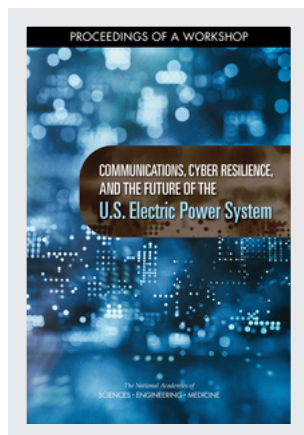


This PDF is available at <http://nap.edu/25782>

SHARE



Communications, Cyber Resilience, and the Future of the U.S. Electric Power System: Proceedings of a Workshop (2020)

DETAILS

74 pages | 6 x 9 | PAPERBACK

ISBN 978-0-309-67680-9 | DOI 10.17226/25782

CONTRIBUTORS

Anne Frances Johnson, Rapporteur; Committee on the Future of Electric Power in the U.S.; Board on Energy and Environmental Systems; Division on Engineering and Physical Sciences; National Academies of Sciences, Engineering, and Medicine

SUGGESTED CITATION

National Academies of Sciences, Engineering, and Medicine 2020. *Communications, Cyber Resilience, and the Future of the U.S. Electric Power System: Proceedings of a Workshop*. Washington, DC: The National Academies Press.
<https://doi.org/10.17226/25782>.

GET THIS BOOK

FIND RELATED TITLES

Visit the National Academies Press at NAP.edu and login or register to get:

- Access to free PDF downloads of thousands of scientific reports
- 10% off the price of print titles
- Email or social media notifications of new titles related to your interests
- Special offers and discounts



Distribution, posting, or copying of this PDF is strictly prohibited without written permission of the National Academies Press. (Request Permission) Unless otherwise indicated, all materials in this PDF are copyrighted by the National Academy of Sciences.

Copyright © National Academy of Sciences. All rights reserved.

COMMUNICATIONS, CYBER RESILIENCE, AND THE FUTURE OF THE U.S. Electric Power System

PROCEEDINGS OF A WORKSHOP

Anne Frances Johnson, Rapporteur

Committee on the Future of Electric Power in the U.S.

Board on Energy and Environmental Systems

Division on Engineering and Physical Sciences

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

THE NATIONAL ACADEMIES PRESS

Washington, DC

www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, NW Washington, DC 20001

This activity was supported by Contract/Grant No. DE-EP000006/89303018FOE400001 with the U.S. Department of Energy. Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of any organization or agency that provided support for the project.

International Standard Book Number-13: 978-0-309-67680-9

International Standard Book Number-10: 0-309-67680-0

Digital Object Identifier: <https://doi.org/10.17226/25782>

This publication is available in limited quantities from:

Board on Energy and Environmental Systems

500 Fifth Street, NW

Washington, DC 20001

bees@nas.edu

<http://www.sites.nationalacademies.org/DEPS/BEES>

Additional copies of this publication are available from the National Academies Press, 500 Fifth Street, NW, Keck 360, Washington, DC 20001; (800) 624-6242 or (202) 334-3313; <http://www.nap.edu>.

Copyright 2020 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America

Suggested citation: National Academies of Sciences, Engineering, and Medicine. 2020. *Communications, Cyber Resilience, and the Future of the U.S. Electric Power System: Proceedings of a Workshop*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/25782>.

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

The **National Academy of Sciences** was established in 1863 by an Act of Congress, signed by President Lincoln, as a private, nongovernmental institution to advise the nation on issues related to science and technology. Members are elected by their peers for outstanding contributions to research. Dr. Marcia McNutt is president.

The **National Academy of Engineering** was established in 1964 under the charter of the National Academy of Sciences to bring the practices of engineering to advising the nation. Members are elected by their peers for extraordinary contributions to engineering. Dr. John L. Anderson is president.

The **National Academy of Medicine** (formerly the Institute of Medicine) was established in 1970 under the charter of the National Academy of Sciences to advise the nation on medical and health issues. Members are elected by their peers for distinguished contributions to medicine and health. Dr. Victor J. Dzau is president.

The three Academies work together as the **National Academies of Sciences, Engineering, and Medicine** to provide independent, objective analysis and advice to the nation and conduct other activities to solve complex problems and inform public policy decisions. The National Academies also encourage education and research, recognize outstanding contributions to knowledge, and increase public understanding in matters of science, engineering, and medicine.

Learn more about the National Academies of Sciences, Engineering, and Medicine at **www.nationalacademies.org**.

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

Consensus Study Reports published by the National Academies of Sciences, Engineering, and Medicine document the evidence-based consensus on the study's statement of task by an authoring committee of experts. Reports typically include findings, conclusions, and recommendations based on information gathered by the committee and the committee's deliberations. Each report has been subjected to a rigorous and independent peer-review process and it represents the position of the National Academies on the statement of task.

Proceedings published by the National Academies of Sciences, Engineering, and Medicine chronicle the presentations and discussions at a workshop, symposium, or other event convened by the National Academies. The statements and opinions contained in proceedings are those of the participants and are not endorsed by other participants, the planning committee, or the National Academies.

For information about other products and activities of the National Academies, please visit www.nationalacademies.org/about/whatwedo.

COMMITTEE ON THE FUTURE OF ELECTRIC POWER IN THE U.S.

M. GRANGER MORGAN, NAS,¹ Carnegie Mellon University, *Chair*
ANURADHA M. ANNASWAMY, Massachusetts Institute of Technology
ANJAN BOSE, NAE,² Washington State University
TERRY BOSTON, NAE, Terry Boston, LLC
KAREN BUTLER-PURRY, Texas A&M University
JEFFERY DAGLE, Pacific Northwest National Laboratory
DEEPAKRAJ M. DIVAN, NAE, Georgia Institute of Technology
MICHAEL HOWARD, Electric Power Research Institute
CYNTHIA HSU, National Rural Electric Cooperative Association
REIKO KERR, Los Angeles Department of Water and Power
NANCY LANGE, MISO Board of Directors
KAREN L. PALMER, Resources for the Future
H. VINCENT POOR, NAE/NAS, Princeton University
WILLIAM H. SANDERS, Carnegie Mellon University
SUSAN F. TIERNEY, Analysis Group
DAVID G. VICTOR, University of California, San Diego
ELIZABETH J. WILSON, Dartmouth College

Staff

K. JOHN HOLMES, Director, Board on Energy and Environmental
Systems
ELIZABETH ZEITLER, Senior Program Officer
BRENT HEARD, Associate Program Officer
HEATHER LOZOWSKI, Financial Manager
MICHAELA KERXHALLI-KLEINFELD, Research Associate
REBECCA DEBOER, Research Assistant

¹ Member, National Academy of Sciences.

² Member, National Academy of Engineering.

BOARD ON ENERGY AND ENVIRONMENTAL SYSTEMS

JARED COHON, NAE,¹ Carnegie Mellon University, *Chair*
DAVID T. ALLEN, University of Texas, Austin
VICKY BAILEY, Anderson Stratton Enterprises, LLC
CARLA BAILO, Center for Automotive Research
W. TERRY BOSTON, NAE, Terry Boston, LLC
WILLIAM BRINKMAN, NAS,² Princeton University
DEEPAKRAJ M. DIVAN, NAE, Georgia Institute of Technology
MARCIUS EXTAVOUR, XPRIZE
T.J. GLAUTHIER, TJ Glauthier Associates, LLC
NAT GOLDHABER, Claremont Creek Ventures
KELLY SIMS GALLAGHER, Tufts University
BARBARA KATES-GARNICK, Tufts University
JOANN MILLIKEN, Independent Consultant
DOROTHY ROBYN, Boston University
ALEXANDER SLOCUM, NAE, Massachusetts Institute of Technology
JOHN WALL, NAE, Cummins, Inc.
ROBERT WEISENMILLER, California Energy Commission (Retired)

Staff

K. JOHN HOLMES, Director
JAMES ZUCCHETTO, Senior Scientist
ELIZABETH ZEITLER, Senior Program Officer
BRENT HEARD, Associate Program Officer
HEATHER LOZOWSKI, Financial Manager
MICHAELA KERXHALLI-KLEINFELD, Research Associate
REBECCA DEBOER, Research Assistant

¹ Member, National Academy of Engineering.

² Member, National Academy of Sciences.

Acknowledgment of Reviewers

This Proceedings of a Workshop was reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise. The purpose of this independent review is to provide candid and critical comments that will assist the National Academies of Sciences, Engineering, and Medicine in making each published proceedings as sound as possible and to ensure that it meets the institutional standards for quality, objectivity, evidence, and responsiveness to the charge. The review comments and draft manuscript remain confidential to protect the integrity of the process.

We thank the following individuals for their review of this proceedings:

David Batz, Edison Electric Institute,
Marc Child, Great River Energy, and
Paul Skare, Pacific Northwest Laboratory.

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the content of the proceedings nor did they see the final draft before its release. The review of this proceedings was overseen by John Manferdelli, Northeastern University. He was responsible for making certain that an independent examination of this proceedings was carried out in accordance with standards of the National Academies and that all review comments were carefully considered. Responsibility for the final content rests entirely with the rapporteur and the National Academies.

Contents

OVERVIEW	1
1 INTRODUCTION	9
2 UNDERSTANDING THE THREAT LANDSCAPE	11
Computing in the Grid, 11	
Cybersecurity Challenges, 13	
EMP and GMD Challenges, 18	
National Security Implications, 23	
3 STRATEGIES TO INCREASE RESILIENCE	29
Technological Capabilities, 29	
Culture Change, 35	
Translational R&D, 41	
APPENDIXES	
A Statement of Task	49
B Workshop Agenda	51
C Registered Workshop Participants	55
D Acronyms	63

Overview

Electric power is a critical infrastructure that is vital to the U.S. economy and national security. Today, the nation's electric power infrastructure is threatened by malicious attacks, accidents, and failures, as well as disruptive natural events. As the electric grid evolves and becomes increasingly interdependent with other critical infrastructures, the nation is challenged to defend against these threats and to advance grid capabilities with reliable defenses.

The Committee on the Future of Electric Power in the U.S. was convened by the National Academies of Sciences, Engineering, and Medicine to evaluate strategies for incorporating new technologies, planning and operating strategies, business models, and architectures in the U.S. electric power system. As part of its information gathering, the committee organized the workshop on Communications, Cyber Resilience, and the Future of the U.S. Electric Power System on November 1, 2019. The workshop was attended by representatives from industry, government, and academia and featured a keynote address, expert panels, and lively open discussions among workshop participants. The presentations and discussions at the workshop provided the committee with diverse perspectives on current and future threats to the electric power system, activities that the subsector is pursuing to defend itself, and how this work may evolve over the coming decades.

Specific focus areas for the presentations and discussions included the current state and security of the electric system and its relationship to national security, challenges posed by cybersecurity attacks and

electromagnetic pulse (EMP) and geomagnetic disturbance (GMD) events, opportunities for developing and implementing technological solutions to improve grid resiliency, and the cultural and policy context of cybersecurity. While the list of topics discussed was not exhaustive, the workshop was organized with the goals of bringing diverse and potentially conflicting ideas into one room to facilitate transparent discussion, to challenge assumptions, and to lead to new insights to address cybersecurity risks facing the grid. A more robust discussion of the physical threats to the grid can be found in the previous National Academies reports *Enhancing the Resilience of the Nation's Electricity System*¹ and *Terrorism and the Electric Power Delivery System*.²

STRENGTHS OF THE ELECTRIC POWER SYSTEM

Several key themes emerged over the course of the workshop. First, participants described many steps that utilities and regulators have taken to help improve cybersecurity practices, which have in some respects made the electricity subsector a leader among critical infrastructure sectors. "I can only wish that other critical infrastructure sectors were as forward leaning as the electricity subsector is. There's a lot to be proud of," said Brian Harrell, Cybersecurity and Infrastructure Agency (CISA), Department of Homeland Security (DHS). Standards and regulations, best practices, and technology innovations all contribute to the safe and reliable operation of electric power infrastructure in the United States. Supervisory control and data acquisition (SCADA) systems, sensors, and other technologies provide granular situational awareness on grid operations in many places. Various reports, standards, and regulations guide resiliency protection protocols; examples include the *Roadmap to Achieve Energy Delivery Systems Cybersecurity*³ and requirements from the Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC). Many entities across the nation are actively involved in collaborative activities to increase resilience such as grid security exercises, mutual aid agreements, and peer-to-peer knowledge sharing through organizations such as the North American Transmission Forum and the North American Generator Forum. The Neighborhood

¹ National Academies of Sciences, Engineering, and Medicine, 2017, *Enhancing the Resilience of the Nation's Electricity System*, The National Academies Press, Washington, D.C., <https://doi.org/10.17226/24836>.

² National Research Council, 2012, *Terrorism and the Electric Power Delivery System*, The National Academies Press, Washington, D.C., <https://doi.org/10.17226/12050>.

³ Energy Sector Control Systems Working Group, 2011, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, U.S. Department of Energy, Washington, D.C.

Keeper program is an example of a solution incorporating vendors, utilities, and other electric system entities in information sharing.⁴

FACING MYRIAD THREATS

However, participants recognized that risk can never be totally eliminated and much opportunity for improvement remains. Many attendees stressed the gravity of the current and future threats, particularly those posed by the known capabilities of nation-state adversaries such as China and Russia. Several participants underscored statements in a 2017 Department of Defense (DoD) report⁵ indicating that “major powers (Russia and China) have a significant and growing ability to hold U.S. critical infrastructure at risk via cyber attack, and an increasing potential to also use cyber to thwart U.S. military responses to any such attacks.”

Speakers pointed to lessons offered by previous outages such as the 2003 blackout in the U.S. Northeast and the Ukraine grid attacks in 2016 and 2017, as well as malware incidents such as the 2014 Dragonfly cyberespionage attack⁶ and the 2017 TRISIS/TRITON attack.⁷ The threats come from numerous adversaries and are often underappreciated by the public and policy makers, speakers noted. “The reality is things are much more active than people would realize,” said Robert Lee of the cybersecurity firm Dragos. “Today, my firm tracks 10 different state actors that are exclusively targeting industrial systems. Only two of them have shown the capability to be destructive, but I’m worried about those eight that across that same trend in 3 to 4 years are going to be learning about how to achieve this.”

In addition to the complex cybersecurity threats presented by malicious actors, the grid faces threats from design flaws, accidents, and natural events. Particularly worrisome to some participants are the threats posed by EMP events, resulting from nuclear detonation at a high altitude or in space, and GMD events, which result from activity of the sun.

⁴ For more information on the Neighborhood Keeper program, see Dragos, “Neighborhood Keeper,” <https://dragos.com/neighborhood-keeper/>, accessed February 2, 2020.

⁵ Defense Science Board Task Force on Cyber Deterrence, 2017, *Report for the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics*, U.S. Department of Defense, Washington, D.C., https://www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf, accessed February 2, 2020.

⁶ For more information on the Dragonfly cyberespionage attacks, see https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf, accessed April 29, 2020.

⁷ For more information on TRISIS/TRITON attack, see Dragos, *TRISIS Malware: Analysis of Safety System Targeted Malware*, <https://dragos.com/wp-content/uploads/TRISIS-01.pdf>, accessed February 20, 2020.

Design changes over the decades—specifically, a shift toward single-phase transformers—have unintentionally increased the potential impacts of EMP and GMD events on grid infrastructure. The increased reliance on electronic control networks within and between substations has further compounded these vulnerabilities. Taken together, the design of today’s system combined with the likelihood of future GMD events creates the potential for widespread catastrophic failure involving unprecedented blackouts and permanent equipment damage affecting a large portion of the country. “Given sufficient time, the reoccurrence of a large [solar] storm event is a certainty—and it’s probably going to come with much more serious consequences than we’ve had in the past,” said John Kappenman of Storm Analysis Consultants.

Today’s threats are of a different nature and on a different scale than what existing systems were originally designed to withstand, some participants noted, and the impacts of a large-scale failure could be catastrophic for the U.S. economy and the health and safety of the American people. “The security and resilience of our country is becoming more intertwined with critical infrastructure than ever before,” said Caitlin Durkovich, Toffler Associates. “We also know that nation states understand and continue to get better insight into the importance of our nation’s infrastructure to our national security and our economic security.”

WORKING TOWARD RESILIENCE

To counter these threats, participants stressed the need to build resilient power systems, which committee member Bill Sanders defined as being capable of “providing trustworthy grid operation in hostile environments.” Several speakers urged a proactive effort to increase the capacity not only to protect and defend against attacks but to respond and recover when they occur. “We have to look at both sides of the equation,” said Scott Aaronson of the Edison Electric Institute. “We have to secure our infrastructure [and] we also have to be prepared to respond and recover.” Aaronson stressed that building for resilience goes beyond the subsector’s past emphasis on reliability. “Reliability assumes blue skies. Resilience is the ability to take a punch,” he said.

Many participants highlighted the increasing complexity of electric infrastructure. “The resiliency of the electric grid is highly dependent on the resiliency of cyber infrastructure,” said Sanders. “Grid resiliency is tied intimately to cyber infrastructure resiliency, but that translation, that connection [between the cyber and physical side] is a very complex one.” Component and software supply chains, as well as the growing interconnections with other critical infrastructure sectors such as communications, further complicate the challenge, to the extent that some

posited that the electric system is too complex to be adequately defended. “We are getting close to the limits of defensibility, mostly because we are at the limits of detectability,” said Tim Roxey, formerly of the Electricity Information Sharing and Analysis Center (E-ISAC). “Things occur and we don’t even know that they happened.”

The wide heterogeneity in the resources, capabilities, and operating models of different utilities suggests that there is no one-size-fits-all security solution. In some areas, attendees described how knowledge and tools are available to improve resilience but are not being implemented in practice due to financial, legal, or regulatory concerns. In other cases, knowledge gaps and technology limitations point to a need for additional research and development (R&D) investments. For example, grid exercises are valuable for bulk power systems, but state- and local-level entities have less involvement in these types of efforts and as a result may be less equipped to respond and communicate effectively when compromised. For EMP and GMD threats, participants discussed physical barriers and designs that could protect certain electric system elements, such as shielding conductive concrete, but noted that additional research, technology development, and modeling is needed to better understand, detect, and prepare for these threats. As another example, advanced sensing, analytics, and control functions can lead to better detection and response abilities for cyber and physical systems, but it will be important to transition to smart grid technologies in ways that enhance security and resilience without unwittingly increasing the attack surface. Throughout the workshop, participants pointed to a tension between improving existing legacy infrastructure and building new components more securely from the start, noting that it is necessary to do both.

STAKEHOLDER ROLES AND RELATIONSHIPS

Participants recognized government standards as an important component of the effort to address grid cybersecurity challenges, but some noted that standards and regulations are not agile enough to keep up with the threat landscape and the pace of technology innovation. The regulatory landscape is also highly varied: Speakers pointed out differences in regulation of bulk power versus public service commissions, bulk power transmission versus distribution, and commercial communications networks versus utilities’ private networks. For commercial communications networks, speakers noted that vulnerabilities could be introduced by the connections between the utilities’ private networks and the commercial system. Speakers also identified sectors and subsectors that are interdependent with the electric grid, such as natural gas and communications, noting that interruptions in these other systems could have major impacts

on the grid's ability to function and vice versa. "If you want to think about the future of the grid in a national security context, I urge you to think about taking a holistic approach," said Paul Stockton, Sonecon, LLC.

Participants grappled with questions about which areas are best advanced by government regulation, which are best advanced by best practices, and where incentives, assistance, or funding structures can reduce barriers to adoption. In addition, many participants noted that regulation can have the unintended consequence of reducing cybersecurity practices to a matter of compliance—in which utility personnel fear auditors more than they fear adversaries—rather than a true culture of security. "It has developed a culture where our technology experts fear the auditors more than they fear the enemy. . . . We have to get past that," said Marc Child, Great River Energy.

The solution, participants agreed, is not just about technologies: People, processes, and technologies are all essential components to improve cyber security and resilience. "There are cyber approaches to it, there are the traditional physical parts, and there are human parts that we need to account for as we put all of this together," said Sanders. Attendees discussed concrete ways for the field to move toward prioritizing and embedding security and preparedness into the daily operations of the electric grid, akin to the process by which the field successfully created a culture of safety decades ago. "I think now we're moving to this culture of security or resiliency," said Michael Hyland, American Public Power Association (APPA). But, he and others cautioned, "It's not going to come easy. We need to change the way people think."

The vast majority of the U.S. grid is owned and operated by private entities. Their job, and their expertise, is not to anticipate the military capabilities of the nation's potential adversaries, yet they find themselves on the front lines of defending their operations against nation-state and state-sponsored adversaries. Against this backdrop, participants underscored the need for collaboration—in particular, bridging between government and industry with public-private partnerships—to create and share vulnerability assessments, lessons learned, and mitigation strategies. In addition, some suggested that a central federal coordinating body is needed to establish an overarching strategy and corresponding policies, authorities, and regulations to achieve it. The government can support infrastructure security by providing faster, better, and more scalable mechanisms for information sharing; creating incentives for military defense-critical security installations; and maturing the national security doctrine and toolkit for when and how systems respond when adversaries probe them.

Last, throughout the day attendees raised the need to optimize the roles and relationships among all stakeholders, including industry,

regulators, vendors, researchers, policy makers, and the national defense community. By better defining the roles of various contributors and identifying ways for them to be complementary and supportive, rather than adversarial or duplicative, the field as a whole can better allocate its resources and facilitate the flow of information to accelerate progress. “We have to move beyond this current ‘piece-and-patch’ mentality,” urged Sanders. “We have to be ahead of the game.” While the challenges are substantial, he and other participants expressed hope in the subsector’s ability to meet them through collaborative efforts to create a secure, resilient, integrated, and modern infrastructure. “I think it’s critical that we act now,” Sanders said. “There has been a long set of basic work . . . and I think we have the basic understanding in place to allow us to make quick progress.”

Introduction

The Committee on the Future of the Electric Power System in the U.S., convened at the request of Congress and the Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability, is undertaking a comprehensive evaluation of strategies for adopting new technologies, operating and planning approaches, business models, and grid architectures in the U.S. electric power system. The committee is also considering ways to improve the reliability, resiliency, and flexibility of the grid, with an emphasis on cybersecurity and affordability challenges.

To support its information gathering, the committee convened a workshop on November 1, 2019, titled Communications, Cyber Resilience, and the Future of the U.S. Electric Power System. More than 330 individuals registered for the workshop to share perspectives on key cybersecurity challenges to the nation's electric grid and opportunities to address them. The workshop was the first of two events organized by the committee, with the second, held in February 2020, focused on models used for grid planning.

Granger Morgan of Carnegie Mellon University, committee chair, welcomed participants to the workshop. Committee member Bill Sanders set the stage for the discussions with a brief synthesis of the current state of computing in the grid and a charge for participants: "What I hope you all will do today is to help us understand how to build a modernized grid, but a modernized grid that improves, not compromises, the resiliency and the cybersecurity of the grid," Sanders said.

The workshop included six panel discussions featuring experts from industry, government, and academia, each followed by open discussions

among speakers, committee members, and workshop attendees. The agenda was designed to help the committee to synthesize current efforts, to increase the cyber resilience of the electric power system, and to explore fundamental tensions that underlie grid architecture and different computing and communication technologies and strategies, such as between simple and complex systems, or between compliance and preparedness. The field's approach to these issues will shape the evolution and the security of electric power systems over the coming decades.

The workshop was unclassified and open to the public. This report offers a condensed summary of the proceedings based on recordings, slides, and transcripts from the workshop, which can be accessed on the study webpage at www.nas.edu/gridmod.

Understanding the Threat Landscape

Several workshop sessions explored various facets of the threats facing the U.S. electric power system. Speakers examined the role and context of computing and communications technology in the electric grid; addressed the imperative to improve grid security from a national security perspective; and considered what constitutes grid resiliency and its cyber, physical, and human components. Panelists also addressed natural and man-made threats from electromagnetic pulse (EMP) and geomagnetic disturbance (GMD) events.

COMPUTING IN THE GRID

- Grid resiliency means providing trustworthy grid operations in hostile environments.
- The resiliency of the electric grid is highly dependent on the resiliency of cyber infrastructure.
- A holistic approach is needed to address the cyber, physical, and human components of grid resiliency.

William Sanders, Carnegie Mellon University, set the stage for the workshop with a broad overview of the issues surrounding security and resilience in the U.S. electric power system.

At the broadest level, Sanders said that the goal of grid resiliency is to provide trustworthy grid operations in hostile environments. To be trustworthy, a system should do what it is supposed to do, and nothing else.

In the context of electric power, this in part requires balancing and supporting goals for safety, confidentiality, integrity, and availability. It is also crucial to recognize that electric power systems operate in hostile environments beset by threats from accidental failures, design flaws, natural threats, and malicious attacks.

Advancing grid resiliency involves strengthening/enhancing cyber, physical, and human components. While there is much that can be learned from cyber resilience work in other fields, such as non-safety-critical business information technology (IT) systems security, the electric power system has important, unique attributes in terms of the systems, goals, and priorities involved. Existing reports, standards, and regulations in this area provide valuable guidance for resiliency protection protocols; examples include the *Roadmap to Achieve Energy Delivery Systems Cybersecurity*¹ and requirements from the Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC). However, in order to best support true cyber security, Sanders urged that the subsector must transition from a culture of compliance to a culture of true security and resiliency.

Pointing to some recent examples of malware attacks involving energy cyberinfrastructure, Sanders emphasized that the threats are real, they are becoming more sophisticated, and they are increasingly targeting both the physical and cyber elements of our power grid. He described disruptive trends that raise new issues and potential vulnerabilities: the development of “smart” grid infrastructure, adoption of Internet of Things (IoT) devices and cloud services in grid operations, use of dynamic renewable energy sources, and increased electrification of transportation. Against this fast-evolving backdrop, Sanders said that it is critical to recognize that grid resiliency is highly dependent on the resiliency of cyber infrastructure via a complex, interdependent relationship that is not well understood. The picture is complicated even further by interdependencies with other infrastructures, such as telecommunications, transportation, and financial systems.

Sanders highlighted what he sees as key gaps in efforts to advance grid resiliency, including advanced sensing, analytics, and control functions; better detection and response capabilities for cyber and physical systems; well-defined resiliency metrics and assessments; and more attention to the social, cultural, and human factors at play. He urged a holistic view as the field works to close these gaps. “We have to move beyond

¹ Energy Sector Control Systems Working Group, 2011, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, U.S. Department of Energy, Washington, D.C.

this current ‘piece-and-patch’ mentality,” he said. “We have to be ahead of the game.”

To ensure that resilience and security are enhanced (and not compromised) as the grid is modernized, Sanders emphasized that it is imperative for all players—industry, academia, and government—to collaborate to address both the near-term and the long-term challenges. While the challenges are substantial, he expressed hope in the field’s ability to meet them. “I think it’s critical that we act now,” Sanders said. “There has been a long set of basic work . . . and I think we have the basic understanding in place to allow us to make quick progress.”

CYBERSECURITY CHALLENGES

- There is wide heterogeneity in the cybersecurity challenges and capabilities of electric utilities across the United States.
- The threats facing the electric grid are heterogeneous, ranging from accidents, infrastructure failures, and natural events to malicious attacks from both outsiders and insiders.
- Existing tools, mechanisms, and partnerships offer promise, but significant progress has been stymied by a lack of research and development (R&D), implementation of existing solutions, or coordination.

Sanders introduced the first panel and moderated an open discussion following their remarks. The speakers were Brian Harrell, Cybersecurity and Infrastructure Agency (CISA) in the Department of Homeland Security (DHS); Michael Hyland, American Public Power Association (APPA); and Robert M. Lee, Dragos.

Brian Harrell, Cybersecurity and Infrastructure Agency

Brian Harrell, assistant secretary for infrastructure protection at CISA, focused on cyber-physical risk reduction. He highlighted risks posed to the grid’s key physical infrastructure in today’s multithreat landscape and described CISA’s perspective on the convergence between physical security and cybersecurity.

Harrell said that it is CISA’s view that the next major attack on critical infrastructure will likely have an insider component, whether from unintended information leaks or from radicalized personnel. An insider attack, by someone with “the keys to the kingdom,” could have devastating and cascading effects to U.S. power systems and other interdependent infrastructures. More worrisome still, existing systems may not be equipped to detect such breaches or recognize their severity when they occur, allowing insider threats to persist unchecked.

Industry standards have strengthened grid security, Harrell said, and the industry has a lot to be proud of. For example, mutual aid assistance agreements among 159 entities covering more than 80 percent of U.S. electricity customers enhance the cybersecurity coverage for those entities through intra-industry cooperation. Nevertheless, there remain reasons for concern and an imperative to act. First, Harrell urged that the industry create a culture of cybersecurity, akin to the culture of safety that was successfully established decades ago, and see that it is ingrained in the grid's daily operations. Second, he argued that supporting career transitions between government and industry would help to transfer knowledge and practices between these sectors and create a workforce that is better equipped to understand and address the threats at hand.

Michael Hyland, American Public Power Association

APPA represents more than 2,000 municipal utilities, from large cities to small towns. Michael Hyland, senior vice president of engineering services, discussed APPA's efforts to support cyber resiliency among its members.

Size and context affect each utility's security needs, priorities, and capabilities. While APPA includes a number of large utilities such as those in Los Angeles, San Antonio, Memphis, and Orlando, most of its members are far smaller, and about half have fewer than 2,000 meters. When it comes to cyber activities and capabilities, Hyland pointed to three main groups of utilities. The first is very small utilities that essentially have no operational technology (OT) such as supervisory control and data acquisition (SCADA) systems or Advanced Metering Infrastructure. Some of these smaller utilities, he said, do not even have websites or use e-mail. The second group is comprised of large utilities that have a well-developed OT/IT interface and staff dedicated to cybersecurity, many of which fall under the NERC, FERC, and Critical Infrastructure Protection (CIP) standards. The third group falls between these two groups. These utilities may have some distributed OT elements with communications such as SCADA, but do not have a great deal of dedicated expertise and often have disconnects between OT and IT systems with respect to managing their cybersecurity.

Echoing other speakers, Hyland said that APPA is working to encourage a culture of cybersecurity across this broad spectrum of electric utilities, but cautioned that it will be a challenge. Due to resource constraints, some utilities struggle to fully adopt a culture of safety or a culture of reliability, and changing the way people think is never quick or easy. To offer tangible support to help utilities strengthen their recovery and resilience capabilities, APPA entered into two agreements with the Department

of Energy (DOE). The Infrastructure Security and Energy Restoration (ISER) cooperative agreement, based on physical mutual aid agreements, is intended to help protect and reinforce physical infrastructure, while the Cybersecurity for Energy Delivery Systems (CEDS) agreement is aimed at bolstering protections on the cyber side.

Robert M. Lee, Dragos

Robert M. Lee, chief executive officer of Dragos, described the current threat landscape along with his concerns about common security practices in the electric power industry.

Lee argued that the threats to the U.S. electric power system are often underappreciated, especially by those outside the industry. Many simply do not realize how active the threat landscape is, how many nation-state actors are involved, and the degree to which U.S. systems are being targeted. While his firm deals with 2-3 major incident response cases per month stemming from activities by approximately 10 different nation-state actors, most are not publicized as is normal practice among those doing incident response. There are likely many more intrusions than are not detected, and of those attacks that are recognized, many are misunderstood. For example, Lee noted that when Symantec analyzed the Dragonfly cyberespionage attack in 2014, its report² focused on the electric industry impacts while largely overlooking impacts in other industries such as mining, transportation, and petrochemicals, which belied the scope of the attack.

Lee noted that our infrastructure is largely safe and reliable due to the significant investment our utilities have made. However, he characterized some of the practices that utilities must follow either due to regulation or “best practice” frameworks as “feel-good” security that wastes resources by focusing too much on ineffective preventative activities. As an example, a significant number of vulnerabilities introduce no risk to utilities yet necessitate a significant focus on vulnerability mitigation. As another example, utilities must deploy antivirus software; while this is not necessarily bad, it does not provide the same value in industrial and operations networks as it does in the context of enterprise networks. Lee said that many of the recommendations to utilities have been based on extending the enterprise security strategy instead of developing a unique and tailored strategy for the operations technology networks. While utilities are not to blame for this, as it was accepted practice for years, Lee argued

² Symantec Security Response, 2014, “Dragonfly: Cyberespionage Attacks Against Energy Suppliers,” https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf.

that practices should change now that the weaknesses of this approach are better known. On the positive side, however, Lee noted that effective defensive cybersecurity mechanisms are available and, when implemented properly, they work well.

Lee noted that, in contrast to decades past, security expertise today is concentrated in the private sector rather than in the government, a shift he attributed to cooperation and partnership between government, which was focused on cyber security earlier than industry, and the private sector over the years. When Congress and others seek to determine best practices and insights on the problem, Lee suggested that they should first look to the security practitioners at leading utilities now. While it is valuable to have this expertise within industry, it is important to note that industry is in the beginning phases of this transition and that today still too few companies undertake a root-cause analysis after an incident to determine if there was a cyber component to the issue or not. As a result, it can take too long to determine if a crisis is created by an attack or by a defect, giving the adversary a second chance to attack, as happened in the 2017 TRISIS/TRITON attack in Saudi Arabia. In that incident, the XENOTIME adversary purposefully tried to kill people by targeting a Safety Instrumented System; the attack was originally erroneously diagnosed as a maintenance issue.³

By contrast, root-cause analysis couples incident response with protections and practices that are implemented from the get-go. “We have to think about the response strategy first,” said Lee. “That response strategy is going to drive the detection strategy to get there, and that’s going to drive the collection and preventative strategy we want to put in place.”

Lee commended current efforts to address this need, including the CEDS agreement, the Roadmap to Achieve Energy Delivery Systems Cybersecurity, and the Neighborhood Keeper program,⁴ a collaboration between Dragos and DOE. Ultimately, to best protect our energy infrastructure, Lee asserted that it will be essential to simultaneously learn from the threats by adopting an intelligence-driven approach while also designing a better infrastructure that reduces the threat landscape and the attack surface, an approach being advanced by efforts such as the DOE Consequence-Driven Cyber-Informed Engineering program.

³ For more information on the TRISIS attack, see Dragos, *TRISIS Malware: Analysis of Safety System Targeted Malware*, <https://dragos.com/wp-content/uploads/TRISIS-01.pdf>, accessed February 20, 2020.

⁴ For more information on the Neighborhood Keeper program, see Dragos, “Neighborhood Keeper,” <https://dragos.com/neighborhood-keeper/>, accessed February 20, 2020.

Discussion

Participants discussed current vulnerabilities, the use of tools and models in this space, and the need for partnerships to address cybersecurity challenges.

Understanding Vulnerabilities

Granger Morgan, Carnegie Mellon University, asked panelists to comment on vulnerabilities posed by legacy infrastructure such as outdated operating systems and unprotected wireless networks. Lee answered that the risk posed by the ongoing use of legacy equipment has been somewhat overplayed, and what is more important is not what operating system is running, but whether utilities can accurately detect attacks and respond to them.

Gavin Donohue, Independent Power Producers of New York, Inc., asked if the cyber operations side has focused on being “prepared to fail” to the same degree that the electricity subsector in general has done. Hyland replied that more education and preparation is needed, and Harrell stressed that grid failure exercises including cyber threats are a valuable learning exercise for these efforts.

Tools and Models

Mark Lauby, NERC, asked about the status of efforts to build simulation tools, models, and risk assessments. Sanders pointed out that while researchers cannot model what is not understood, there are models available that could be scaled up, tested, and used for planning exercises. Hyland agreed, although he noted that while utilities are familiar with the impacts of weather, animals, and other everyday problems, more research is needed to characterize and model malicious attacks. Harrell added that vendors should play a more integral role in these modeling and planning efforts in order to better integrate security into systems.

Lee answered that despite the unknowns, good modeling exists for predictable scenarios and their secondary consequences. In the face of uncertainty as to the optimal amount to invest in cybersecurity, he emphasized that utilities should at a minimum be prepared to respond to known scenarios such as ransomware attacks and the events in Ukraine in 2015 and 2016. He added that there is a lack of a combined voice advocating for using these tools and stressed that a successful solution will rely on a combination of people, process, and technology.

Michael Howard, Electric Power Research Institute (EPRI), wondered if an artificial intelligence (AI)-based approach could be used to detect

and prevent insider threats in the future. Harrell noted that it is not possible to eliminate every threat, but a vigilant threat management program that includes human resources, operations, physical security, legal, and technological means—all of which exist today but are not fully implemented—could be the most successful at detecting suspicious internal activity.

The Need for Partnerships

Hyland emphasized the need for public-private partnerships (PPPs) that include R&D to create new technologies for the grid. Big or small, utilities cannot meet all of the needs alone, he argued. Lee agreed and pointed out that many of the technologies mentioned—such as detection capabilities and prevention strategies—already exist, while some that get advocated as a key to success, such as AI and blockchain, have not yet been shown to deliver value in security.

Jeffery Dagle, Pacific Northwest National Laboratory (PNNL), asked what, specifically, PPPs should be studying. Lee suggested that they deemphasize things that industry is good at, such as incident response, and focus instead on broader needs, such as supply chain security. Hyland praised the partnership that enabled APPA to create a scenario modeled on the attack on Ukraine's electric grid, which municipalities can use to see exactly how much an outage would cost in relation to cybersecurity investments. Harrell added that PPPs also excel at pushing timely, accurate information during crises; as such, they could play a part in securely disseminating information to the right players within government and industry.

EMP AND GMD CHALLENGES

- Although less likely than cyberattacks, GMD and EMP events pose serious threats to grid infrastructure and operations.
- Existing standards, detection capabilities, and mitigation strategies provide some protection against these threats.
- Further research and implementation are needed to better understand the risks and increase resilience to catastrophic events.

Michael Howard, EPRI, set the stage for a panel on challenges related to EMP and GMD events, with a brief discussion of the nature of these events. An EMP is a man-made event resulting from a high-altitude nuclear blast. It has three components: E1 (an intense electromagnetic field occurring within nanoseconds of a nuclear blast), E2 (an intermediate duration pulse, lasting from about one microsecond to one second

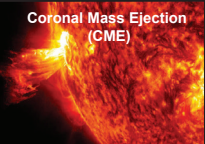
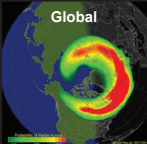


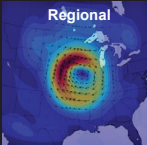

	Source	Area of Impact	Electronics Damage?	Magnitude	Duration	Frequency
GMD	 Coronal Mass Ejection (CME)	 Global	None	 < 10 V/km ~ 0	Days	Occur Frequently With Varying Intensity
HEMP E3	 Detonation of a Nuclear Weapon at High-Altitude or in Space	 Regional	Wide-area Damage from E1 is Possible Before E3 Arrives	 10's V/km ~ 0	< 5 Minutes	HEMP Attack Has Never Occurred

FIGURE 2.1 Comparison of GMD events and the E3 component of a high-altitude EMP (HEMP E3). SOURCE: Michael Howard, presentation to the workshop, from Electric Power Research Institute.

with an intensity similar to a lightning strike), and E3 (a pulse lasting tens to hundreds of seconds whose effects are similar, although not identical, to the effects of a GMD). A GMD is a natural event created by activity on the sun, specifically a coronal mass ejection (CME). While both types of events can have serious impacts on the electric grid, they differ in their spatial range, magnitude, duration, frequency, and impacts on electronics (Figure 2.1).

Howard introduced the speakers and moderated an open discussion following their remarks. Speakers included John Kappenman, Storm Analysis Consultants; Mark Lauby, NERC; and Randy Horton, EPRI.

John Kappenman, Storm Analysis Consultants

John Kappenman, founder of Storm Analysis Consultants, emphasized the vulnerability of today’s grid to GMD and E3-EMP events (E3-EMP, the slow pulse component of EMP, is similar to naturally occurring GMD events). The bulk transmission network has been growing more vulnerable to these threats for many decades for two important reasons, Kappenman said: The development and growth of extra-high-voltage networks, which allow larger geomagnetically induced current (GIC) flows, and the usage of single-phase transformers on these same networks that are more easily saturated by GIC flows. These combined design decisions have unintentionally increased the potential impacts of EMP and GMD events on grid infrastructure and have been unchecked by a rational design code that took this threat into consideration, Kappenman said.

Kappenman added that, for the fast pulse E1-EMP, the increased reliance on electronic-based controls and devices that have replaced older style electromagnetic relays and control systems in the electric grid has greatly increased vulnerability to this threat. The E1-EMP could disrupt operation and permanently damage distributed electronic control systems used in SCADA across the bulk transmission network, in distributed control systems in power plants, and even within critical end-user systems.

Kappenman noted that both severe GMD and EMP threats will have large geographic footprints of continental scale and could impact most of the bulk electric grids simultaneously across North America.

GMD threats are not purely theoretical: In 1989, a solar storm caused a grid collapse in Quebec, Canada, with intensities of about 400 nanotesla per minute,⁵ and scientists estimate storms could be 4-10 times more intense. Taken together, the design of today's system combined with the likelihood of future GMD events creates the potential for widespread catastrophic failure involving unprecedented blackouts and permanent equipment damage affecting a large portion of the country. "Given sufficient time, the reoccurrence of a large storm event is a certainty—and it's probably going to come with much more serious consequences than we've had in the past," Kappenman said.

In regard to EMP, Kappenman emphasized that many critical state-of-the-art control systems utilized in power plants and SCADA are restricted from being exposed to electric fields from cell phones, which have an output in the range of 1-3 volts per meter (V/m). By comparison, the E1-EMP pulse field strength can be as high as 50,000 V/m, a level that would not only disrupt sensitive control system operation but that is also likely to cause widespread permanent damage to many of these electronic-based systems and hamper the ability to rapidly restore critical infrastructures necessary to sustain lifeline services to the population.

Due to the large geographic footprint of EMP events, even a regional EMP E1 event could expose thousands of substations and generating plants across the U.S. grid's infrastructure at once. Unfortunately, this vulnerability both invites and rewards attacks. To reduce this vulnerability, Kappenman suggested targeting skeletal portions of the existing power grid that could provide at least limited lifeline support in a post-EMP attack scenario. For construction of new facilities, newly developed radio frequency-absorbing shielding concrete and new designs for protective control buildings could be used to encase and protect sensitive electronic infrastructure with minimal additional costs over previous designs, he said.

⁵ The tesla is a unit of measurement for magnetic fields. One nanotesla equals one billionth of a tesla; Earth's magnetic field is in the range of 25,000-65,000 nanotesla.

Protecting our infrastructure will require balancing costs and efficiencies, but maintaining the capability to rapidly restore operations and support basic lifeline services in a worse-case scenario is essential, Kappenman concluded.

Mark Lauby, North American Electric Reliability Corporation

Mark Lauby, senior vice president and chief engineer at NERC, discussed NERC's work on creating GMD and EMP protection standards.

NERC has mandatory GMD reliability standards, developed in partnership with government, industry, and academic experts. As zero risk is impossible, the goal instead is to minimize risk, Lauby said. The standards include mechanisms for understanding potential attacks, practicing risk assessments, and creating action plans for various scenarios.

NERC is also in the process of developing an EMP strategy, based on EPRI research. A task force is identifying vulnerabilities, reliability concerns, and resiliency methods. The next step is to seek input from government, industry, and researchers and incorporate ideas for response and recovery.

Randy Horton, Electric Power Research Institute

Randy Horton, senior program manager at EPRI, described a recently completed 3-year study⁶ that his team conducted on how to best respond to and mitigate a high-altitude EMP (HEMP) event. The project, a collaboration involving 63 U.S. utilities, DOE, the U.S. Department of Defense (DoD), and several national laboratories, sought to identify the impacts of a HEMP attack on transmission systems (switchyards, lines, and substations) and identify the most cost-efficient protections to implement.

While the team considered impacts of all three HEMP components (E1, E2, and E3), a significant portion of the research focused on E1 HEMP impacts. Team members developed computer models to estimate anticipated stress levels to compare against the strength of existing equipment; where data were not available, such as for digital protective relays, they conducted laboratory tests to fill knowledge gaps. Their findings indicated that some equipment, such as relays, were fairly resilient to a free field E1 HEMP pulse, but conducted surges—for example, the voltage and current surges that can be generated by the coupling of the E1 HEMP pulse into a control cable—pose a greater threat. Using low-voltage surge protection

⁶ Electric Power Research Institute, 2019, *High-Altitude Electromagnetic Pulse and the Bulk Power System: Potential Impacts and Mitigation Strategies*, EPRI Technical Report 3002014979, Palo Alto, Calif.

devices and filters, shielded control cables, and enhanced grounding and bonding practices could help mitigate this risk, Horton said. Improving the shielding of substation control houses is also recommended and can help mitigate any potential risk from free field E1 HEMP.

For the project's second phase, the team is working with 19 U.S. utilities to develop tailored risk and impact assessments and then install and test mitigation solutions. They hope that this effort will not only benefit the involved utilities but also provide valuable data on costs and maintenance needs, Horton said. Noting that transmission impacts are only one part of the puzzle, Horton added that EPRI is also examining interactions and sharing information with other infrastructures, such as telecommunications, which could also be affected by a HEMP attack.

Discussion

Panelists and attendees discussed priority areas for further research into EMP and GDM events and opportunities to improve protection and response capabilities.

EMP Research Needs

Recognizing that it is impossible to fully defend against EMP attacks, Kappenman suggested that future work should focus on building better protective spaces, based on better design standards, that incorporate visionary approaches such as shielding concrete. Lauby stated that better EMP protection will come from more reliable wavefront information. He also suggested expanding the research scope beyond transmission systems into generation and distribution impacts, and even, Horton added, into interactions with other critical infrastructures. To support these efforts, Horton and Lauby agreed that industry and utilities need to have access to high-quality EMP-E1 assessment tools, as well as the expertise to use them.

GMD Research Needs

On the GMD side, Kappenman stated that better GIC measurements are needed to increase understanding of the complexities surrounding ground conductivity to depths of hundreds of kilometers. Participants pointed to research being advanced by the American Geophysical Union as relevant to improving knowledge in this area. Lauby, Kappenman, and Horton added that GMD research should also zero in on transformer thermal impacts, given their potential for catastrophic consequences, including to public health.

Improving Capabilities

Jeffery Dagle, PNNL, asked whether utilities have the capability to proactively take precautions when GMD events are approaching that exceed the magnitude their systems were designed to withstand. Lauby replied that every utility has an emergency operations plan to pre-position systems, and that includes restoration plans for unpredictable events. Kappenman added that while transformers have resiliency standards and ratings, many fall short of these standards in practice, making transformer failure a real possibility. In addition, he noted that there remain gaps in our understanding of how GMDs occur and how large and how long they can be, raising the troubling prospect that the true threats may go beyond what is captured in existing models. The more data that is uncovered, released, and studied, the better utilities can prepare, he said.

In response to a question by Mark Adamiak, Adamiak Consulting, panelists agreed that more solutions could evolve from available and emerging technologies, such as GIC blocking devices and other possible mitigation actions.

Cynthia Hsu, National Rural Electric Cooperative Association (NRECA), asked about the lifespan of existing GMD detection infrastructure in space and whether additional or replacement monitoring satellites are needed. Lauby agreed that better equipment for advanced detection was necessary, particularly to reduce false positives, but noted that existing equipment is tested on a regular basis. Horton stated that more descriptive measurements of the storm—estimating the electric field on the ground that determines the impacts, rather than only the K-index of the storm's impact on Earth's magnetic field—would be helpful. Kappenman added that satellites to measure GMD are single-point-of-failure machines, operating in the harsh space environment, and so are not fully reliable.

NATIONAL SECURITY IMPLICATIONS

- The electric power system is vital to U.S. national and economic security.
- The electricity subsector is enmeshed within an ecosystem of interdependent infrastructures.
- A holistic approach that accounts for the current and future threat landscape and the different roles and capabilities of government and industry could help improve the defensibility and resilience of the U.S. electric power system.

Morgan introduced a panel and moderated a discussion on national security implications of cybersecurity threats to the electric power system.

The speakers were Caitlin Durkovich, Toffler Associates; Paul Stockton, Sonecon, LLC; and David Batz, Edison Electric Institute.

Caitlin Durkovich, Toffler Associates

Caitlin Durkovich, director at Toffler Associates, discussed the importance of critical infrastructure to our national and economic security. Any disruption, from a weather event or a deliberate attack, could cascade across sectors and have significant consequences. Durkovich argued that the stakes have risen as infrastructures grow more interdependent and our adversaries look for opportunities to cause widescale disruption. “The security and resilience of our country is becoming more intertwined with critical infrastructure than ever before,” Durkovich said. “We also know that nation-states understand and continue to get better insight into the importance of our nation’s infrastructure to our national security and our economic security.”

To better protect our electric power grid and design systems that are secure, resilient, integrated, and modern, Durkovich outlined her vision for a central “belly button” in the federal government that would be responsible for establishing an overarching strategy and the corresponding policies, authorities, and regulations to achieve it. While the private sector owns and operates the assets within this critical infrastructure, she asserted that the federal government should have a role in creating a roadmap for a modern infrastructure system, and that public-private partnerships could be a valuable mechanism for building security and resilience into electric power infrastructure from the beginning.

This new vision, she stressed, must also account for the initiatives, processes, sensors, and technologies being deployed in the shift toward “smart” communities, both in the civilian and military context. While acknowledging that some important steps have been taken, Durkovich expressed her view that federal policy needs to further encourage and enable the shift to smart infrastructure. “Current federal policy is not incentivizing a shift to a modern infrastructure, especially in the energy sector, Durkovich said. “I think that we have to move quickly if we are going to get this right.”

America’s adversaries are adept at pushing the boundaries of engagement without generating a kinetic response from the United States, Durkovich said, and it is apparent that nation-state adversaries such as Russia have the potential to infiltrate U.S. infrastructure with malware and other technologies and “lie in wait,” ready to act when tensions escalate. China’s theft of U.S. intellectual property and its integral role in our supply chain further underscore the threats from abroad. To counter these threats, she reiterated the need to establish a centralized group

authorized to formulate and implement a smart infrastructure strategy and suggested updating and continuing the work already ongoing under *Presidential Policy Directive 21*.⁷ She urged a renewed focus on foreign interference, improving understanding of risks posed by new technologies, and expanding our capability to anticipate decades into the future, not years.

Paul Stockton, Sonecon, LLC

Paul Stockton, managing director of Sonecon, urged taking a holistic perspective on the future of the grid in a national security context. While he believes that today's bulk power system entities and mandatory standards have kept pace with past threats reasonably well, he argued that further evolution is necessary given the severity of today's threats, particularly those posed by Russia and China.

Beyond the infrastructure that comprises the actual electric grid, there are many interdependent sectors that enable and support the electricity subsector that are often overlooked and less well protected, making them susceptible to attack. For example, natural gas is a critical fuel source for power generation, and an attack on those pipelines could disrupt power generation—an indirect but effective way to compromise grid reliability. Stockton noted that former Director of National Intelligence Daniel Coates said in the Office of the Director of National Intelligence's 2019 threat assessment⁸ that China has the ability to disrupt the flow of natural gas in a transmission pipeline for days to weeks.

To address these gaps, Stockton suggested establishing a design basis threat (DBT) for the oil and natural gas subsector. This would give grid owners and operators, as well as regional transmission organizations and independent system operators, a shared understanding of the threats to design resilience initiatives against. This understanding would include lessons learned from nuclear power plants and grid DBTs for physical security threats.

Stockton added that another often overlooked area of potential vulnerability is the nation's ability to conduct blackstart power restoration—that is, to restart electricity generation from within a blacked-out area, rather than by importing power from outside the area to restart generation assets. Utilities responsible for blackstart must comply with rigorous

⁷ Office of the Press Secretary, 2013, *Presidential Policy Directive 21—Critical Infrastructure Security and Resilience*, The White House, Washington, D.C.

⁸ D.R. Coates, 2019, *Worldwide Threat Assessment of the U.S. Intelligence Community. Statement for the Senate Select Committee on Intelligence*, <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR-SSCI.pdf>, accessed February 20, 2020.

training and simulation requirements. However, it is impractical for them to test blackstart operations under fully realistic conditions (i.e., by intentionally turning off parts of the grid). In addition, because many blackstart generators run on natural gas, they could be vulnerable to a disruption of gas supplies. This vulnerability represents another example of the challenges presented by hidden interdependencies in our critical infrastructure.

Stockton noted in closing that similar cross-sector dependencies exist for many other infrastructure sectors, including communications systems and water utilities.

David Batz, Edison Electric Institute

David Batz, senior director of cyber and infrastructure security at the Edison Electric Institute, delineated the different roles for government and industry in increasing the resiliency of the nation's electric power system, and how each can best operate within its own "swim lanes" to do this more effectively.

The vast majority of the U.S. grid is owned and operated by private entities. Their job, and their expertise, is not to anticipate the nation's war-fighting capabilities, yet they find themselves on the front lines of defending their operations against nation-state and state-sponsored adversaries. The government, Batz suggested, can support infrastructure security by providing faster, better, and more scalable mechanisms for information sharing; creating incentives for defense-critical security installations; and detailing response plans for when adversaries probe systems.

Funding is also a challenge. Resilience mechanisms cost money, yet today's rate-making structures are on the whole insufficient to support adequate defense and resilience against today's threats, Batz argued. He added that rate structures fail to account for the relative importance of different electricity needs, giving equal weight, for example, to a recreational ice-skating rink and to a military base.

To move forward, Batz stressed the need to diversify fuel sources, vendors, and suppliers across the U.S. electricity subsector and in particular underscored the need to provide adequate funding for nuclear facilities. In addition, he stressed the need for collaboration as researchers seek to increase resiliency. As an example, he pointed to the 2006 Spare Transformer Equipment Program (STEP), in which utility owners and operators collaborated with FERC to create a transformer-sharing program for physical attack recovery. The program required incremental cost increases, which were absorbed into utility rates. Batz suggested that similar approaches could be implemented elsewhere where a relatively small investment could bring big payoffs in terms of resiliency.

“Let’s broaden the aperture and think about where else within our critical infrastructure we can invest toward resilience and not in all cases drive toward the lowest cost,” he said.

Discussion

Attendees and panelists discussed challenges related to funding and the supply chain and identified suggestions for improvement more broadly.

The Need for Funding

Providing adequate funding to address national security threats related to the electric power system is a difficult balance, Morgan said. While customers and business structures in this subsector have driven prices ever lower, government financing or incentives run the risk of overcompensating and leading utilities to “gold plate” infrastructure unnecessarily.

Durkovich added that customers demand low prices, not better security. A public education campaign may help, but she contended that little will change until people are willing to pay more for a secure and resilient infrastructure.

Stockton agreed that consumers rarely prioritize security over low prices, and added that certain basic needs, like water, *should* be kept inexpensive. It may be possible, instead, to make a compelling economic argument for the utilities to invest in security—for example, by assigning a dollar value to resilient power.

Securing the Supply Chain

Jeffery Dagle, PNNL, asked how cybersecurity supply chain vulnerabilities could be reduced. Batz answered that securing the supply chain will require a complete risk management overhaul, with multiple components that enable operators to understand the potential threats at every layer. While some cybersecurity components, transformers, and protective relays are made in North America or Europe, he noted that heavy equipment and consumer products are largely made in China, which creates vulnerabilities.

Suggestions for Improvement

Cynthia Hsu, NRECA, asked what responsibilities for national defense and cybersecurity are falling through the cracks between efforts and missions across federal agencies and the federal government.

Morgan pointed out that while bulk power is regulated by the federal government, public service commissions operate at the state level in a complicated regulatory environment. He and Durkovich noted that state- and local-level critical assets will shoulder a significant share of the burden when serious problems occur and would benefit from more exercises in order to build their capacity to respond effectively. Hsu agreed that local and smaller, state-level infrastructures would benefit from cybersecurity exercises to improve communication and response capabilities.

From a broader perspective, Durkovich suggested that the government should reassess security priorities and counterthreat mechanisms, perhaps creating regime similar to the 2002 SAFETY Act, which encourages anti-terrorism technological innovations, for the energy sector. She also noted that government and industry are both facing workplace talent challenges that will affect how we build, maintain, and secure our infrastructure.

Stockton pointed to information warfare as another important and often overlooked threat. For example, pairing a grid attack with disinformation to sow public distrust in leaders could be more damaging than a grid attack alone. Durkovich agreed, positing that while our enemies get ever more creative and capable in terms of manipulating perceptions, the U.S. government remains too focused on the current risk landscape, to the detriment of its ability to imagine and plan for future threats. “The thing that I am concerned about is that we are so focused on today—are we doing enough to think about tomorrow?” Durkovich asked, reiterating her suggestion that the government fund a new entity that considers the whole spectrum of critical infrastructure and looks decades into the future, creating a roadmap not only for new technologies but also for new threats.

John Kappenman, Storm Analysis Consultants, noted that the grid’s dependency on natural gas, especially for a blackstart, has fallen through the cracks, and emphasized the need to find a different fuel source or create a national policy regarding fuel reserves during a crisis. Batz agreed that such an investment would improve resilience, as would creating a fully realized catastrophe plan that ensures sufficient reserves and reduces utilities’ dependence on “just in time” inventory.

Stockton pointed out that system tests and crisis exercises would be more effective if they considered the impact of infrastructure interdependencies, instead of focusing on just one sector. Anjan Bose, Washington State University, noted that better modeling and simulation tools are also needed, and Michael Howard, EPRI, added that there is also a particular need for tools to better understand the interactions between the multiple infrastructures. Durkovich agreed that simulation tools are important, but emphasized that it is important to recognize that no simulation can fully re-create a true crisis. The human element is essential, she added, because in a real crisis, nothing will go as planned.

Strategies to Increase Resilience

A second set of panels focused on addressing the challenges faced by the grid through concrete steps to increase resilience. These panels addressed technological means to improve cybersecurity as well as the cultural, business, and policy contexts of implementing those technologies. Speakers also addressed ways to speed the path from solution development to deployment in order to keep pace with a rapidly evolving threat landscape.

TECHNOLOGICAL CAPABILITIES

- The electricity subsector has taken many steps to improve cybersecurity practices, but risk can never be totally eliminated and there remains much to do.
- Grid security is affected by both utility-owned operational communications networks and commercially owned enterprise communications networks, along with the interactions between these networks.
- Existing and emerging security mechanisms offer promise, but their development and adoption are affected by complex business and regulatory contexts.

Jeffery Dagle, Pacific Northwest National Laboratory (PNNL), moderated a panel exploring how technologies can be used to improve security and resiliency. While complexity is the enemy of security, adding security measures to electric infrastructure is anything but simple, Dagle said. Utilities and the country as a whole are challenged to determine when and

where cybersecurity should be incorporated into electric power systems, whether these efforts should be centralized or distributed, and which players should be responsible for what. Speakers included Joy Ditto, Utilities Technologies Council (UTC); Mark Adamiak, Adamiak Consulting; Samara Moore, Amazon Web Services; and Tim Roxey, formerly of the Electricity Information Sharing and Analysis Center (E-ISAC).

Joy Ditto, Utilities Technologies Council

Joy Ditto, president and chief executive officer of UTC, described how the relationship between the electric power system and the U.S. telecommunications infrastructure has evolved over the decades.

After World War II, the U.S. electric power infrastructure was identified as critical to the nation's security and economic well-being. Utilities recognized the importance of reliable communications to support the electric grid, but existing telecommunications carriers were unable to provide the level of service they needed at a reasonable price. This, Ditto explained, drove the electric utilities to build their own private communications networks, based on a combination of copper wire lines and microwave wireless components. These networks supported reliable voice communication within operations centers and between personnel in the field.

In the 1980s, utilities began layering digital communications technologies over these existing networks, gradually replacing copper wire lines with fiber where feasible. This digital layer broadened communications beyond voice to include data collection, enabling supervisory control and data acquisition (SCADA) systems, sensors, and other technologies providing granular situational awareness on grid operations. In addition to these utility-owned networks, some utilities also use commercial telecommunications services for purposes other than critical operations support, such as for corporate telephones and external-facing websites.

Ditto argued that operational digital communications technologies, built on the backbone of the utilities' private communications networks, are crucial to enabling integration of renewables and energy storage technology into today's grid and will likely be key to enabling advanced distribution technologies in the future. Utility-owned networks are more reliable, better hardened against damage, and more resilient than commercial carriers, Ditto asserted, noting that utilities were able to help telecommunications companies recover after Hurricane Katrina.

Despite their benefits, the digitization of these networks also introduced vulnerabilities, which were largely overlooked until the late 1990s. Because cybersecurity protections were not built in from the beginning, Ditto said that strengthening security for these systems requires a combination of adding security measures to existing infrastructure while also

building protections into any new components. She urged a closer look at how the vulnerabilities within these private networks, and their coexistence with commercial networks, affect grid security.

Mark Adamiak, Adamiak Consulting

Mark Adamiak, principal at Adamiak Consulting, discussed cybersecurity in the context of utilities' private operations communications networks and the commercial telecommunications services they also use.

As Ditto noted, utilities often use a private network for critical operations controls (the operations network) and commercial telecommunications services to access the Internet and communicate with customers (the enterprise network). While most utilities keep these networks completely separate, with air gaps to help ensure that operations networks are not in any way connected to the Internet, Adamiak said that some utilities connect them through a jump box. The jump box creates a highly regulated path by which approved information can flow from the enterprise network into the operations network—for example, to allow an engineer to update relay settings. Utilities have less control over the enterprise network, so it is more difficult to secure. Common protections include firewalls and external access controls, but the sheer number of attack attempts suggests stronger mechanisms may be warranted, Adamiak noted.

Operations networks, for their part, have various defensive protections built in, some of which are mandated by North American Electric Reliability Corporation (NERC) guidelines. Common mechanisms today include nonroutable IP addresses, firewalls, air gaps, cryptographic accelerators, and role-based access control. In addition, many utilities are adopting new cybersecurity mechanisms for their operations networks. Examples include trusted platform modules for SCADA remote terminal units; password management systems and key distribution centers that take the human element out of password protections; and the use of secure communication protocols such as Secure File Transfer Protocol, Secure Shell, virtual private networks, PUSH mechanisms such as data diodes, the industry's own protocol IEC 61850, and routable Generic Object-Oriented Substation Event (GOOSE). Adamiak noted that securing operational communications will be particularly essential as grids transition to microgrids.

Samara Moore, Amazon Web Services

Samara Moore, security assurance and energy specialist at Amazon Web Services, discussed electric utilities' increased adoption of cloud services for enterprise information technology (IT).

Cloud services provide on-demand delivery of IT services over the Internet under a pay-as-you-go model with strong security and resiliency features, Moore said. She asserted that cloud services could help utilities be more agile and elastic, especially in times of crisis, by allowing them to increase or decrease IT resources rapidly; save on IT costs—for example, by reducing the resources needed to maintain infrastructure and data centers; and drive innovation through access to advanced services, tools, and automation capabilities. She suggested that cloud services could be especially beneficial for smaller utilities without a large IT staff, for whom the security mechanisms and advanced tools offered by cloud services might be otherwise unattainable.

Moore expressed her view that cloud services can support utilities' security objectives, including those related to regulatory requirements. Cloud infrastructure is built to meet very secure standards, is tested on multiple frameworks to meet multiple global requirements, and supports government, academia, and large enterprise customers. In addition, cloud service companies are constantly innovating to anticipate future needs and develop technologies to address them, allowing their customers to take advantage of the latest innovations without having to make large IT investments in-house.

Tim Roxey, Electricity Information Sharing and Analysis Center (Retired)

Tim Roxey, who previously held roles at E-ISAC and NERC, argued that the electric power system is reaching the limits of defensibility.

In massively complex systems such as electric power infrastructure, Roxey argued that we have accepted heightened dependence on automation technologies without fully understanding how the Industrial Control System (ICS) and power elements interact and without an appreciation for the consequences of their failure. As a result, he posited that we have arrived at a place where reliability, safety, and security are all uncertain.

Asset owners tend to overestimate their ability to defend these systems and underestimate the extent to which they have become almost entirely dependent on them, Roxey said, raising the question: How do you defend a complex system when you don't even understand its contents? Comprehensive, current, and accurate asset inventories are rare and fleeting. Furthermore, he argued that it is no longer possible to fully understand our systems of systems; thus, they can no longer be fully defended. We are stymied by the massive complexity of aggregate systems as well as by the overly complex software-centric components they comprise.

Roxey characterized the ICS field's current tack on cybersecurity as an incremental approach in which small changes are made over time to ICS and its components that offer more functions or implement new technologies. Many times, new security methods are even implemented. Over time, the individual elements of the ICS become more advanced—for example, incorporating Internet of Things (IoT), artificial intelligence (AI), and 5G elements—and the collective system they form becomes ever more complex.

A far more effective approach, he argued, would be a transformational overhaul in which legacy vulnerabilities are eliminated by re-creating and recompiling systems from the fundamental physics on up. He acknowledged that this path is difficult but asserted that it is nevertheless possible, and clearly necessary if we are to continue to operate with confidence in a cyber world that former Navy Secretary Richard Danzig has characterized as “continuously contested.”

As an example of the weaknesses of existing systems, Roxey detailed a vulnerability known as Aurora, which targets motors and generators, rotating AC machines. When the digital protective control devices (DPCDs) that protect motors and generators are manipulated by remote adversaries to open and close rapidly, the associated motor or generator can be damaged or destroyed. The vendor community stepped up to address this vulnerability by changing the programs (software logic) inside the DPCDs. This incrementalistic solution does indeed address the specific vulnerability that was found, but the essential vulnerability remains. It is indeed the actual DPCD device that can be discovered and reached over the networks and then controlled to perform the rapid open-close sequence that is the issue.

A transformational approach would implement Aurora protection using the basic grid physics of rotating AC machines and do so in a manner not dependent on modern, highly networked ICS devices.

Discussion

Panelists and participants discussed the effectiveness of existing defense mechanisms, policy and regulatory issues, and system-level solutions.

The Effectiveness of Existing Defense Mechanisms

Dagle and Granger Morgan, Carnegie Mellon University, asked panelists to elaborate on the use and effectiveness of existing defense mechanisms such as air gaps and firewalls. Ditto noted that while air gaps are currently effective, adversaries may eventually find a way around them.

When it comes to firewalls, Roxey agreed with Dagle that firewalls are far more porous and less secure than is generally assumed, making them another example of how network configurations are often too complex to be fully understood, leading to vulnerabilities.

In the face of imperfect protections, Ditto posited that it is key to at least be able to detect any breaches that occur. “I think it comes back to how much situational awareness do you have around your network, and if you know that you are going to have vulnerabilities but you can limit them or you can at least be aware when those vulnerabilities are being exploited, that is a good place to be,” she said. To achieve that awareness, she stressed the importance of collaborating internally across departments so that involved personnel know what protections are in the network and how reliable they are.

In the context of cloud services, Moore noted that customers inherit the security controls for the cloud infrastructure but still must secure their own resources and data flows in the cloud. David Batz, Edison Electric Institute, expressed concern that some utilities may feel forced to use cloud services, and Anjan Bose, Washington State University, asked how utilities could reconcile cloud services with their culture of owning physical systems. Moore answered that it is best for utilities to collaborate with cloud service providers and regulators to identify specific challenges, create implementation guidance, and revise existing standards to clarify how utilities can use cloud services.

Adamiak noted that utilities own and manage the communications infrastructure for the transmission side but that this is not necessarily true of the distribution networks, which more often use off-the-shelf broadband networks. Ditto pointed out that even where utilities use private networks, they still buy their communications equipment from vendors, which creates supply chain concerns and underscores the importance of careful vendor evaluation.

Policy and Regulatory Issues

Ditto noted that the Federal Communications Commission (FCC) governs commercial communications networks. However, although the electric system relies on the commercial telecommunications infrastructure, FCC policies do not differentiate between the reliability needs of electric system critical infrastructure and the commercial telecommunications sector. This can sometimes undercut the ability for grid operational networks to ensure reliability and resiliency, she said.

Cynthia Hsu, National Rural Electric Cooperative Association (NRECA), asked about cybersecurity and reliability requirements for the hybrid of public and private communications networks. Ditto responded

that the utilities that UTC represents seem to be trending toward deploying their own networks into distribution grids instead of depending on corporate carriers. Utilities do not always have that option, and some are forced to rely on commercial carriers, but better collaboration among critical infrastructure owners and operators, the government, and the commercial carriers could improve mutual understanding, she said.

System-Level Solutions

Sanders asked panelists to suggest system-level solutions to improve both the cyber infrastructure and the grid itself. Adamiak proposed increased use of air gapping and secure jump boxes, as well as continuing the adoption of multiprotocol label switching, which improves the ability to switch paths. Ditto suggested that perhaps the utilities' individual private networks be treated en masse as one large network that could share wireless networks within a designated spectrum band, allowing utilities to work together to protect the use of that designated band.

Roxey reiterated that electricity grid systems have become too complex to understand and defend. "We are getting close to the limits of defensibility mostly because we are at the limits of detectability," he said. "Things occur and we don't even know that they happened." He added that "the performance of today's cybersecurity solutions cannot be evaluated with any deterministic methods that definitively show they are working."

CULTURE CHANGE

- A culture of security will be vital to effectively countering threats to the U.S. electric grid. Security is not limited to protection and defense but also encompasses preparedness, response, and resilience.
- Standards and regulations provide an important foundation but are not sufficient to ensure grid security. Best practices are necessary to protect the most critical infrastructure.
- All parties benefit when the relationship between industry and government is collaborative rather than adversarial.

Cynthia Hsu, National Rural Electric Cooperative Association (NRECA), moderated a panel focused on creating an ingrained culture of cybersecurity within the electric utility workforce. She emphasized that it takes a combination of people, process, and technology to achieve such a culture and urged participants to focus not on elucidating the challenges but on integrating lessons learned to inform tangible action. The speakers

were Marc Child, Great River Energy; Joe McClelland, Federal Energy Regulatory Commission (FERC); and Scott Aaronson, Edison Electric Institute. Hsu moderated an open discussion following their remarks.

Marc Child, Great River Energy

Marc Child, information security program manager at Great River Energy and chair of NERC Critical Infrastructure Protection (CIP) Committee, shared perspectives on NERC's CIP regulatory standards, enacted after the 2003 blackout in the Northeast United States.

NERC's CIP standards have had both positive and negative impacts, Child said. A key downside is that the standards ushered in a culture of compliance in which utility personnel grew to fear auditors more than actual attackers. "We have to get past that," Child urged. Also, the standards led to a homogenization of security features across utilities, which undermines security overall. "We shouldn't all have the same type of fence or lock," Child explained. "Why should we have the same cyber defenses?"

On the positive side, the standards did succeed in elevating all utilities to a minimum level of security by establishing a baseline set of requirements, Child said. The phased rollout of requirements also made it feasible for utilities with different levels of resources and security needs to build their security protections up to the appropriate level over time. In addition, he credited NERC's CIP standards with opening a dialogue and a more collaborative relationship between utilities and vendors around cybersecurity.

Despite these valuable impacts, there are limits to what NERC standards can or should reach, Child said. He expressed his view that regulation for today's intelligent, distributed, digital network and new grid regimes such as distributed energy resources should reflect the ongoing innovation in that area, and drive meaningful change in security as opposed to a focus on compliance. While these developments have vastly expanded the attack surface for the grid overall, he suggested that these new vulnerabilities are beyond the scope of CIP and best addressed through collaborations among utilities, vendors, national laboratories, and research organizations, which he felt would yield results faster than waiting for NERC to update standards.

Building on this point, Child suggested several ways in which he thinks utilities and the grid overall would benefit from greater freedom from mandatory standards. He urged utilities to empower their engineers to invest in effective—not merely compliant—technologies such as software-defined networks and decoy networks, and to base their decisions on timely and actionable intelligence. He recognized the CIP

standards as a necessary minimum baseline but suggested that their scope should be capped and that utilities should be free to address new threats through means other than mandatory standards. In addition, to replace today's "gotcha" environment with a culture of cooperation based on a shared mission between utilities and auditors, he proposed eliminating financial penalties for CIP noncompliance and replacing them with binding recommendations for improvements.

Closing, Child pointed to a need for greater collaboration among research and trade groups around cybersecurity; enhanced partnerships with Canadian stakeholder organizations, such as by including them in classified Department of Energy (DOE) briefings; and the reduction of barriers for participating in the DOE Cyber Risk Information Sharing Program (CRISP). CRISP enables utilities and intelligence agencies to share real-time data about cyberattacks, but the program is relatively expensive and therefore typically implemented only at larger utilities.

Joe McClelland, Federal Energy Regulatory Commission

Joe McClelland, FERC director of the Office of Energy Infrastructure Security, discussed FERC's approach to utility security. Just as the electric power system comprises several interdependent infrastructures, FERC's purview intersects with the authority of several other government agencies. While their responsibilities vary—for example, FERC sets standards for hydroelectric facilities and the bulk power system while other agencies cover oil and natural gas facilities and security standards—McClelland said FERC works in partnership with these other agencies to identify threats, vulnerabilities, and mitigations.

Whether industry's motivation to ensure security stems from the threats themselves or from a motivation to comply with standards and regulations, McClelland stressed that the threats are real. He quoted from a 2017 Department of Defense (DoD) report¹ whose findings he described as "sobering":

Major powers (Russia and China) have a significant and growing ability to hold U.S. critical infrastructure at risk via cyber attack, and an increasing potential to also use cyber to thwart U.S. military responses to any such attacks. This emerging situation threatens to place the United States

¹ Defense Science Board Task Force on Cyber Deterrence, 2017, *Report for the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics*, U.S. Department of Defense, Washington, D.C., https://www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf, accessed February 20, 2020.

in an untenable strategic position. Although progress is being made to reduce the pervasive cyber vulnerabilities of U.S. critical infrastructure, the unfortunate reality is that for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructures.

He also quoted a 2019 statement,² referenced earlier by Stockton, in which Director of National Intelligence Daniel Coates asserted that China has the ability to disrupt U.S. natural gas pipelines through cyberattacks:

China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States.

The assessment also concludes that:

Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage.

In light of these and other threats, FERC recommends a dual approach to security comprising both baseline standards and best practices. McClelland described NERC's CIP standards as the base of a pyramid—foundational, solid, and broad. While these are valuable and should be considered virtually everywhere within a system, they are not sufficient alone: Adversaries can read the standards, too, and work to find ways around them. Best practices are the pinnacle of the pyramid and they should be used with foundational standards as necessary to stop nation-state adversaries, putting them in place in the most critical facilities.

McClelland said success will require that owners and operators of the nation's most critical facilities be able answer three questions: Are you fully informed of an adversary's capabilities? Do you know what best practices can stop them? Have you identified which critical facilities should be protected by these best practices? FERC's experts are focused on those questions and aim to help facility owners and operators improve

² D.R. Coates, 2019, *Worldwide Threat Assessment of the U.S. Intelligence Community. Statement for the Senate Select Committee on Intelligence*, <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR-SSCI.pdf>, accessed February 20, 2020.

their awareness and capabilities to put the right protections in the right places.

Scott Aaronson, Edison Electric Institute

Scott Aaronson, vice president of security and preparedness at the Edison Electric Institute, discussed the importance of moving toward a culture of security that encompasses both protection *and* preparedness. While it is important to secure our infrastructure, inevitably attacks will occur; the defender must be effective 100 percent of the time, but an adversary has to be effective only once in order to cause significant impacts. In this context, Aaronson stressed that it is crucial to be prepared to respond and recover from attacks in order to protect national security, the economy, and the life, health, and safety of utility customers.

Aaronson described security as a three-legged stool supported by standards that provide the necessary (though insufficient) foundation; partnerships across industry and government; and preparedness, which encompasses response, recovery, and resilience. While standards are valuable for ensuring reliability of operations under normal conditions, he stressed that preparedness is essential for true resilience when conditions become abnormal. “Reliability assumes blue skies,” Aaronson said. “Resilience is the ability to take a punch.”

Aaronson outlined strategies to increase preparedness by leveraging the grid’s inherent redundancy and resilience. These include mutual assistance capabilities, in which utilities contribute resources to respond when one fails; supplemental operating strategies that provide backup when normal operations are degraded; and inventorying spare assets that could be utilized after an attack.

When Iran struck down a U.S. drone in June 2019, the United States implemented what Aaronson considered an appropriate response: a cyberattack targeting military infrastructure. This response, in his view, demonstrated U.S. cyber capabilities to Iran and other adversaries like China, Russia, North Korea, and criminal networks while, importantly, stopping short of using those capabilities against civilian or critical infrastructure. However, he cautioned that our adversaries cannot be depended on to follow the same rules of war, underscoring the critical importance of staying prepared for an attack that does target critical civilian infrastructure.

Discussion

Participants discussed the role and appropriate scope of standards, along with what steps could be taken to create a culture of security.

The Role and Scope of Standards

Jeffery Dagle, PNNL, asked if standards compliance may be unintentionally inhibiting the adoption of new technology. He pointed to synchrophasors, which support situational awareness, as an example of a technology that has been deployed less widely than it otherwise might be due to utilities' fears of running afoul of auditors. Child argued that emerging technologies must be secured, and if utilities do not adopt new technology because they fear an audit, that auditor-utility relationship is the problem, not the standards. Aaronson agreed, and noted that the question underscores the broader point that security is not a binary feature wherein standards compliance is equated with complete security. Recognizing that standards evolve too slowly to keep up with fast-moving security threats, he suggested new technology could be covered by best practices instead. McClelland added that standards are open to public comment and can be updated if they present unnecessary impediments to improvement. He also cautioned that helpful tools can open new vulnerabilities: Even a single insecure node, however insubstantial, can be used by an adversary to gain entry to the larger system.

Cynthia Hsu, NRECA, asked whether there were lessons learned from how the NERC CIP standards have or have not worked that can inform conversations on extending it beyond its current base of covered entities. McClelland pointed out that the electricity subsector is very mature and capable, in part due to standards, but also because of long-standing exchange between government and industry. He suggested that conversation could be extended to other sectors, bearing in mind each sector's focus, maturity, and role in critical infrastructure.

Adamiak asked if FERC was creating standards specifically for EMP events. McClelland acknowledged that EMP was a major concern, and noted that FERC is working closely with other relevant agencies to create a coordinated industry-outreach effort that will likely be a best practice, and not a standard at this time. Aaronson stated that EMP was not ready for a standard, but noted that it is possible to better understand EMP impacts and prepare for the consequences.

Creating a Culture of Security

Cynthia Hsu, NRECA, and Morgan both asked what steps panelists recommend in order to create a culture of security against today's threat landscape. Child highlighted the value of collaborating on and sharing vulnerability assessments, lessons learned, and mitigation strategies. The specific threat is unimportant, he said; what matters is system resilience and consequence management.

McClelland emphasized the value of partnerships between government and industry. Bringing government expertise together with operational experience can help both parties to create security assessments, refine best practices, and understand adversarial activities. He highlighted FERC's one-on-one work with utilities to provide information, assess practices, and recommend mitigations. While attacks targeting a key facility may be very difficult to stop, a valuable way to counter these threats is to identify, prioritize, and protect military-critical and society-critical skeletal services.

Aaronson added that CEO leadership was very important to creating a culture of security, as CEOs set priorities and direct resources throughout an organization. Self-assessment tools can also help leaders determine where to direct energy and identify problem areas, such as supply chain security, that go beyond the organization itself.

TRANSLATIONAL R&D

- Government, academia, and the private sector generate innovations that are valuable for advancing grid security.
- Innovations are developed and deployed within the broader context of standards and regulation, which can either complement or, at times, impede, their adoption.
- Stakeholders can benefit from identifying opportunities to share information and optimize resource allocation in order to speed progress.

Anjan Bose, Washington State University, moderated a panel focused on how technology can quickly move from the lab into practice. The panelists were Kevin Stine, Information Technology Laboratory, National Institute of Standards and Technology (NIST); Yair Amir, Johns Hopkins University; and Carol Hawk, U.S. Department of Energy (DOE). An open discussion followed the speakers' remarks.

Kevin Stine, National Institute of Standards and Technology

Kevin Stine, leader of applied cybersecurity within the NIST Information Technology Laboratory, described how NIST helps organizations apply standards, guides, and practices in order to better understand and manage cybersecurity risks.

NIST is a nonregulatory agency, so its standards are voluntary and consensus-based, not mandatory. NIST experts conduct early-stage foundational research as well as facilitate its transition into active practice. While its activities span a broad range of areas, NIST's cybersecurity activities are aimed at advancing standards, technology, and measurement science to cultivate trust in information and systems.

One of its primary tools in this area, the NIST Cybersecurity Framework,³ provides organizations with a common language for cybersecurity activities and outcomes, enabling them to bridge communication gaps both within and between organizations, Stine said. The Framework has three key focuses: the alignment of an organization's business processes with its cybersecurity capabilities and technologies; recognition of interdependencies among organizations, sectors, and shared infrastructures; and the imperative to increase resilience, which is defined as post-attack response and recovery mechanisms that best position an organization to continue critical operations.

In addition to its cybersecurity expertise, NIST supports standards and tools for energy sector operations, including smart grid technologies. Energy cybersecurity, which lies at the intersection of those two areas, can be approached through two lenses, Stine said. The first focuses on the cybersecurity of organizations, guiding what utility owners and operators do to prioritize and implement cybersecurity activities. The second considers the cybersecurity of the grid architecture as a whole, with particular focus on the interfaces between different grid components.

To facilitate the application of standards and technologies to address today's cybersecurity needs, NIST's National Cybersecurity Center of Excellence⁴ provides blueprints, developed in collaboration with the broader electricity subsector community, that show how utilities can implement the latest tools. For example, the center offers insights on tools and technologies that maintain appropriate identity verification and access management when transitioning between IT and operational technology (OT) infrastructures. It also offers guidance on architectures to support situational awareness, asset management, and security for connected grid technology within the "industrial Internet of Things."

Yair Amir, Johns Hopkins University

Yair Amir, professor of computer science at Johns Hopkins University, discussed how system-level changes can improve utilities' security and resiliency. He described Spire, an open-source, intrusion-tolerant SCADA operations system that Amir's research group created, as an example of this type of change.

³ For more information on the NIST Cybersecurity Framework, see NIST, "Cybersecurity Framework," <https://www.nist.gov/cyberframework>, accessed February 20, 2020.

⁴ For more information on the NIST National Cybersecurity Center of Excellence, see NIST, "National Cybersecurity Center of Excellence," <https://www.nccoe.nist.gov/>, accessed February 20, 2020.

The Defense Advanced Research Projects Agency (DARPA) provided seed funding for transitioning intrusion-tolerant capabilities employing resilient clouds to the power grid. In a follow-up 2017 DoD project, experts from Sandia National Laboratories posing as adversaries were able to penetrate and damage a best-practices-compliant commercial test grid within hours, but a Spire-protected test grid withstood their attempts for 3 days. The next year, Spire performed similarly well in a test conducted at an operating electric utility.

Since then, several utilities have expressed interest in adopting Spire, but Amir noted that structural barriers, including financial and legal barriers, limit how quickly (or if at all) new innovations are accepted and deployed. At a basic level, Amir noted that even the question of who is ultimately responsible for dealing with attacks from a nation-state actor—the utility or the government—remains, to some extent, unanswered.

Carol Hawk, U.S. Department of Energy

Carol Hawk is a program manager within the Cybersecurity for Energy Delivery Systems (CEDS) division of the DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER). Recognizing that standards and regulations move at a slower pace than both the threat landscape and technological innovations, Hawk posited that these different time scales are complementary, not conflicting. She said that while standards and regulation provide a baseline but not an anchor, innovations enable the field to move from a reactive to a resilient posture.

As the industry works to increase the capacities, reliability, and efficiency of energy delivery systems, Hawk stressed that innovation remains critical to addressing emerging threats. She described how the 2011 standards-based *Roadmap to Achieve Energy Delivery Systems Cybersecurity*⁵ helped inspire new technologies to help utilities withstand a cyber incident. She emphasized the importance of grounding innovations in utilities' control, operational, and energy delivery systems in order to enable attack recognition and "self-healing" capabilities whereby a utility can sustain critical functions even if compromised. "It is essential that innovation takes into consideration and uses the operational characteristics of that system," Hawk said, describing the ideal system as being able to recognize an attack and then adapt the way it is operating in order to continue delivering energy while the attack is being contained and eradicated.

⁵ Energy Sector Control Systems Working Group, 2011, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, U.S. Department of Energy, Washington, D.C.

Hawk noted that some attacks can be sufficiently defended by standards that regulate good cyber hygiene, such as efforts to reduce the attack surface. However, as threats evolve rapidly, an ecosystem of continued innovation—comprising experts from suppliers, utilities, academia, and the government—is also necessary, she said.

Discussion

Participants and panelists discussed product security and regulation, how security can be better incorporated into educational and training programs, and opportunities to speed progress through information sharing.

Product Security and Regulation

Noting the perennial tension between building a product fast and building a product that is secure, Michael Howard, EPRI, asked if there should be mechanisms to hold liable vendors that sell insecure products. Stine suggested that incentives, rather than regulation, might be the best way to encourage companies to prioritize product security over speed, although the success of such incentives also depends on customers recognizing the importance of security. Establishing a repository for trusted code, complementary to the National Vulnerability Database that inventories known software vulnerabilities, could also help, he added. Hawk noted that DOE's research into secure development life cycles for operational technology systems could also play a role. Amir pointed out that regulation in this area could have the unintended consequence of undermining the use of open source code to help secure the power grid, which could be detrimental.

Morgan noted that product security is an even bigger problem in the IoT space, where installed devices are never patched, leading to persistent vulnerabilities. Stine added that NIST recently closed a public comment period that addresses the IoT-cybersecurity intersection and will soon issue baseline recommendations. Morgan pointed out, and others agreed, that efforts in this area are undermined by a lack of clarity with regard to which agency has regulatory control over IoT devices.

Bose added that electric power systems are comprised of many layers of equipment, with devices constantly being added at the grid edge, and that each additional layer increases the attack surface. Hawk agreed that grid-edge IoT activity requires close attention and noted that DOE is actively working to address needs at the grid edge through generation, transmission, and distribution, including in the IoT realm, but reiterated that DOE is not a regulatory agency and that she could not comment on the potential for standards and regulations in this area.

Adamiak noted that Russia recently announced that it was able to sever its connections to the global Internet as a mechanism to prevent remote access to its assets, and asked if the United States was considering a similar capability. Gavin Donohue, Independent Power Producers of New York, Inc., replied that the Internet, the U.S. economy, and the global economy are too entwined for the United States to pursue such a model. He also expressed skepticism regarding Russia's claim and the effectiveness of such an approach.

Bringing Security into Education and Training

An attendee from Oak Ridge National Laboratory raised the need to better incorporate security awareness and expertise into relevant educational programs. Amir agreed, and noted that the computer science field does not consistently teach basic security skills. Participants discussed how requiring security courses as part of degree programs in computer science and electrical engineering programs could improve security for electric utilities and their cyber infrastructure. Hawk suggested taking a cross-disciplinary approach combining power systems engineering with cybersecurity.

Information Sharing to Accelerate Progress

Dagle brought up the imbalance in the time scales on which defenders and attackers operate. He pointed out that there is a necessary lag between identifying vulnerabilities and deploying patches to address them: Defenders must test their solutions sufficiently to ensure that patches do not create new vulnerabilities. A related issue is the degree to which different stakeholders on the defender's side are permitted access to information about known vulnerabilities. The desire to keep such information from falling into an adversary's hands is understandable, he said, but it nonetheless creates a barrier that slows the defender's ability to solve the problem. Attackers, on the other hand, can freely share information among themselves and innovate quickly. Would it be possible, he asked, for defensive systems to work at a similar speed?

Amir answered that moving from enterprise to cloud-based solutions could help to address this on the industry side. Cloud services support rapid deployment of innovations and benefit from a concentration of talent that better positions them to keep pace with the threat landscape, he said. Alternatively, another approach would be essentially the opposite, to completely separate everything so that one attack cannot take out the whole grid. While possible, Amir suggested that this approach is likely to be more expensive. Stine added that collaboration across the diverse and complex electric power community is important and suggested that increased automation could also help close the time scale gap.

Appendixes

A

Statement of Task

In its 2018 appropriations for the Department of Energy, the U.S. Congress directed the National Academies of Sciences, Engineering, and Medicine to appoint an ad hoc committee of experts to “conduct an evaluation of the expected medium- and long-term evolution of the grid. This evaluation shall focus on developments that include the emergence of new technologies, planning and operating techniques, grid architecture, and business models.”

In developing its report, the committee will consider: (1) trends in generation resources, their operational characteristics, and what capabilities will be required in energy infrastructure to provide reliable and resilient service; (2) trends in end use, including technologies for intelligent load control, and their implications for grid modernization investments; and (3) interdependencies with other infrastructure systems such as natural gas, telecommunications, and transportation systems. The committee will be informed by a broad suite of alternative scenarios for the medium- and long-term evolution of the grid, and will identify potential “no-regret” strategic federal investments and approaches that will help create a platform for a reliable, resilient, and secure power system, including cyber security. In its discussions, the committee will consider the evolution of external forces that influence grid investment, planning, and operations.

The committee will gather evidence, deliberate, and provide findings and recommendations across the following broad categories.

- *Technologies*—Identify opportunities to improve existing technologies or develop and apply emerging technologies in generation, storage, power electronics, sensing and measurement devices, control systems, cyber security, and loads.
- *Planning and Operations*—Investigate how current planning and operational practices may need to evolve in the future given the breadth of potential scenarios for changes in generation, grid technologies, and end use.
- *Business Models*—Consider broadly the cost and benefits of modernizing the power system relative to current business and operating procedures and explore how oversight and market operations may need to change with new technologies and customer arrangements.
- *Grid Architectures*—Evaluate both technical and jurisdictional challenges to implement a broadly applicable approach to grid architectures.

B

Workshop Agenda

COMMUNICATIONS, CYBER RESILIENCE, AND THE FUTURE OF THE U.S. ELECTRIC POWER SYSTEM

November 1, 2019
Keck Center of the National Academies
Washington, D.C.

Computing, communications, and information technologies have become essential in the planning and operation of the nation's electricity system, a trend that is expected to increase in the future. How can we take advantage of new technologies while mitigating cyber security and resilience risks? This meeting will synthesize current efforts to increase the cyber resilience of the electric power system. We will explore fundamental tensions that underlie different computing and communication technologies and strategies—for example, between simple and complex technologies and systems and between compliance versus security cultures. Join the National Academies' Committee on the Future of Electric Power in the United States for a discussion of these tensions and how they could shape electric power systems over the next 30 years.

8:45 a.m. ***Welcome and thanks from the committee***

Granger Morgan,* Carnegie Mellon University

8:50 ***Setting the Stage—The Past and the Future of Computing in the Grid***

William Sanders,* Carnegie Mellon University

9:10 ***Panel 1a—Electric System Cyber Security: Perspectives on Current Status and Future Concerns***

Moderator: Bill Sanders,* Discovery Partners Institute

- Brian Harrell, Cybersecurity and Infrastructure Agency (CISA), Department of Homeland Security (DHS)
- Michael Hyland, American Public Power Association (APPA)
- Robert M. Lee, Dragos

10:10 ***Panel 1b—EMP and GMD: Perspectives on Current Status and Future Concerns***

Moderator: Michael Howard,* Electric Power Research Institute (EPRI)

- John Kappenman, Storm Analysis Consultants
- Mark Lauby, North American Electric Reliability Corporation (NERC)
- Randy Horton, Electric Power Research Institute

11:10 Break

11:25 ***Panel 2—Where and How Should Digital Technologies Be Used to Improve Security and Resiliency?***

Moderator: Jeffery Dagle,* Pacific Northwest National Laboratory (PNNL)

- Joy Ditto, Utilities Technologies Council (UTC)
- Mark Adamiak, Adamiak Consulting and Former General Electric (GE)
- Samara Moore, Amazon Web Services
- Tim Roxey, Former Electricity Information Sharing and Analysis Center (E-ISAC)

12:35 p.m. Lunch

1:15 ***Panel 3—Strategies for Moving from a Culture of Compliance to a Culture of Security***

Moderator: Cynthia Hsu,* National Rural Electric Cooperative Association (NRECA)

- Marc Child, Great River Energy
- Joe McClelland, Federal Energy Regulatory Commission (FERC)
- Scott Aaronson, Edison Electric Institute

2:15 ***Panel 4—How to Reconcile the Time Scales of Innovation with Standards and Regulation?***

Moderator: Anjan Bose,* Washington State University

- Kevin Stine, Information Technology Laboratory, National Institute of Standards and Technology (NIST)
- Yair Amir, Johns Hopkins University
- Carol Hawk, Cybersecurity for Energy Delivery Systems, Department of Energy (DOE)

3:15 Break

3:30 ***Panel 5—Boundaries and Interactions Between Utilities and National Security Efforts***

Moderator: Granger Morgan,* Carnegie Mellon University

- Caitlin Durkovich, Toffler Associates
- Paul Stockton, Sonecon, LLC
- David Batz, Edison Electric Institute

4:45 ***Workshop Adjourns***

* Denotes member of National Academies Committee on the Future of Electric Power in the U.S.

C

Registered Workshop Participants

Luqman Abdullah—U.S. Government Accountability Office
Prasanna Abeysekera—Vocus Group Limited
Janet Addoh
Ebenezer Adewunmi
Ahmad Shabir Ahmadyar—Jacobs Engineering
Micheal Akibaleye
Vincent Alcazar—U.S. Military
Richard Alexander—Trinidad and Tobago Defense Force
Marcelo Almeida—Brazilian Energy Research Office
James Alves-Foss—University of Idaho
Patrick Amon—École Polytechnique Fédérale de Lausanne
Juanita Andrade
William Angel
David Anspach
Kathy Araujo—Energy Policy Institute
Jeffrey Arnold Sr.—U.S. Navy
Henry Artigues—Florida International University
Sharla Artz—Utilities Technology Council
Linquan Bai—University North Carolina, Charlotte
George Baker—National Security Council
Chuck Banks—Chucks Banks Associates
David Bardin
Fred Barrantes—LG&E and KU Energy, LLC
Matthew Bateman

Michael Bear
 Tamara Becejac—Pacific Northwest National Laboratory
 Kevin Berent—Electric Power Research Institute
 Konstantin Berestizshevsky—Tel Aviv University
 Mitchell Berge
 Pankaj Bhowmik—Oak Ridge National Laboratory
 Klara Bilgin—Cybernow Labs
 George Bivens—Aggreko
 Edward Blum—Blum and Co., Inc.
 Rui Bo—Missouri University of Science and Technology
 Gaylord Booto
 Cynthia Bothwell—U.S. Department of Energy, Office of Energy and
 Renewable Energy
 Dayne Broderson—University of Alaska, Fairbanks
 William Bruner—Gadgettronix
 Nicole Buell—U.S. Senate Energy and Natural Resource Committee
 Richard Campbell—Library of Congress
 Sharon Cardash—Auburn University
 Amy Casuscelli—Xcel Energy
 Rachael Chambers
 Abhijit Chandra—Iowa State University
 Mohammad Chowdhury—Port Authority Trans-Hudson
 Mark Christian—Argonne National Laboratory
 Howard Christiansen—Montana State University, Bozeman
 Paul Ciampoli
 Maureen Clapper—U.S. Department of Energy
 Mason Clark—Ice Miller, LLP
 Kathyne Cleary
 Derrick Cogburn—American University
 George Cotter
 Bree Cox
 Noel Crisostomo—California Energy Commission
 Tanya Das—U.S. House of Representatives Science, Space, and
 Technology Committee
 Roop Dave
 Andrew Dawe—Embassy of Canada
 Payman Dehghanian—George Washington University
 Mercy DeMenno
 Rob Denaburg—Sonecon, LLC
 Sahar Derakhshan—University of South Carolina
 Michael Ditmore—The Novim Group
 Ganesh Doluweera—Canadian Energy Research Institute
 Thomas Donahue—High Point Cyber, LLC

Bharat Doshi—Office of Naval Research
 Jessica Eadie
 Carly Eckstrom—U.S. Senate Energy and Natural Resources Committee
 Matthew Eggers—U.S. Chamber of Commerce
 Matt Ekram—Infinite Convergence
 Sai Mounika Errapotu—University of Texas, El Paso
 Alexander Evers—Office of Senator Lisa Murkowski
 Donald Faatz—National Cybersecurity Center of Excellence
 Xiaoyuan Fan—Pacific Northwest National Laboratory
 Teresa Feo—California Council on Science and Technology
 Mark Ference—Innovation Emergency Management
 Ron Fisher—Idaho National Laboratory
 Kris Flaig—Bureau of Sanitation City of Los Angeles
 Jennifer Flandermeyer—Evergy
 William Flink—International Association of Directors of Law
 Enforcement Standards and Training
 Alex Flueck—Illinois Institute of Technology
 David Frelinger—RAND Corporation
 John Frink
 Russell Frisby—Stinson, LLP
 Alex Fu—Federal Aviation Administration
 Peter Fuhr—Oak Ridge National Laboratory
 Genevieve Gadwali—The MITRE Corporation
 Wang Gan
 Mehdi Ganjkhani—University of Utah
 Maëva Ghonda—University of Maryland
 Daniel Giamo—U.S. Office of Management and Budget
 Mostafa Gilanifar—University of Utah
 Changdeok Gim—University of California, Irvine
 Chen Gingqing
 Jairo Giraldo—University of Utah
 Cliff Glantz—Pacific Northwest National Laboratory
 Tassos Golnas—U.S. Department of Energy
 Daniel Gonzales—RAND Corporation
 Idelfonso Arturo Gonzáles Domador—IntecoPeru
 Avi Gopstein—National Institute of Standards and Technology
 Lori Gordon—Aerospace Corporation
 Mark Gray—Edison Electric Institute
 Thushara Gunda—Sandia National Laboratories
 Charles Hakkarinen
 Bryan Hannegan—Holy Cross Energy
 William Harris—Foundation for Resilient Societies
 Rich Heidorn—RTO Insider

Nelson Alejandro Herrera Gómez—Universidade Federal de Itajubá
 Robert Hershey—Robert L. Hershey, P.E.
 Aimee Higby—Washington Utilities and Transportation Commission
 Lee Hinga—U.S. Government Accountability Office
 Fred Hintermister—Global Resilience Federation
 Jason Hissam—U.S. Department of Energy
 John Howes—Redland Energy Group
 Daisy Huang—University of Alaska at Fairbanks
 David Hunter—Electric Power Research Institute
 Abidemi Ilori—University of Uyo
 Hiroyuki Iseki—University of Maryland, College Park
 Roshni Anna Jacob—University of Texas, Dallas
 Kat Janowicz—3COTECH, Inc.
 Joseph Januszewski—Electricity Information Sharing and Analysis
 Center
 Anne Johnson—Creative Science Writing
 Chip Justice
 Wayne Kangas
 John Kappenman—Storm Analysis Consultants
 Bandana Kar—Oak Ridge National Laboratory
 Arthur Katz—American University
 Tanu Kaushik
 Len Kennedy—Kennedy Associates
 Malik Khalil
 Mohammed Masum Siraj Khan—University of Utah
 Kush Khanna—Iowa State University
 Hannah Kim—U.S. Government Accountability Office
 Heath Knakmuhs—U.S. Chamber of Commerce
 Charalambos Konstantinou
 Mert Korkali—Lawrence Livermore National Laboratory
 Aria Kovalovich—U.S. House of Representatives Committee on Science,
 Space, and Technology
 Frank Koza—EIS Council
 Prashant Kr—Seer, Inc.
 Bheshaj Krishnappa—ReliabilityFirst
 Abhijit Kshirsagar—University of Minnesota
 Andreas Kuehn—EastWest Institute
 Wang Kun
 Alberto Lamadrid—Lehigh University
 Mary Lancaster
 Michael Larsen—Boeing
 Marcia Levetown
 Binghui Li

Sylvia Li
 Brie Lindsey—California Council on Science and Technology
 Mingxi Liu—University of Utah
 Shelly Liu—Florida State University
 John Lundgren—Breachbits
 Kenneth Lutz—University of Delaware
 Julia Ma—Catholic University of America
 Sajedah Mahomed—Eskom Holdings SOC, Ltd
 Majid Majidi—University of Utah
 Marc Mangel—University of California
 Gabriela Manrique—University of Montreal
 Christopher Mansour—Mercyhurst University
 Jacinto Marques—Webster University
 Julius Matusewicz—Butler Weihmuller Katz Craig, LLP
 Richard Matzner—University of Texas, Austin
 Jessee McBroom—H2Phusion
 Laura McWilliams—California Senate
 Karan Mehta—Karna Solutions
 Karishma Mehta
 Stephen Mensah—Stantec
 Javier Meza—IID
 Matt Michael
 Dion Mikkelsen—Powerlink Queensland
 Laurie Miller—Pacific Northwest National Laboratory
 Lynette Millett
 David Millman
 Andrew Moore—U.S. Government Accountability Office
 Margaret Morganti—Oak Ridge National Laboratory
 Shaina Mosley—Meemee’s House
 Vilas Mujumdar
 Prashanth Mundkur
 Thomas Murray—Acute Management Strategies, LLC
 Wade Narin van Court—TRC Companies
 Morteza Nazari—Pennsylvania State University
 Ricardo Neeb—PUC
 Cameron Nelson—U.S. Senate Energy and Natural Resources Committee
 Nenad Nenadic—Rochester Institute of Technology
 E. Nigenda
 Ginger Norris—National Infrastructure Advisory Council
 Paul Ntim—COCO BOD
 Joe Nunes—U.S. Bureau of Labor Statistics
 Colin Ogilvie
 Miho Ohsawa

Terry Oliver—TVOGlobal, LLC
 Gaby Ou—University of Utah
 Seemita Pal—Pacific Northwest National Laboratory
 Silvia Palma Rojas
 Alejandro Palomino—University of Utah
 Amritanshu Pandey—Pearl Street Technologies
 Ruth Pannill—Southern States Energy Board
 David Paoella
 Bryan Parker—International Healthcare Access Group
 Edward Parker—RAND Corporation
 Samir Patel
 Victor Pearson—U.S. Department of Energy
 Malaquias Pena—Eversource Energy Center
 Ninoshka Perez—Western Governors University
 James Plewniak—Georgetown University
 Marta Poncela—European Commission Joint Research Centre
 Kiel Pratt—California Energy Commission
 Hannah Rabinowitz—U.S. Department of Energy
 Yvette Rachelle
 Jubeyar Rahman—University of Texas, Dallas
 Steve Rawson—Idaho National Laboratory
 Jean Raymond—Hydro-Quebec
 Lavanya Reddy—Kogod School of Business
 Malcolm Reid—Brison, LLC
 Daniel Retter—Yona Systems Group
 Theodore Robin, Jr.
 Dorothy Robyn—Boston University
 Emilie Roth—Roth Cognitive Engineering
 Melio Saenz—Clacsii
 Mostafa Sahraei Ardakani—University of Utah
 George Samaras—Samaras & Associates, Inc.
 Umit Sami—Memcus, Inc.
 Char Sample—Idaho National Laboratory
 John Sanders—I3S
 Yuanrui Sang—University of Texas, El Paso
 Alan Sanstad—Lawrence Berkeley National Laboratory
 Joseph Santoro—Acceleprise
 Ashwini Sathnur—United Nations Development Programme
 Ali Sayghe—Florida State University
 Fred Schneider—Cornell University
 Michael Schulsinger—Clark County Emergency Management Agency
 Stephen Self—SP Global
 Julia Selker

Abdollah Shafieezadeh—Ohio State University
 Syed Faisal Shah—U.S.-Pakistan Center for Advanced Studies in Energy
 Surja Sharma—University of Maryland
 Zhiwen Sheng—Huazhong University of Science and Technology
 David Shum—DkS Engineering Consulting
 Simone Simone
 Rebecca E. Skinner—San Francisco AQ
 Molly Slocum—Nehemiah Security
 Michael Smith—Acacia Security, LLC
 Karen Snider
 Bruce Snyder
 Adefunke Sonaïke—Robust Analytics Lab
 Rohini Srivastava—American Council for an Energy Efficient Economy
 Parker Stanley—IEM
 Steven Strasburg
 Richard Stuebi—Future Energy Advisors
 Charles Sun—U.S. Department of Homeland Security
 Philip Sussler
 Sam Tedesco—Trident Global Technologies
 Rita Tehan—Congressional Research Service, Library of Congress
 Mehari Teklay—RMH
 Audra Thomas
 Lionel Toba—Idaho National Laboratory
 Anh Tran—Sandia National Laboratories
 Douglas Tucker—U.S. Air Force
 David Turner—National Oceanic and Atmospheric Administration
 Hiroyuki Uehara—Johns Hopkins University
 Nik Urlaub—The MITRE Corporation
 Kristin Van Abel—RAND Corporation
 Debbie van Opstal—U.S. Resilience Project
 Eusebio Vargas—Pontificia Universidad Catolica de Valparaiso
 Padmaja Vedula—RAND Corporation
 Nathan Vincent—Irvington Public Schools
 Samuel Visner—The MITRE Corporation
 Ann Vroom—Vroom Consults
 Jack Wang
 Jingyu Wang—Virginia Tech
 Ross Wang—Oak Ridge National Laboratory
 Ziyu Wang—Huazhong University of Science and Technology
 Jean-Paul Watson—Sandia National Laboratories
 Douglas Webb—Evergy
 Keith Weber—Idaho State University
 Ajith Weerasinghe—California State University, Fresno

Scott Weidman—National Academies of Sciences, Engineering, and
Medicine

Jack Werner—Climate Institute

Thomas Wilkinson—U.S. Department of Homeland Security

Jay Wilson

Denise Wojcik—Exelon

David Wollman—National Institute of Standards and Technology

Anier Landon Woodyard—Innovation Et Cetera Corp./Tao Institute for
Actualization

Bunli Yang—E4

Daniel Yang—Bureau of Land Statistics

John Yankeelov—U.S. Department of Energy

Eugene Yeh

Ayla Yilmaz

Guohui Yuan—U.S. Department of Energy

Meng Yue—Brookhaven National Laboratory

Vahraz Zamani—GridBright

Connie Zaremsky—U.S. Department of Energy

Junpeng Zhan—Brookhaven National Laboratory

Jie Zhang—University of Texas, Dallas

Junbo Zhao—Mississippi State University

Hui Zheng

Zhangxin Zhou—Texas A&M University

Ioannis Zografopoulos—Florida State University

D

Acronyms

AI	artificial intelligence
APPA	American Public Power Association
CEDS	Cybersecurity for Energy Delivery Systems
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Agency
CME	coronal mass ejection
CRISP	Cyber Risk Information Sharing Program
DARPA	Defense Advanced Research Projects Agency
DBT	design basis threat
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DPCD	digital protective control device
E-ISAC	Electricity Information Sharing and Analysis Center
EMP	electromagnetic pulse
EPRI	Electric Power Research Institute
FCC	Federal Communications Commission
FERC	Federal Energy Regulatory Commission

GIC	geomagnetically induced current
GMD	geomagnetic disturbance
HEMP	high-altitude electromagnetic pulse
ICS	Industrial Control System
IoT	Internet of Things
ISER	Infrastructure Security and Energy Restoration
IT	information technology
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRECA	National Rural Electric Cooperative Association
OT	operational technology
PNNL	Pacific Northwest National Laboratory
PPP	public-private partnership
R&D	research and development
SCADA	supervisory control and data acquisition
STEP	Spare Transformer Equipment Program
UTC	Utilities Technologies Council