. It's just a piece of that puzzle.

However, quantum technology solves two very important problems, and it's the foundation upon which you can build a more secure grid. The first is it provides a way to immediately detect if somebody is tampering with your communication channels, and the second thing that it can do is it can provide encryption that cannot be broken. There always is a concern about insider threat. Quantum technology doesn't address that. It addresses the securing of channels, but you need that first before you can build up the rest of the solution.

The CHAIRMAN. So very quickly on the quantum technology. You have mentioned the traditional systems can be integrated. How easy is it to do that?

You have technology—does the technology need to be built into the grid during its development or is it relatively easy to add it to existing structure?

Dr. EARL. We can retrofit it, and we argue that it's actually easier than other approaches that we might use for the internet for securing and establishing secret keys among devices. So, it is very grid centric. It is very easy to implement and retrofit.

The CHAIRMAN. Okay.

Senator Cantwell.

Senator CANTWELL. I would like to yield to my colleague for a question.

Senator RISCH. Thank you. I appreciate that.

Senator CANTWELL. He is going to go take care of us in small business——

[Laughter.]

——which probably should be part of this discussion.

Senator RISCH. As you know this is Women's Small Business Month, so the hearing is on that. I knew you would be very interested in that.

Senator CANTWELL. Good. And I am sure this subject interests you too, as we talk about solutions on cyber where you have to think about how we help small businesses.

Senator RISCH. That is true.

Senator CANTWELL. Because they have the least ability to put some of these things in place. So we need to think about that.

Go ahead. I'm sorry.

Senator RISCH. Thank you so much.

Mr. Tudor, you mentioned the CCE methodology during your testimony. You also provided written testimony, and I have not had a chance to look at that yet. Do you expound on that methodology in your testimony that you have submitted?

Mr. TUDOR. I did, sir.

Senator RISCH. Okay.

That methodology was first introduced as INL's unique cybersecurity innovation in April by Mr. Andy Bachman to this Committee. Since then it has attracted some positive attention. But in addition to that, it seems to have created some confusion, indeed some might even say criticism, that discussing whether it is really

a process that is a step backward from technology innovation. Could you address that, please?

Mr. TUDOR. Sure. Thank you for your question, Senator.

We feel that Consequence-driven, Cyber-informed Engineering, or CCE, is actually a step forward in some of our engineering processes in that we look to use the right technology, you know, for the right purpose and implementation of cyber controls.

I think some of the criticism has been about the mention of using analog devices as if it's a step back into the Stone Age. But in some of these cases we can use the CCE methodology to understand those critical consequences and the attack paths that lead up to them.

We can identify choke points for various of these different attacks and do what we call disruption zones, areas where we can place a discreet, non-programmable component, potentially an analog component, that can't be hacked by software means, doesn't have software vulnerabilities in it. And then, we'll just drive that attacker work factor, you know, way up because their normal methods of internet-based, of software-based activity will be thwarted at that point.

So as you work with an organization and, once again, this is not something that just the national lab or another provider can do. The organization that's being protected works very closely to understand what those consequences are, what their engineering processes are.

Identify those paths, work with them, understand who might potentially attack and what potential motivations there are. And then, develop those mitigating ideas and identify the disruption zones and implement them. We found with our partner that they felt that the entire process helped them give them a different perspective on how to protect their environments.

Senator RISCH. Thank you. I think that is a clear explanation.

Thank you, Madam Chairman. Thank you, Senator Cantwell, for yielding.

The CHAIRMAN. Senator Cantwell.

Senator CANTWELL. Thank you, Madam Chair.

I just want to thank all the witnesses again. This is excellent testimony across many fronts and, actually, the diversity of ideas yet cohesiveness of the ideas is so important. So I thank you for that.

I obviously want to thank Mr. Imhoff again for your leadership. You have helped the State of Washington provide on this, everything from working with our National Guard to creating a response to the technologies that we've been able to deploy.

I think when we think about this, the synchro-phasor technology that the lab has worked on and was part of your testimony actually saved California customers an estimated $360 million plus due to improved utilization of existing systems and making these tools more resilient to cyber threats.

We can see already there is work and application that is being done that is helping us strengthen the grid from blackouts, and we need to keep going.

Mr. Earl, the Department of Energy Office of Electricity's Cybersecurity for Energy Delivery Systems program helped fund the work that you are doing. I feel that one of the key aspects here is

the need to continue to do R&D and innovate and test and apply. I see you are all nodding on that. I guess that is what I am trying to help our colleagues understand here.

Sometimes I say in the information age we are only in the third inning of the ballgame. Here, I'm not even sure if we have started the game. Actually we have because of the great work that you all are doing.

But how would you characterize where we need to go with research, workforce, and this continued collaborative effort, in the context of where we are today and how this will evolve?

Mr. Earl, I think you said it, or Mr. Riedel did, that this is ever changing. Whatever we are doing today is going to change and evolve. So where are we with the level of investment and workforce and level of interconnected responses and I mean people responses that we need to build here?

Maybe we can just start with you, Mr. Imhoff?

Mr. IMHOFF. Thank you, Senator Cantwell.

It's a complex question. I would say on the Department of Energy side, programs like the CEDS cyber program at OE and others are funding a lot of the innovations here, several of them today, where the injection of funding is adding value.

In terms of the grid modernization initiative, the Congress Appropriations, that initiative is strong and moving forward at this point in time.

I think one of the challenges, while we have over 100 industrial partners working on these projects, the public-private partnership is essential. You have to have the field validation so that the people, the operators, the switchmen, et cetera, understand and can get their arms around the new concepts so what they bring to bear, to offer.

The industry is a little challenged now because they're facing flat sales and a lot of challenges on cyber and other things. So industry is stretched thin from a human workforce standpoint. They have a challenge adding more things on to their plate.

But the manpower issue is part of that, clearly. The training, the access, the large number of utility workers who are retiring, and there's a lot of work in terms of development and feeding the pipe for the next generation, whether it's cyber or other grid activities. So I think it's all very closely interwoven in terms of getting the workforce right, getting the training done.

And I would say that there are many, some of the new topics around analytics and other things are new dimensions that need to be added, I think, to the workforce, focus that needs to go beyond just enterprise cybersecurity, which, I think, has been the dominant focus for, let's say, the past decade.

We're having a hard time keeping up with the volume of cyber analysts, but we're—they now need to have new skills in terms of advanced analytics and other things. So we need to look to how do we refresh those, curricular development. How do we build the partnerships between public and private to train people, cross-train existing employees or develop new staff and continue to look for those public-private partnerships on field validation of new concepts coming out of the R&D portfolio? Because that's what it takes

at the regional level for commissioners and utility commissions and others to get comfortable with making the investments to deliver.

Senator CANTWELL. Thank you. It might have been a complex question, but you did a very good job.

Anybody else want to weigh in quickly on that?

Mr. RIEDEL. I can briefly.

Thank you for the question, Senator Cantwell, Ranking Member, sorry.

So we deal with this a lot with our company. We're trying to hire qualified people, and finding enough qualified people out there is, I think, a challenge for every organization.

We try and train and make sure that everyone understands that security inside of an enterprise or in a corporation is not one person's ability or one person's responsibility. So the things that we look at are how do we educate our workforce? We would love to work with schools and universities to make sure they're educating folks.

I think that the thing that we will try to tell enterprises as they deal with this, and utilities as they deal with this, is that security, cybersecurity, is a group responsibility, that you cannot just expect the security professionals to take care of this. You need to take ownership of that while you build and engineer your products. And so, those are things that we are looking at.

The only thing I would add to that is, you know, our focus is automation. We want to be able to be able to roll out this automation that we talked about today into the grid, but to do that we have to be able to trust that we understand where that automation comes from.

So not only do we have to make sure that we educate and bring these people to be professionals, we also have to make sure as we bring them on to our networks and as we have them work on those networks we're able to identify those people so we can trust the information that they're giving us and then trust the remediations they create.

Senator CANTWELL. Thank you.

Thank you, Madam Chair.

The CHAIRMAN. Senator Cassidy.

Senator CASSIDY. Should it be one of those folks over there? I don't want to step out of place——

Senator MANCHIN. Bill, would you mind if I? I've got——

The CHAIRMAN. This is a cooperative Committee.

[Laughter.]

If Senator Cassidy doesn't mind, we will certainly turn to Senator Manchin.

Senator MANCHIN. This is a great Committee. Thank you.

The CHAIRMAN. It is.

Senator MANCHIN. I appreciate both of you. Thank you, Bill, I appreciate it.

Let me just say real quickly. The reliability of the grid system, basically the baseload, do any of you all have concerns that the baseload might not be able to energize the grid or we could be in concern about a relapse or a collapse? Does anybody have that concern?

From baseload, as I am understanding, nuclear, coal is to the basic baseload, 24/7, rain or shine. Gas—we are depending on gas being baseload now. And all of our renewables are coming on, I guess, with the new battery, the battery storage. That will eventually move into that. We have not gotten there yet.

You all have no concerns in different segments across the country? PJM about collapsed over the last polar vortex we had. You all knew that, right? They came within that sliver of going down.

Anybody want to talk?

Mr. IMHOFF. So, the—we've seen no evidence that there's a lack of capacity to deliver in terms of frequency response and other things on the power system.

Clearly there are changes in some of the resources mix. And the NERC bodies, as well as the reliability councils and all have not indicated that there is a gap that's an issue. But they're having to change some of the processes and all, but I think we are, have adequate capacity going forward.

Senator MANCHIN. Anybody? Feel the same?

Dr. RAINES. Senator, yes, sir.

Senator MANCHIN. Okay.

Dr. Earl, on quantum. You are talking about, you know, of course, cyber is what we are concerned about. I am on Intel and every meeting we have deals with cyber and some type of cyberattacks that we are getting regularly and how we can stave that off.

In this, I have been to an awful lot of the power plants and we have an awful lot of coal plants and then they are all switching stations. So when they produce, the power coming out goes into, kind of, a switching station, it, kind of, puts it out on the grid. And you are saying that you are quantum. You can protect that from the internet or being hacked by the internet, correct?

Dr. EARL. So maybe a slightly different way to define that.

We definitely are trying to protect the communications between those switching facilities, the substations, and command centers. It's imperative that you're able to trust those communications. And so, the channels that they're communicated over are not defended. These might be fiber optics, airwaves. You don't have complete control over those communication channels. So it's important we have a technology that can ensure that communication channel is secure first.

Senator MANCHIN. And you say that can be retrofitted also on this?

Dr. EARL. It could be, that's right, especially if it dovetails well with what they described, ONL described, about the Dark Net where you use existing OR, existing fiber optic cables, to basically put this system in place.

Senator MANCHIN. Let me ask any of you all who would answer this question because I have been to an awful lot of these power stations, however they are operated, but the switching stations, it is not all that secure. I could, if I wanted to do some kind of criminal act, I could walk up to it and make it happen. Have you all suggested or basically lobbied for securing, making every utility company responsible for the securing of those switching stations?

It could be natural gas also. We are concerned about the gas lines, the pipelines, pumping stations.

Mr. IMHOFF. So you're voicing concern around physical security?

Senator MANCHIN. Yes.

Mr. IMHOFF. We have extensive infrastructure across thousands of miles, and out West some of those are very lonely, empty miles.

Senator MANCHIN. Right.

Mr. IMHOFF. They are favorite target practice opportunities, but I will say that over the past year PNNL has worked with NERC to help develop what's called design basis threat which is a systematic approach at looking at what are the series of threats that could be done on a pipeline, gas pipeline, compressor station, or switch yards coming out of coal plants, et cetera, and then helping the utilities walk through and classifying the degree of consequence and risk and identifying what other options actually provide physical security because you can do that, but you can't do it on every single substation or every single transmission tower out there in the power system.

What they are doing is putting in place a systematic process to help prioritize those risks and identify their options for protection. That process is beginning, and it's been very well received by the utilities over the last 12 months. So I think they're moving in that direction, Senator.

Senator MANCHIN. Well, I was just going to say you all come from the technical end of it and can really help us there and advocate for this because I see a lot needs to be done. I mean, we are talking about the internet, and we are talking about technology and all this and that. I am talking about just plain attacks, just, I mean, criminal activities.

Okay, thank you very much.

Senator CANTWELL. If I could just follow up on that?

Isn't it true that most—I am just thinking of Bonneville's system. If you go into their command center, they have pretty good eyes on most of everything in their grid system. I would assume utilities are similar. They have eyes everywhere. Right? Is that correct? I mean, besides the technical detection of what is happening on a line, they also have eyes on practically every aspect of the infrastructure.

Dr. EARL. I think it depends a little bit on the utilities, you know. There's small ones and large ones and they approach it differently, but definitely for the larger utilities, I think, you're absolutely correct. It's a fairly sophisticated operation.

Senator CANTWELL. Thank you.

The CHAIRMAN. But we worry about some of those smaller ones like we have up North.

Senator Cassidy, we are over to you now.

Senator CASSIDY. Mr. Raines, I think it was you that spoke of the Dark Net. Does the Dark Net require a lane of different fiber optic cables or can it go through the same fiber optic cables?

Dr. RAINES. Thank you, Senator, for the question.

Certainly we can use existing fiber that is not being utilized because generally speaking there's a lot of bundles that are laid, multiple fibers that occur and not all the capacity is being used.

In the incidences where you have smaller utilities or cooperatives that don't have the fiber, there are other avenues that we look at in using some of the advanced communication capabilities and emerging capabilities to also take and look at hardening. But yes, sir, certainly we can utilize those existing fibers where they exist.

Senator CASSIDY. Could we overlay? To what degree could we now go to Dark Net?

I once went to a DoD facility and they have their internet here and they have their, kind of, closed system there. It was two different, I don't know if there are two different terminals, but somehow I understood this is this and that is that. To what degree do we have that now for utilities?

Dr. RAINES. Well, sir, I cannot answer in totality of that for you right now. We are having people that are looking at, as I mentioned before, over the 100,000 miles of existing fiber that we have, to see exactly where the connectivities are relative to, you know, the commercial entities, the industry out there. So, certainly, I can get back with you on that question, sir.

Senator CASSIDY. That is a nice segue to my next question. My staff gave me this from August 17, from the President's National Infrastructure Advisory Committee. They have 11 different recommendations.

There is a sort of, kind of, urgency behind it and a sort of assumption that we should have done this yesterday and we haven't done it yet, with agencies and Congress required to put things together which apparently we have not. So I appreciate the Chair and the Ranking Member holding these hearings, but to what degree is leadership being exerted by the Federal Government to make sure that all this happens ASAP? Because I gather you all think it should happen ASAP. Fair statement?

Mr. Tudor is smiling, kind of discreetly and diplomatically, but to what degree are we providing that leadership?

Mr. Tudor?

Mr. TUDOR. Thank you, Senator.

And I am nothing, if not discreet and diplomatic.

[Laughter.]

I would say that I do believe that the Department of Energy, the Department of Homeland Security, know this, are taking leadership within the bounds of what we were able to accomplish, what we understand that we should do, but I also think that leadership understands that we all can do more.

We've been, you know, working——

Senator CASSIDY. Let me just pause for a second because I have actually heard some very good suggestions from you all ranging from quantum mechanics which I, kind of, don't understand, but am always, kind of, fascinated by to put an analog switch in there. Really, kind of, two different approaches with a Dark Net overlay. Those are very tangible. This is what you could do now and would probably work really well.

What is the state of play? Are we now moving toward that or are we just waiting for someone to propose it?

Dr. RAINES. Well, sir?

Senator CASSIDY. Go ahead.

Dr. RAINES. If I may answer that for you.

One of the test cases that we're working with now is the electric power DoD out of Chattanooga which we have fiber connections with, and we're looking at how we can establish some of that test bed capabilities with them. So on a smaller scale we are moving forward.

Senator CASSIDY. So are you telling me although DoD has a parallel internet, and you mentioned the Dark Net, is this just something, is this a strong recommendation yes, we should be doing it, or no, we need to test it before we go fully to scale?

Dr. RAINES. Sir, we believe that the technology exists to increase our capabilities to defend the electric grid from a communications and control standpoint, if we go forward with this. And that's what we're proposing for——

Senator CASSIDY. And is that generally agreed upon?

So, one thing we could do is appropriate the dollars to immediately begin putting in a Dark Net for everybody who is connected to the grid, except maybe a distributed, you know, if I am selling electricity off the roof of my house, maybe not, but other than that. Is that something we should be writing in legislation now, in your opinion?

Dr. EARL. So we currently have utility partners with extensive fiber optic networks that are ready to start implementing this today or testing this today.

Senator CASSIDY. The quantum or the Dark Net?

Dr. EARL. The quantum and the Dark Net. It really is tied together. So, there's, now that's not all utilities, and it's going to have to start small and eventually grow.

Senator CASSIDY. Now, just let me ask you, just interrupt because when you say not all utilities. I always mispronounce it. I don't know if it is miso or myso. But you have this exchange of electrons through the whole Mississippi Valley. If there is somebody who is a weak link, who does not have Dark Net, does not have quantum, does not have analog, can that go through the whole network getting those that do have it?

Dr. EARL. So, ultimately, you're only as strong as your weakest link, but your biggest links need to be secured first. And the propagation can be limited by focusing there and prioritizing there, initially. And there are three separate grids, of course, that would be independent from one another.

But let me just, sort of, echo the question of, you know, can we implement this quickly? It is a question of funding.

The CEDS program within DOE is doing a great job, but they don't have a large enough budget, really, to take on Dark Net yet. So, at least from my perspective, I think that increasing the funding to that program is an excellent thing to do right away.

The other point I'd like to quickly make is these new technologies will take time to be implemented. It could be as long as, you know, five to ten years for some of these technologies to be implemented. If you think of where hackers were ten years ago and you think about where hackers are going to be in ten years from now, that's where the urgency is coming from. We really have got to get ahead of this.

Mr. TUDOR. I would like to say, though, that across the industry our utility partners are really beginning to move out even faster in

developing pilots, working with commercial and industry, working with national labs to develop the process and procedures to implement these new technologies.

Mr. Riedel mentioned the CES-21 is a great example of those three major utilities working together to implement and prototype and demonstrate these technologies and give lessons learned out to other utilities across the nation so we can understand what the scope of the issue is, how to deploy these, and then also provide that expertise as others do it, similar to other utilities here on the East Coast as well.

So I think we are moving out faster than we have been. We would all love to do it faster.

Senator CASSIDY. I am way over. I apologize, Senator Franken. I yield back.

The CHAIRMAN. Thank you, Senator Cassidy.

Senator Franken.

Senator FRANKEN. Thank you, Madam Chair.

I know this is about cybersecurity and the grid, but Dr. Raines, I was struck in your testimony by your discussion of microgrid technology and its potential application to Puerto Rico. The Chair knows that I am very interested in this, and I think all of us are. After the devastation of Hurricanes Irma and Maria, millions of Americans in Puerto Rico and the Virgin Islands are still without power. This is really inexcusable.

I am going to read from your testimony, "Most recently Oak Ridge National Laboratory has considered how its scientific expertise may be leveraged to help an area in which the local power grid is essentially being rebuilt from the ground up. Puerto Rico was devastated by Hurricane Maria last month. The island's critical infrastructure, including its power, transmission, and distribution grid serving more than 1.4 million customers was nearly demolished by the powerful storm.

As the relief and recovery effort continues, we are mindful that many of the solutions developed for grid resilience could be purposely built into a completely new, robust system for Puerto Rico through distributed energy resources, for instance, Puerto Rico Electric Power Authority could benefit from microgrids with more power generation spread throughout its territory, sited locally in neighborhoods and communities and providing greater flexibility when the larger grid is disrupted. Complementary opportunities exist to support the development of a more secure and resilient Puerto Rican infrastructure which will ultimately lead to a better quality of life for its residents and reliable electricity to support its businesses."

This is something that we have been talking a lot about, a number of us, including the Chair and the Ranking Member of this Committee.

Dr. Raines, could you elaborate on the work that Oak Ridge is doing to improve resilience for the grid and how that might relate to our responsibility after these hurricanes to approach rebuilding the grid, getting them up again, as fast as possible, but then building something that is resilient and sustainable? And if anyone else wants to weigh in on that, please do.

Dr. RAINES. Senator, thank you for the question. I'll start and turn it over to Carl.

Earlier this year in the spring we had a team down in Puerto Rico that was actually looking at the infrastructure, understanding the infrastructure and looking at how we could possibly take and redesign or enhance the architecture, the existing architecture. You know, we certainly did not foresee the devastation that occurred in September and the agony and things that people are going through there down there now.

We have, for a number of years, been looking at microgrid technologies. How we can take and build those where given different types of power electronics and charging and sensing type systems that they can have the isolation from other, the larger infrastructure and be able to operate in the events of——

Senator FRANKEN. In island mode if they need it.

Dr. RAINES. Yes, sir.

Senator FRANKEN. Okay.

Dr. RAINES. Yeah, from that standpoint.

And so, with that I know that Carl is leading an effort among the different labs and he can probably address it quite well as well.

Senator FRANKEN. Please?

Mr. IMHOFF. Specifically for Puerto Rico DOE has asked the 12 grid modernization laboratories to frame some options that could add value in the 1 to 6 months, 6 to 12 months and then 12 months to 5 years timeframes.

And the notion of evaluating what critical loads, in terms of drinking water purification, health care, communications, island communications, et cetera. How did they come down and identify where it might be worth the incremental expense for microgrids to harden those against future events and leverage some of the work that we've done in the grid modernization in New Orleans and other places on how to coordinate multiple microgrids that during bad storms can actually adjust and focus just on the critical loads for emergency applications? That's, I think, a good opportunity for us to bring new concepts to the rebuild of Puerto Rico over the next couple years.

Senator FRANKEN. I think it is just responsible to do that and smart to do that and, you know, their grid, and I know I am out of time, but their grid is right now powered so much by diesel and a lot of people from Minnesota in the winter go to Puerto Rico and the Virgin Islands for the sun. I am just saying. So I think that perhaps in rebuilding this grid we can make it more resilient and use more sustainable energy as well.

It is something that I am glad that national laboratories have been asked by the Energy Department to look at. I think everybody is rolling in the same direction is what I am saying. I feel good about that.

The CHAIRMAN. Thank you, Senator Franken. I think it was a good question, an important one.

We will be having a hearing focusing on the current situation in Puerto Rico and going forward, the future of that energy grid there, and we will look forward to input from the national labs.

To know that you have taken point on that, Mr. Imhoff, I think is important. We will look for more detail in the next couple weeks but it is very, very important. So thank you.

Senator Duckworth.

Senator DUCKWORTH. Thank you, Madam Chair. I want to thank you and the Ranking Member for today's hearing. And I definitely want to thank our witnesses for participating today.

And recently, as my colleague, Mr. Franken, mentioned, we have seen frightening weather patterns and infrastructure instability in Puerto Rico and in the Ukraine even in 2015 when malicious actors destabilized the country's power grid.

I had to learn that cybersecurity can take many forms. I come to this from a military perspective where it is all about enemies hacking, trying to attack you, but cybersecurity also applies to trying to prevent technological failures from occurring as well.

I am proud that the national labs are partnering with industry to develop solutions to modernize our grid, including Illinois' own Argonne National Lab. We are leading eight projects under DOE's Grid Modernization Laboratory Consortium. And we heard this earlier when you responded to my colleague from Louisiana about the investments that need to be made. That is where my question is going.

You know, it seems to me that there is a cycle of scientific discovery that then provides necessary impetus to develop technologies that address those known concerns and then we develop ones. We develop those initial technologies and prototype then we move toward bringing them to a place where they can demonstrate effectiveness and be deployed to the marketplace. I would like to further elaborate on that.

For all the witnesses. In terms of this cycle of discovery, prototype development, and then development toward deployment, as it relates to cybersecurity threats, where are we in that process for our energy infrastructure? And are there specific investments we should be making?

You mentioned informing municipalities and communities, but is there anything specific because it seems like this is a continual cycle that we go through. Anyone want to take that?

Mr. IMHOFF. Well, I'll get started and hand it over to my colleagues.

Senator DUCKWORTH. Yes.

Mr. IMHOFF. We're in all phases of that cycle.

Senator DUCKWORTH. Okay.

Mr. IMHOFF. There are many dimensions to this grid modernization activity. There are many dimensions to cybersecurity. On cybersecurity, I mentioned in my testimony, that there are, we have roughly 3,000 utilities in the United States. The largest 1,000 are pretty far along on their cybersecurity journey. The smallest 1,000 don't have any digital devices, so it's not much of an issue. The middle 1,000 have devices but they have very small engineering staffs and very limited budgets, and so it's harder for them just to do the basic fundamentals of maintaining good enterprise discipline on their infrastructures. So they are in a very different place on the development cycle than some of the larger utilities who are looking at quantum encryption and other activities.

We are in all phases, and I think it will always be that way. Some things are near the more mature state, but you're having to work them out into 3,000 utilities that are across 50 different regulatory jurisdictions. So it just doesn't happen overnight. It takes time for things to unfold.

Dr. RAINES. And the thing I'd like to add, Senator, with that, our partnerships are absolutely critical because the national labs will take and produce lower technology readiness level type of solutions. And so, to take and transition those to industry or work with the industry partners is absolutely critical in this arena.

I come from a military background as well from the standpoint of rapidly getting those products to the field where they're needed. And in cybersecurity, like I said earlier in the testimony, we are in that very tight loop of adversaries are far outpacing us in terms of how we can respond to them. So the industry partner is absolutely critical.

Mr. TUDOR. Senator, I'd like to respond to that as well.

I've been involved in, kind of, technology innovation for cybersecurity for about ten years in other jobs. One of the things that we do realize, you know, between the development and the deployment of technologies is what is called a valley of death. I think a lot of times the national labs, their place in developing those lower technology, readiness level technologies to solve particular problems at the time, have not had the emphasis on commercialization, probably not the lab's major role to do that. However, in the last few years we have seen more and more emphasis from DOE, DHS, and others to bring these technologies to bear. But we do need commercial partners, whether it's venture capitals or others, to come and help invest in these.

I know the other DHS transition to practice program did a wonderful job of coming into the national labs, but Pacific Northwest National Lab, Oak Ridge and INL all have technologies that were transitioned in some of those. But we need more of those types of activities and we need more emphasis on it if we really feel that we can get those out there and then entrepreneurs like Dr. Earl and Mr. Riedel can then take those technologies forward.

Dr. EARL. Is it okay to add to that as well?

Senator DUCKWORTH. Madam Chair?

Dr. EARL. Alright.

So, in terms of development to deployment, shortening that time, I think, one of the biggest challenges is, as was mentioned earlier, we have over 3,000 utilities, some big, some small. And they're going up against very sophisticated adversaries. These nation-state hackers have much more sophisticated operations than utilities are used to. And so, we're asking big and small utilities to come up with solutions on very rapidly changing technology.

One of the things that the government can help to do, national labs can help to do, partnerships can help to do, is to identify a template solution, sort of, cookie cutter solution that at least could be a starting point for these utilities. And then ultimately they need assistance in implementing it and maintaining it. That right now doesn't really exist for those utilities.

Mr. RIEDEL. Senator Duckworth, thank you for the question of the panel.

I wouldn't be here today without the support of the DOE, the State of California and some of the funding, so I'm very appreciative of that. For me, I think the funding is critical. It's a holistic approach that we need to take. There's no one technology that's going to solve this problem.

I think we talked a lot about networks today, about the dark fiber and the quantum, but you know, we also still need automation to be able to respond to these things in a timely fashion and to support the growth of the devices we're getting.

And at the end of the day, we also need to trust people who are operating those devices so we need to move beyond current credential technology and look at new ways that we can actually assert that the people who are operating are who they say they are which helps, sort of, I think, bring everything around. So, for me, it's a holistic approach and we need to continue investing in all those areas.

Senator DUCKWORTH. Thank you.

Madam Chair, you have been very generous. Thank you.

The CHAIRMAN. Thank you each for your response on that.

Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you, Madam Chair.

Let me just follow up, and this question is for all of you.

Do you think the small and midsized utilities are more challenged to really find the programs to address the cyber threats than maybe some of the larger utilities?

Dr. RAINES. Senator, I would agree with that statement, mainly from a standpoint of the resources that these smaller utilities have available for this.

Senator CORTEZ MASTO. So the programs are there. It is just a matter of having the capital or the resources to access those programs or afford those programs. Is that right?

Dr. RAINES. I would have a tendency to agree with that, ma'am.

Mr. IMHOFF. I agree, but I must say that some of their representing organizations, like for the co-ops, the National Electric Cooperative Association and the American Public Power Association, they do have relationships with DOE and they help aggregate numbers of small utilities for them to be involved in demonstrations. But in general, smaller utilities have smaller engineering staffs, smaller resources, so it's more of an uphill walk for them than some of the larger entities.

Mr. TUDOR. I think it is worthwhile to note though, as we mentioned before, in things like the CES-21 project, some projects on the East Coast—RADICS, that the intent is to have the large utility partners who have those resources help to validate a lot of these approaches and then share that information into the rural cooperatives and other types of environments that don't have those resources. They won't need to spend the time to do that validation, but it will be able to be handed out to them.

Senator CORTEZ MASTO. And then, and you may have already addressed this, and I apologize I had another committee hearing, but I am also curious how the states play into this. I know in the State of Nevada Governor Sandoval has created a new Office of Cyber Defense (OCD) which will serve as the primary focal point for cyber threats and security for the State of Nevada. With the addition of

that cyber defense coordinator, the OCD will serve as the primary conduit with the Federal Government as well as the primary entity managing cyber threat issues across the State of Nevada.

Do you see that as a role most states should be involved with and coordinating with the federal level and then, particularly, the private sector to address the cyber threat?

Mr. TUDOR. Thank you for your question, Senator.

You mentioned the important word there and that's "coordination." I don't think that every state should invest their resources to go off on their own and potentially have redundant systems. But as we mentioned with California, their work on their regional, you know, things that happened in the Pacific Northwest. I know PNNL, INL, and others work together with regional entities. And I think that coordination with leadership from the government can help rapidly advance some of the technology areas.

Dr. EARL. I do think as well in utilities there's a follow the leader mentality. So if a set of utilities, larger utilities, in one state identifies a solution that works well and they can share that with their counterparts, other utilities will see that filter down.

And just to echo what was mentioned, California has the California CES-21 project which involves utilities across the state. They've really developed some innovative package solutions that are being adopted in California. If that is successful then hopefully that will spread to the rest of the country as well.

Senator CORTEZ MASTO. Great.

Mr. RIEDEL. May I follow on real quick?

Senator CORTEZ MASTO. Please.

Mr. RIEDEL. Senator Cortez Masto, thank you very much.

CES-21 has already made an effect and we are already starting to work with other organizations such as STIX so the research coming out of that is actually having real world effects, not only for the U.S. but also that's promulgating around the globe. And that's all based on the funding that's come in to actually make that happen. So if we can continue that, that's only going to grow and I think that's a very good thing.

Senator CORTEZ MASTO. Great. Thank you.

Dr. Raines, I am actually very intrigued with your Dark Net concept. Assuming adequate funding, how many years away are we from being able to implement a Dark Net solution for our nation's electrical grid?

Dr. RAINES. Senator, thank you for that question.

As we had mentioned earlier in the testimony, there are different phases that are occurring and can occur with the Dark Net concept. Utilizing existing infrastructure, you know, such as some of the fiber. There are capabilities that Dr. Earl and others have been developing that can be implemented relatively quickly. There are also other advanced communication capabilities that can be implemented for some of the smaller cooperatives, if you will.

So, there's a lot of things that can be done near-term, but I think, as Dr. Earl mentioned earlier in testimony, some of these advances may take five to ten years to fully mature.

Senator CORTEZ MASTO. Okay. Thank you.

Gentlemen, thank you very much. I appreciate the conversation.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator.

I have just one last question.

Mr. Tudor, you had mentioned in your comments the need for control room operators to have hands on training opportunities and you referenced Ukraine in a box. How ready are we with this program? Do we actually have utility room operators that are training, kind of, hands-on to handle a Ukraine-like attack? And really, to what extent are the men and women that are on the ground or on the front lines being trained to handle a cyberattack?

Mr. TUDOR. Thank you for that question, Madam Chairman.

I must say that the people who operate our grid are highly capable and highly trained. It's really enlightening when you go into some of the command centers in some of the different utilities to talk about how they train, what they do, how they respond to events, what they do in their off time to provide this different training, the amount of training that's required.

Our Ukraine in a box is another tool in their training environments since, for the most part, our utility operators are not constantly responding to cyberattacks, being able to add this into their training regimen will be something that will allow them to see, kind of, real world techniques that may be deployed against them, some of the indicators, and how they might respond in a non-disruptive kind of desktop environment.

So, I do think that, from an operational perspective, we are in very good shape here in the U.S.

The CHAIRMAN. One of the things that I think about coming from a state that is rural and isolated and has more microgrids than large, integrated grids, is that you have different levels of opportunity for that kind of training that you are saying you think is pretty much in place.

I am thinking that perhaps with our bigger utilities they do have that opportunity, but our smaller grids that are perhaps not as integrated, as sophisticated, I worry about that level of vulnerability and I worry that perhaps we don't have a level of training that is applicable for the different types of grid that we have throughout the country. Can you put my mind at ease a little bit there?

Mr. TUDOR. Thank you, Madam Chairman, I'll try.

I think that you're right, there are different levels of need and different levels of training. I think the development of some of these desktop trainings, you know, INL and the other labs are known for their very large infrastructure, being able to bring people in and give some very unique sophisticated training, but also to be able to put some of this training via web-based which is happening now. These desktop type of environments, we are hoping to potentially make this an open source type of learning environment as well so they don't have to have our equipment to be able to run this type of training. So we are trying to export the training for more accessibility all across the nation.

Mr. IMHOFF. Madam Chairman?

The CHAIRMAN. Mr. Imhoff, go ahead.

Dr. RAINES. Oh, I'm sorry.

The CHAIRMAN. Mr. Imhoff and then Dr. Raines.

Mr. IMHOFF. So I was just talking the other day with the head of the Northwest Public Power Association and they're based in

Vancouver, outside of Portland. I believe that a number of the smaller utilities in Alaska are small, public and rural co-ops, et cetera. And they have training opportunities that they provide for their members, but they are voluntary. So it's not just Alaska. A lot of states, a lot of small utilities struggle to send their staff to training.

I think that there are opportunities there, processes, to work with the associations that they belong to, et cetera, but my guess is if you're to talk to those community entities, a large fraction of it has to do with the resources available to send people to train. And that would be where I would start, trying to get a sense for what resources do they need to participate in the already existing training opportunities that probably would require some travel down to the lower 48.

The CHAIRMAN. Because I do hear from so many of them that they are anxious for their own security and knowing that there are avenues via the web.

Dr. Raines, did you want to weigh in here?

Dr. RAINES. Yes, Madam Chairman.

What I wanted to say was basically there are some good news stories in terms of how we're developing workforce. For close to 20 years DHS, NSA, and National Science Foundation have been partners in these academic centers of excellence for focusing toward cybersecurity. There are over 200 universities and schools at this time producing cyber-educated folks. And that's not just at the graduate level or the undergraduate level, but at the community college level. So we're trying to hit or have been trying to hit for a number of years, you know, getting the workforce developed for the right application areas because a lot of the smaller utilities may be using more technician level folks than advanced degree folks to help operate. So there is a lot of work that's been going into that over the years. I just wanted to give that to you, ma'am, as a good news piece in developing workforce.

The CHAIRMAN. I appreciate that. I appreciate that, thank you.

Senator King, we have had good discussion here this morning with some of the technologies and the efforts through our national labs and out in the private sector as to what we can do to do a better job of ensuring that we are not as vulnerable with our, whether it is our energy grids or other infrastructure and had some good testimony.

We have gone through all the questions, so you are up if you would like to engage our witnesses.

Senator KING. Thank you, Madam Chair.

I want to apologize to you and the witnesses. Speaking of technology, there is no effort made whatsoever around here to schedule hearings in any kind of coordinated way. I had a hearing this morning on the attack in Niger which, obviously, is of great, grave concern.

I understand there has been some discussion of the bill that Senator Risch and I have sponsored involving the national labs and I won't belabor that except to say I think it is a step in the right direction and I understand the panel agrees. We will hopefully move that forward.

This isn't really a comment directed at the panel, but I think it is important, Madam Chair, as we are dealing with this issue and we spent quite a bit of time on it in the Armed Services and Intelligence Committees as well.

One of the problems is that all of our focus is defensive. How do we structure our system defensively? How do we patch? How do we have the right breakers and all those kinds of things?

In my view, though, ultimately that is not the whole answer. Part of the answer has to be a deterrent strategy or doctrine that is well known across the world that if people attack us in cyberspace they will feel results. They will also be at some risk.

One of the problems and one of the frustrations is that we don't have such a doctrine. And this isn't a criticism of the current Administration. The prior Administration did not do this either.

But I think, Madam Chair, if we are going to effectively deal with the risk of cyberattack, there has to be a deterrent doctrine whereby our adversaries know this kind of attack will not be accepted, will be responded to in some way. So I think that is a big part of the problem here. We can be the best bobbers and weavers in the history of the world, but if you are not allowed to ever punch back, you are going to lose the fight.

I think that is something very important that we are talking about in Armed Services and we passed amendments to the National Defense bill, but we are waiting for the Administration and we were waiting for the prior Administration to come forth with a cyber strategy beyond simply patching a system.

With that, if you can find a question in there you are welcome to it.

[Laughter.]

But I just felt that was an important part of this discussion. It is not only the technology of strengthening the grid, but it is also strengthening the deterrent so that the attack doesn't come in the first place.

Dr. EARL. If you don't mind, I'd like to address that.

So we talked a little today about quantum technology, quantum key distribution technology, which can defend the grid. The great thing about that technology or the flip side of that technology is it also can be used on the offense. Quantum computing can be used to crack codes and really take a much more aggressive stance on the offense side. So by investing in our own defense, we actually do provide a path to an offensive strategy as well if we needed it.

Senator KING. And one of the problems I have observed is we are so secretive about what we develop. A secret deterrent is not a deterrent. The world has to know what we can do. That was the rule with nuclear weapons for 70 years and blessedly it has protected us from that kind of catastrophe because of the understanding that, if nuclear weapons are used, there is mutually assured destruction.

So I agree with you, but we also, we all tend to, particularly in the government, want to keep things secret.

You all remember, I don't know, you may not, some of you are too young, this famous scene in Dr. Strangelove where George C. Scott says, "But Commissar, if you didn't tell us about the doomsday machine, it wouldn't work. Well, we were going to announce

it on May Day." We have got to have a deterrent. It has to be well known. It has to be clearly part of our doctrine.

Thank you.

Thank you, Madam Chair.

The CHAIRMAN. Well and to follow on that we had a little bit of discussion about where the Chinese are with their quantum technology and the distances that they have bridged. That is no secret. But I am sure that everyone in the world is, kind of, paying attention to what is going on there. So I hear your comment.

One further question on that. I raised China in my opening. You spoke to it. What other nations are out there that are leading in this space?

Dr. EARL. So, unfortunately, there's a number of countries that are leading the U.S. China, definitely, would be at the top of the list. But the EU is making a concerted effort. They're spending quite a bit of money to pursue quantum technology. Australia and Canada as well are very aggressive in this area. So, we're probably fourth or fifth on that list.

The CHAIRMAN. Interesting.

Any further questions from either of the Senators?

Thank you, gentlemen. We appreciate the time that you have given us and the level of expertise that you bring to this subject.

Know that as it relates to Puerto Rico, as we mentioned earlier, we will look forward to the input from our national labs there. But obviously we have a great deal of work to do going forward as we work to make things more secure.

Senator KING. Madam Chair?

The CHAIRMAN. Senator King.

Senator KING. I apologize. You mentioning Puerto Rico did provoke one thought.

I hope, as we are working on the rebuilding of the Puerto Rican grid, we can be thinking to the future instead of building a 20th century grid and think about things like distributed energy and underground wires and all of those kinds of things so that we don't just rebuild——

The CHAIRMAN. Yes.

Senator KING. ——something that is liable to be knocked down again in the next great storm. I think this is an opportunity that we should seize, and I hope we can all work together to see that that happens.

Thanks again.

The CHAIRMAN. Know that we concur up here.

Thank you, all.

With that, we stand adjourned.

[Whereupon, at 11:38 a.m. the hearing was adjourned.]

APPENDIX MATERIAL SUBMITTED

U.S. Senate Committee on Energy and Natural Resources
October 26, 2017 Hearing
Advanced Cyber Technologies that could be used to Help Protect Electric Grids and Other Energy Infrastructure from Cyberattacks
Questions for the Record Submitted to Mr. Carl Imhoff

Question from Senator Debbie Stabenow

Question: In your written testimony, you underscore the importance of continued DOE investment in fundamental sciences, applied technologies, and public-private partnerships to secure our electric grid and critical energy infrastructure. However, the Administration's budget proposal for Fiscal Year 2018 cuts nearly $900 million from the DOE's Office of Science, which supports 10 national labs and scientific research at more than 300 universities and institutions of higher learning across the country.

This administration's posture towards critical research and development is particularly upsetting upon hearing China has already developed and installed the foundations of their own nationwide quantum network; and has committed $10 billion to the creation of a new quantum laboratory.

While the Administration has sought increases in certain cybersecurity programs, what impact would the proposed cuts to the Office of Science have on our national labs' work to protect our nation's energy systems from cyberattacks?

Answer: Science and technology work is an important component underpinning cybersecurity programs—from high performance computing to advances in machine learning, the analytics we are using today count on advancements in these areas. The Department of Energy's cyber research program, housed in the Department's Office of Electricity Delivery and Energy Reliability (OE) is robust and includes both cyber protection and improved emergency response. In September, OE awarded new projects led by national laboratories that advances the OE Cybersecurity for Energy Delivery Systems (CEDS) Roadmap.

Question from Senator Steve Daines

Question: In your opening testimony, you discussed PNNL's role in fostering successful public-private partnerships in Washington State that have improved shared situational awareness and network resiliency. I also understand the Washington State National Guard has had a significant role in providing defensive capability to mitigate vulnerabilities in critical infrastructure. What successes have you observed between these public-private partnerships involving the National Guard, and where do you see opportunity for growth?

What successes have you observed between these public-private partnerships involving the National Guard?

Where do you see opportunity for growth?

U.S. Senate Committee on Energy and Natural Resources
October 26, 2017 Hearing
Advanced Cyber Technologies that could be used to Help Protect Electric Grids and Other Energy Infrastructure from Cyberattacks
Questions for the Record Submitted to Mr. Carl Imhoff

Answer: The Washington National Guard strategy calls for treating a cyber event as they do any other natural or manmade disaster. This strategy has resulted in the state's Guard units having emergency management processes and procedures for cyber events just as they do for other emergencies. As a result, the Washington National Guard has a Cyber Team of 500 citizen soldiers that are trained to provide cyber emergency support. Recent successes include the following:

- Snohomish County Public Utility District (PUD) teamed with the Washington State National Guard (NG) and the State of Washington to engage the NG Cyber Team in a historic collaboration to enable the NG Cyber team the opportunity to "penetration test" the PUD network. The NG was able to exercise its Cyber Team and the PUD was able to test its detection, response, and recovery plans and capabilities.

- The NG works with critical infrastructure providers (water supply, transportation, fuel supply etc.) on cyber issues since many times these providers don't know who to call for support or training.

Regarding emerging opportunities for additional public-private collaborations, I offer the following:

- Exercising cyber response training events with more critical infrastructure providers to ensure plans and procedures are aligned.

- Developing small (e.g. 10 person) cyber civil support teams in each state to build partnerships and relationships to ensure strong connections between Guard resources and the state groups needing their support.

- Consider how private sector assets in vulnerability assessments and emergency response can better support NG-DOD in times of crisis, to include cyber, should the NG-DOD not be able to perform their mission critical functions.

Questions from Senator Mazie K. Hirono

Question 1: In your testimony, you mention how PNNL and DOE have developed and deployed the Cyber Risk Information Sharing Program – or CRISP – as a way of monitoring and managing the security and resiliency of the electric grid. CRISP is a voluntary situational awareness program that identifies cyber threats to utilities and shares that information with utilities.

U.S. Senate Committee on Energy and Natural Resources
October 26, 2017 Hearing
Advanced Cyber Technologies that could be used to Help Protect Electric Grids and Other Energy Infrastructure from Cyberattacks
Questions for the Record Submitted to Mr. Carl Imhoff

Since CRISP is a voluntary program, I am interested in hearing how forthcoming you believe utilities have been in sharing sensitive information related to the cyber risks they are confronting on a daily and weekly basis. I would imagine a utility may not be inclined to voluntarily report a cyber-incident that may have exposed a weakness in their cybersecurity posture and if they are not required to do so. In your view, is there a way to induce and encourage greater participation in programs like CRISP?

Answer: The CRISP program model relies on utilities choosing to join the effort and sharing data and insights with the collective analytic effort and CRISP member utilities. Because the analytic results remove the identity of specific utilities before release to the full CRISP membership, we have witnessed strong willingness by member utilities to make data available and to actively engage in the analysis and development of collective response strategies.

While the CRISP program covers approximately 75 percent of the nation's electricity generation, membership is comprised primarily of the largest utilities as the model is utility-funded. Medium and small-sized utilities are interested in participating, but cost and technical readiness are currently barriers to participation. We believe that the key to getting more medium and small utilities to join is to reduce the cost and simplify implementation of cyber tools and lessons learned. These small utilities have strong interest in participating yet they lack financial resources and technical staff that are trained in cyber readiness. The Department of Energy (DOE) is currently conducting pilot efforts with the American Public Power Association and National Rural Electric Cooperative Association to develop tools and fee structures better tuned to the needs of small and medium-sized utilities. Providing these resources and programmatic support to accelerate the tools and outreach to this underserved portion of utilities is likely to deliver substantial improvement in U.S. utility cyber readiness, and follows the original implementation of CRISP, which was initially developed with DOE support.

Question 2: PNNL has been at the forefront in researching and developing technologies to increase cyber situational awareness of grid control systems that are internal to utilities. In your view, is the Administration and Congress investing enough resources to keep up with the cyber threat? Also, in your view, are utilities investing enough resources to adequately address cyber threats that continue to evolve?

Answer: The utility industry and DOE have made significant progress in improving the cyber readiness of our nation's grid infrastructure with regard to the information technology (IT) side, and are generally staying in front of the threat profiles such as have been observed in other countries over the past two years. The NERC Critical Infrastructure Plan processes have marshalled significant industry response that addresses the bulk grid, which is the responsibility of NERC. There is more that needs to be done to extend the protection and situational awareness to include grid control systems (also known as industrial control systems, or operational technology) in addition to the current IT efforts. There is also a need to deliver more guidance to

industry on standards for acquisition of new grid products that ensure security of the supply chain of new products. To the second question, it is the small and medium utilities that struggle to provide sufficient financial and technical resources to meet the basic "best practices" for cyber readiness. DOE has pilot efforts underway to help industry groups like the American Public Power Association and the National Rural Electric Cooperative Association develop tools and approaches to help this class of utilities.

Question 3: As industrial control systems become more complex, they becoming more connected and potentially more vulnerable. On the other hand, however, technical advances could potentially make these systems easier to protect because they can incorporate the latest state of the art security technology such as advanced encryption algorithms and other measures.

Is progress being made to ensure these systems are more secure as the technology becomes better, or are we losing ground because these systems are becoming more complex and inherently more vulnerable to advanced persistent cyber threats?

Answer: Progress is being made and, in general, U.S. utilities are staying ahead of the threat profiles such as was seen in Ukraine and elsewhere in the past several years. The challenge is to achieve enhanced situational awareness across the information technology (IT) side of the house (e.g. the CRISP program) and industrial control systems (OT) to give a full sense of cyber readiness. A number of projects across DOE's Office of Electricity Deliverability and Energy Reliability Cybersecurity for Energy Delivery Systems program research portfolio with national laboratories and industry are addressing this from both the IT and OT perspective. Advanced analytics such as machine learning will substantially enhance our readiness in this domain.

U.S. Senate Committee on Energy and Natural Resources
October 26, 2017 Hearing
Advanced Cyber Technologies that could be used to Help Protect Electric Grids and Other Energy Infrastructure from Cyberattacks
Question for the Record Submitted to Dr. Richard Raines

Question from Senator Debbie Stabenow

Question: Distributed energy systems can offer efficiency, flexibility, and reliability. However, in terms of cybersecurity, what are the benefits and risks to having a distributed energy network, and what does an increasingly decentralized network mean for the government and industry's role in combatting cyber threats?

Answer: Historically, the U.S. power grid was controlled manually, and protection measures were based on physics. With the introduction of microprocessor-based control systems, a majority of the energy enterprise is computer-controlled and automated. Even though this automation is much more efficient, opportunities for malicious actors to cause serious harm have never been greater. Malicious attacks could stem from supply chain interdiction or a cyber attacker sending unauthorized commands that result in loss of power or even destruction of expensive hardware.

Distributed energy networks, also referred to as microgrids, offer efficiencies and resilience over traditional energy systems by allowing electricity to be generated closer to where it will be used. These systems also offer the potential to integrate disparate sources such as wind, solar, and battery technologies, and thereby increase the reliability of the distributed system over the traditional energy grid. These microgrids can benefit local utilities by providing on-demand generation and grid load balancing. These efficiencies make microgrids an attractive technology for deployment. However, both traditional energy systems and distributed energy networks are vulnerable to cyber intrusion and require that security be designed and built into the system.

To consider the cybersecurity benefits and risks of distributed energy architectures, one must understand the proposed distributed architecture. The microgrid architecture can exist as a set of locally controlled enclaves, segmented from each other and from the backbone grid while also possessing cybersecurity controls and processes. Each microgrid will have very well-defined logical and physical network boundaries with the operations (control and communications) occurring within the trusted environment. This isolation and locality-of-control of the enclaves serve to reduce the risk to cyber threat. Resiliency for the microgrid is increased due to the local span of control and the various technology switch-over generation options (hydro, solar, wind).

While no architecture will eliminate all cyber risks, the proposed microgrids, if properly configured and maintained/managed, can yield protections far stronger than present day architectures. The risks associated with distributed architectures mainly deal with the increased number of microgrids—which could present an increased number of targets for an adversary—and how well the local owning entity protects and manages the microgrid (e.g., are strong security measures in place and updated on a regular basis by highly qualified security professionals and operators). The distributed nature of the energy network will require that increased and enhanced cyber situational awareness resources and mechanisms, such as anticipatory threat discovery, monitoring, mitigation, reporting and recovery, be in place and

U.S. Senate Committee on Energy and Natural Resources
October 26, 2017 Hearing
Advanced Cyber Technologies that could be used to Help Protect Electric Grids and Other Energy Infrastructure from Cyberattacks
Question for the Record Submitted to Dr. Richard Raines

dynamic enough to handle changes within the microgrids. If properly performed, the cybersecurity and operational benefits associated with microgrids outweigh risks associated with maintaining present-day architectures.

With regards to the last portion of the question, with decentralized systems, government and industry roles could and should be to:

- Continue to support the development and deployment of cutting-edge technologies, through programs such as DOE's Cybersecurity for Energy Delivery Systems, which mitigate risks and thwart adversarial activities;
- Nationally lead and support the development of the technical workforce that will be operating these systems through existing programs such as the National Center of Academic Excellence (NSA and DHS partnership) in Information Assurance and Cyber Operations programs and the Scholarship for Service CyberCorp (NSF led);
- Encourage critical infrastructure sectors to embrace and implement national standards such as NIST SP 800-39 and SP 800-37 to guide risk management of information systems security; and
- Ensure that coordinating and reporting structures, as well as information-sharing organizations (such as the Electricity Information Sharing Analysis Center, or E-ISAC) are sufficiently equipped to rapidly identify and disseminate information regarding emerging threats and mitigation processes.

U.S. Senate Committee on Energy and Natural Resources
October 26, 2017 Hearing
Advanced Cyber Technologies that could be used to Help Protect Electric Grids and Other Energy Infrastructure from Cyberattacks
Questions for the Record Submitted to Mr. Zachary Tudor

Questions from Senator Debbie Stabenow

Questions: Thank you for stressing the importance of building a nationwide, multidisciplinary cybersecurity workforce. If we want to fully secure our electric grid and preserve our international standing in the cybersecurity space, it is critical that we not only sustain our current workforce, but inspire the next generation of researchers and experts as well.

Presently, what are the challenges to hiring and retaining experts in cybersecurity? How could universities better fill the cybersecurity skills gap for energy infrastructure?

Response:
Attracting, hiring and retaining the highly qualified cybersecurity experts the nation needs to address grid and energy infrastructure challenges is a daunting task. INL's insight, gained from the many requests for expertise from U.S. government and private sector, leads INL to estimate that the available specialized expertise may possibly be less than 10 percent of what the nation needs. This gap is in the specialized expertise that can address industrial control systems (ICS) cybersecurity threats across the range of needs for high-quality and immediate incident response, innovative research and development, actionable threat analyses, relevant training, and advanced technology education. As a result of this gap, energy owners/operators, manufacturers, national laboratories, and government agencies are vying for the same talent. Shrinking this critical skills gap requires a multipronged approach that addresses: 1) retention of current experts through competitive compensation improvement initiatives, skills bonuses, etc. 2) engaging the creative interests of this unique talent pool by providing access to a variety of complex technical challenges, work environments, and unique experimental tools 3) retooling and/or reshaping cybersecurity training programs to include operational technology (i.e., ICS, control systems) 4) revamping traditional university computer science and computer engineering programs to add the critical hands-on cybersecurity skills essential to the protection of critical infrastructure, such as reverse engineering and deep understanding of control systems 5) creating K-12 interest and excitement through Science, Technology, Engineering, and Math programs. Additional information is provided below for each of the five topics.

Retention of Current Experts: INL made significant progress in attracting and retaining expertise by adjusting compensation ranges and instantiating a critical skills-based bonus program. Due to the evolution of this career field, INL redefined position descriptions and performance criteria to align with the highly specialized skills and experiences needed to defeat very sophisticated threats, rather than aligning positions and compensation with the traditional laboratory approach of education degrees, years of experience, and scholarly publication record. This approach enabled INL to define positions and provide compensation ranges more aligned with the private sector market environment of performance and impact. Also, INL is enabling more flexibility in work assignments through joint appointments with universities, alternative work locations, and nonstandard work hours.

U.S. Senate Committee on Energy and Natural Resources
October 26, 2017 Hearing
Advanced Cyber Technologies that could be used to Help Protect Electric Grids and Other Energy Infrastructure from Cyberattacks
Questions for the Record Submitted to Mr. Zachary Tudor

Access to Technical Challenges: Beyond compensation and the work environment, INL is making more progress in attracting, retaining and building talent by providing a wide breadth of technical challenges – technical challenges that represent exciting opportunities to have a notable impact on national security while inspiring researchers to build skills that far surpass the skills of adversaries. Hence, a key objective of INL's Cybercore Integration Center strategy is to create a technically challenging training, education, and work environment that offers cyber defenders and researchers assignments that advance their skills from novice, apprentice, journeyman, and master. To do this, Cybercore will develop and pilot pathways for individuals to rotate among laboratories, universities, industry, and government to take on technical challenges that span scientific discovery, engineering design, infrastructure operations, incident response, entrepreneurial invention, teaching, and leadership. The principles of Cybercore will enable personnel to rapidly transition among partnering institutions so that their talents are available when needed for national priorities, while their primary focus aligns with their career interests within their most preferred environment. As an example, university faculty will have opportunities to serve in joint appointment roles with INL. This provides the faculty assignee with unfettered access to the laboratory's unique experimentation capabilities and will provide immediate access to threat information that requires security clearances. Other types of appointments with universities are under evaluation for developing and sharing skills among interns, graduate fellows, and postdocs to accelerate the development of a workforce pipeline.

Cybersecurity Training Programs: INL's written testimony provided several examples in which our expertise and capabilities are developing the skills of our national workforce. Beyond these, INL is assessing frameworks for education centers or cyber academies that focus on improving knowledge transfer of lessons learned from cybersecurity incident responses, enhancing training and learning effectiveness when using new advanced technologies, and implementing a cyber-informed engineering culture throughout all levels of any organization. Just as a ubiquitous and effective safety culture reaps benefits across an organization, INL advocates that a cyber-informed culture across an organization will result in a significant reduction in the day-to-day cyber hygiene and nuisance incident response burdens, enabling an organization's cybersecurity elites to focus on more consequential cyber risk reduction priorities.

University Science and Engineering Programs: INL's expertise and capabilities are influencing curricula and skills development within our nation's universities. We are enthused that our Cybercore strategy for partnering with universities in workforce development is consistent with many of the findings and recommendations within an upcoming National Academies of Sciences report, "Assessing and Responding to the Growth of Computer Science Undergraduate Enrollments." With foresight into the evolution of workforce gaps, Cybercore already has developed collaborative research projects and student development commitments with the three Idaho research universities and a few other prominent cybersecurity university programs for interns, graduate fellowships, postdoctoral researchers, and joint appointments. We are sharing our strategy and lessons learned with other laboratories. We are actively seeking additional university partnerships -- especially when the curriculum and research programs emphasize

cyber-informed learning and experimentation with operational technologies (e.g., industrial control systems, embedded control systems, supervisory control and data acquisition systems, etc.). Beyond a primary emphasis on cyber-informed learning with operational technologies, INL also advocates that university computer science and engineering curricula provide opportunities for students to participate in immersive cybersecurity problem-solving exercises and experiments that bring together multidisciplinary skills from information technologies, engineering design, decision science, systems engineering, and automation.

STEM: While INL is investing in building capabilities, partnerships, and programs among the current workforce and with higher education institutions, we also recognize the national value in raising interest and building foundational science and engineering skills throughout the early stages of the education cycle, K-12 students and teachers. Our leaders, researchers, and university partners are actively engaged in and promote new and innovative concepts for advancing Science, Technology, Engineering, and Math (STEM) outreach education programs. Recent cybersecurity activities included completing the inaugural Cybercore STEM Summer Camp -- a three-day event providing high school students with hands-on experience using various ethical hacking techniques and methods. During a recent statewide teacher in-service, INL researchers provided hands-on learning with the Grid Game, a joint INL and Idaho university developed simulation learning tool for understanding the dynamics of power systems, grid control systems, and cybersecurity. This event also included teachers with an introduction to the education opportunities available through Cybercore Summer Camps and an INL staff-sponsored "Girls Who Code" chapter.

U.S. Senate Committee on Energy and Natural Resources
October 26, 2017 Hearing
Advanced Cyber Technologies that could be used to Help Protect Electric Grids and Other Energy Infrastructure from Cyberattacks
Questions for the Record Submitted to Dr. Duncan Earl

Question from Senator Debbie Stabenow

Question: As you may know, the Congress is working on legislation to help advance the development of autonomous vehicles, which have the potential to improve mobility and reduce traffic fatalities and injuries. However, the safety of these vehicles depends on secure communication technologies. Can quantum technology also be applied to help secure communication channels between autonomous vehicles?

Answer:
Yes. The application of quantum technology for protecting vehicle-to-vehicle communications and for authenticating vehicle software/firmware updates is something Qubitekk is already investigating with industry and national laboratory partners. Quantum technology delivers trusted communication channels and can guarantee the integrity of data. For autonomous vehicles making life and death decisions based on received data, trust and data integrity are essential.

There remains, however, technical challenges to applying this technology to autonomous vehicles. These technical challenges mainly revolve around limited road-side resources for supporting quantum optical channels. Similar to how cellular towers allow users to make phone calls while driving, a quantum road-side network is needed as a communication platform for securing vehicle-to-vehicle communications. Efforts to build a "smart" highway are already being proposed and investigated by both federal agencies and private industry. As these solutions emerge, the path for incorporating quantum technology should become more evident.

Questions from Senator Mazie K. Hirono

Question 1: Earlier this year, the President submitted a budget to Congress that would cut $2 billion, or nearly 53 percent, from four major DOE programs including the Office of Electricity Delivery and Energy Reliability which manages the Cybersecurity for Energy Delivery Systems (CEDS) R&D program. You've testified to how your company is putting DOE/CEDS research funding to good use by conducting tests of quantum technology with utilities in California and Tennessee.

Dr. Earl, where in the testing process of quantum technology would Qubitekk be right now without any R&D funding from DOE?

Answer 1:
Without past funding from the DOE CEDS R&D program, my company, Qubitekk, and our quantum technology product for protecting grid communications would likely not exist. Although significant private sector money has also been invested to realize Qubitekk's quantum key distribution technology, the CEDS program has shared the risk in bringing this new

technology to market. Most importantly, Qubitekk's relationship with critical partners (such as major utilities, leading equipment vendors, and national laboratories) would have been difficult to establish without the R&D and demonstration efforts funded by the CEDS program.

Rather than cutting the DOE CEDS program, we would argue that funding to this program office should be increased by $10M as soon as possible to begin developing Darknet. Darknet is a fiber optic based network that would interconnect electrical utilities and be protected by quantum technology. The majority of funding for implementing a nationwide Darknet would ultimately come from utilities, but its early development will require federal funds and coordination which the DOE CEDS program is already positioned to administer.

Question 2: Do you believe the private sector would prioritize and fund this type of cutting edge research on its own?

Answer 2:
The electric utility industry is not known for its rapid adoption of new technology. Consequently, it is challenging to convince private sector investors to pursue a long-term investment in a cutting-edge technology that targets this slow-moving industry. Federal funding for technology development and early pilot testing have been critical and will still be needed to bring quantum technology to market.

Question 3: What are the consequences for the United States if China outpaces the U.S. in developing and installing the next generation of cybersecurity technologies for the electric grid and other critical energy infrastructure?

Answer 3:
China currently has the capabilities to conduct a successful cyber campaign against our critical infrastructure systems. Their greatest deterrent, however, is that the U.S. has similar capabilities and would likely respond with a proportional cyber response. If China implements a quantum network for protecting their critical infrastructure, and the U.S. does not, the balance will be shifted in their favor. The implication would be an emboldened China less restrained in its cyber surveillance and manipulation of our critical systems. Operating with impunity, low-profile cyberattacks aimed at manipulating financial markets, energy prices, and defense capabilities would likely occur in the near-term. More aggressive actions, such as power disruptions, could be expected in a war-time environment or as a proportional response to opposed U.S. foreign policy.

Comments for the Record Submitted by
Amit Yoran, Chairman and CEO, Tenable, Inc., and
Leo Simonovich, VP and Global Head, Industrial Cyber and Digital Security, Siemens Energy
U.S. Senate Committee on Energy and Natural Resources
Regarding Cyber Technology and Energy Infrastructure
November 9, 2017

The Growing Threat to Critical Infrastructure

At a time when the risk of cyberattacks against critical infrastructure has grown exponentially, we applaud the Committee's efforts to better understand all aspects of this issue.

The stakes have never been higher when it comes to cybersecurity for critical infrastructure. The number of cyberattacks worldwide continues to grow, with operational technology (OT) becoming a growing target. According to a recent study conducted by the Ponemon Institute on the state of cybersecurity in the oil and gas industry, OT cyberattacks now comprise 30 percent of all attacks, with a major impact on productivity, uptime, efficiency and safety, according to recent research. The study also found that 68% of respondents reported at least one security compromise in the past year. Additionally, 59% believe there is a greater risk in the OT environment than the IT environment. With the rise of cloud, mobile and IoT and now the convergence of IT with OT, critical systems are increasingly vulnerable to aggressive adversaries and attacks.

In fact, the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) recently detected a coordinated effort by malicious actors to compromise the country's critical infrastructure. These infrastructures include those involved in government, aviation, power production, energy production, and some critical manufacturing sectors. Typically, part of these infrastructures include Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems that control the physical processes. These attacks are ongoing. The "ownership" of any one of these critical infrastructures by a malicious actor would cause significant economic and social distress to the United States.

Understanding Recent Attacks

It is important to note that attackers targeting critical infrastructure are carefully choosing high-value targets, rather than randomly looking for targets of opportunity. They are conducting "open source" research on the targets by studying publicly available information, which reveals business partners, data on employees, data on infrastructure and related information. All of this data is useful for identifying targets and designing attacks.

The most recent attacks follow a pattern of first compromising weakly defended networks, typically operated by suppliers or contractors, that are connected to more strongly defended critical infrastructure targets. Once compromised, the partner/contractor network is used as a bridge to attack the critical infrastructure network. This effectively takes advantage of the trust relationship that exists between the subcontractors/partners and the primary objective of the attack, the critical infrastructure network. The attackers are also manipulating "watering hole" domains - for example, trade and informational websites that relate to Industrial Control, Process Control and Critical Infrastructure.

Targeted, critical infrastructure-specific spear-phishing attacks are used to collect user credentials by sending email attachments that leverage authenticating Microsoft Office functions to retrieve files from Server Message Block (SMB) servers under the control of the attackers. The SMB server may be owned by the malicious actors or may be a compromised machine owned by the victim. This allows the attackers to capture the authentication sequence that takes place between the client and server, allowing credentials to be harvested. A similar SMB credential-stealing technique is also used by the compromised watering hole domains.

Using the stolen credentials, the attackers access the victim network and download tools to establish presence, persistence and control; create user accounts; attempt to escalate the privilege of these user accounts; disable any host firewalls; establish Remote Desktop Protocol access; and install VPN clients.

While no actual ICS/SCADA network has been maliciously manipulated at this point, attackers have viewed files related to wiring diagrams, SCADA panel layouts and so-on. It appears they are analyzing the environment and have established a foothold within the target environments that may be leveraged for something far more sinister in the future.

The current attacks are in many ways similar to those conducted in recent years against power grids outside of the United States. Open source research, credential harvesting, studying the internal infrastructure, establishing persistent presence and the installation of tools on the victim network are typically performed many months before the actual attack against the ICS infrastructure. This appears to be exactly what the malicious actors are doing against United States targets. This is exactly why early detection is so important, and why these attacks are being taken so seriously.

The Need for Passive Scanning

Unfortunately, the deployment of cybersecurity measures isn't keeping pace with the growth of digitalization in operations such as in the oil and gas industries, and the inability to accurately understand and represent cyber risk at any given time creates a gap in organizations' understanding of their overall cyber exposure.

For operators of critical infrastructure, both the traditional IT environment and the ICS environment must be continuously monitored not only for indicators of compromise but also for proper configuration, the presence of vulnerabilities, and changes of state to the endpoints. These steps are critical to detecting and addressing vulnerabilities before they can be exploited and lead to disruption of essential public services like electricity, gas, and water.

A process known as passive scanning is a particularly effective tool for use with sensitive systems such as those inherent in operational technology. This approach provides a safe and non-intrusive way to discover and monitor systems. Passive scanning provides deep packet inspection to continuously discover and track users, applications, cloud infrastructure, trust relationships and vulnerabilities.

Technology Recommendations

Technology solutions designed to address OT security should at a minimum be able to do the following:

- Discover all assets at all times to understand and reduce risk due to "unknown unknowns"
- Continuously monitor devices for vulnerabilities
- Constantly search for the presence of unknown software or active unknown processes on endpoints
- Continuously monitor critical infrastructure devices for proper secure configuration and detect systems where the configuration has mysteriously changed

- Monitor for changes in critical directories or executable files to detect malicious modifications
- Monitor for new user accounts on endpoints which may have been created by malicious actors
- Continuously monitor the ICS environment for vulnerabilities and unusual traffic patterns
- Detect, monitor and understand in detail the connections that exist between the IT network and the ICS network
- Detect, monitor and understand in detail the connections that exist between "trusted" third parties and the IT network
- Detect, monitor and understand any outside connections that may exist directly to the ICS network

In addition, organizations running operational technology should ensure that "trusted" third parties comply with minimum security standards and should also consider universal adoption of two factor authentication.

New Private Sector Efforts to Address Threat
Tenable, Inc. and Siemens, a global engineering and technology leader, this week announced a strategic partnership to help energy, utilities and oil and gas companies close the industry readiness gap with a new solution for industrial asset discovery and vulnerability management. These global leaders in cybersecurity and OT have teamed up to launch 'Industrial Security' from Tenable, which Siemens is delivering as a service to help operators secure and protect their critical OT assets.

The Tenable-Siemens partnership can help organizations address the challenge of not knowing where they are at greatest risk. By leveraging the capabilities of both companies, customers will gain a better understanding of where their OT assets may be vulnerable. The combination of Tenable's technology--the first OT-dedicated passive vulnerability detection solution that gives customers continuous visibility into their greatest risks--combined with Siemens' domain expertise and operational knowhow, is a powerful solution that can help customers close this knowledge gap so they can protect their critical assets.

Through the partnership, companies in the critical infrastructure sector will be able to understand the state of their assets at all times, providing them with the information they need to quickly and confidently assess, understand and ultimately reduce their cybersecurity risk.

Conclusion
Organizations running operational technology face a foundational security challenge – the need to understand the entirety of their cyber exposure in the context of a modern attack surface that is constantly evolving. In order to address this threat, organizations running operational technology need a way to monitor and address their attack surface in totality, through a full asset inventory and automated vulnerability management program, to protect those systems – and the people who depend on them – from threats.

Enclosure:
"The State of Cybersecurity in the Oil and Gas Industry: United States" Sponsored by Siemens and independently conducted by Ponemon Institute LLC. Study available here:
http://news.usa.siemens.biz/sites/siemensusa.newshq.businesswire.com/files/press_release/additional/Cyber_readiness_in_Oil__Gas_Final_4.pdf.

○