



U.S. Department of Energy
Electricity Advisory Committee Meeting
National Rural Electric Cooperative Association Conference Center
Arlington, VA
March 14, 2019

Meeting Summary

PARTICIPANTS

Electricity Advisory Committee (EAC) Members:

JOHN ADAMS

Electric Reliability Council of Texas

CHRISTOPHER AYERS

North Carolina Utilities Commission Public Staff

TOM BIALEK

San Diego Gas & Electric Company

LANEY BROWN

Avangrid, Inc.

PAUL CICIO

Industrial Energy Consumers of America

ROBERT CUMMINGS

North American Electric Reliability Corporation

KIMBERLY DENBOW

American Gas Association

ANDREW (DREW) FELLON

Trane Energy Supply Services

FLORA FLYGT

American Transmission Company (Ret.)

SHERI GIVENS

National Grid

LISA GROW

Idaho Power Company

MICHAEL HEYECK

The Grid Group, LLC

PAUL HUDSON

General Infrastructure, LLC

LOLA INFANTE

Edison Electric Institute

MLADEN KEZUNOVIC
Texas A&M

CLAY KOPLIN
Cordova Electric Cooperative

ARTHUR KRESSNER
Grid Connections, LLC

CHARLOTTE LANE
West Virginia House of Delegates (former)

SHAUN MANN
Tri-State Generation and Transmission

JEFF MORRIS
Washington State House of Representatives

RICHARD S. MROZ
Resolute Strategies, LLC

BRYAN OLNICK
Florida Power and Light

DARLENE PHILLIPS
PJM Interconnection, LLC

ANDA RAY
Electric Power Research Institute

WANDA REDER
Grid-X Partners, LLC

RAMTEEN SIOSHANSI
The Ohio State University

TOM WEAVER
American Electric Power

Department of Energy:

HONORABLE KAREN S. EVANS
Department of Energy

RAKESH BATRA
Department of Energy

MAUREEN CLAPPER
Department of Energy

MICHELLE HINDMARCH
Department of Energy

ERIC HSIEH
Department of Energy

KATIE JEREZA
Department of Energy

CHRIS LAWRENCE
Department of Energy

KEVIN LYNN
Department of Energy

LAWRENCE MANSUETI
Department of Energy

DAVID MEYER
Department of Energy

JOE PALADINO
Department of Energy

MICHAEL PESIN
Department of Energy

JULIE SMITH
Department of Energy

Speakers, Guests and Members of the Public:

SCOTT AARONSON
Edison Electric Institute

MOHAMMED ALFAYYONMI
Dominion Energy

MARIANN BARSH
InsideCyber

NICHOLAS CANTRELL
XONA

SAM CHANOSKI
North American Electric Reliability Corporation

LYNN COSTANTINI
National Association of Regulatory Utility Commissioners

CHIP COTTON
General Electric

JOHN DONLEAVY
Uitelligent

DOUG DORR
Electric Power Research Institute

RICHARD FIORAVANTI
Quanta Technology

CHRIS HARVEY
MITRE

CYNTHIA HSU
NRECA

DAVID HUNTER
Electric Power Research Institute

CARL IMHOFF
Pacific Northwest National Lab

MARK JOHNSON
Utility Analytics Institute

STEVE KEREKES
Protect Our Power

MARK KNIGHT
Burns & McDonnell

ROBERT LEE
Dragos

JOSEPH MCCLELLAND
Federal Energy Regulatory Commission

JAMES REILLY
Reilly Associates

MARK ROCKWELL
Federal Computer Week

SAM ROZENBERG
APPA

MOUR SHAIKEH
NRECA

SONNY SIHM
Dragos

BLAKE SOBCZAK
E&E News

ROB THORMEYER
UTC

ANGELA TROY
ICF

ESTHER WHIELDON
S&P Global

SHELLY WINGES
Western Area Power Administration

ICF/Support:

PRATISTHA BHANDARI
ICF

CAT HUMPHRIES
ICF

PAUL MCKAY
ICF

JOSHUA S. SMITH
ICF

* * * * *

Presentation: Energy Sector Cybersecurity Activities in Federal Government

Michael Heyeck introduced Joseph McClelland from the Federal Energy Regulatory Commission (FERC). Mr. McClelland was appointed the first Director of the Office of Energy Infrastructure Security (OEIS) in September 2012. OEIS is the FERC office that provides leadership, expertise, and assistance to the Commission to identify, communicate, and seek comprehensive solutions to potential risks to FERC-jurisdictional facilities from cyberattacks and such physical threats as electromagnetic pulses.

Before beginning his remarks, Mr. McClelland stated a disclaimer that the views he expresses are his own and do not necessarily reflect the opinion of the Chairman, any commissioners, or the FERC staff. He said that OEIS is FERC's newest office. FERC has varying degrees of authorities over several different types of energy infrastructure. There is interstate transmission, which includes the subset of bulk power systems, oil and natural gas pipelines, liquefied natural gas (LNG) facilities, and hydroelectric. He noted that these authorities stem from the Federal Power Act, the Natural Gas Act, and the Interstate Commerce Act. In order to properly address the cyber threats, FERC has had to rearrange its organization. In terms of electricity, the commission has considered the prudence of any utility cost and rate proceeding, which includes prudence for security investments. He said that this can act to remedy an instance of insufficient interstate service upon complaint by a state regulatory commission. Moreover, it can direct the development of mandatory requirements of the bulk power system that would be the NERC standards, which include reliability and security. He stressed that considering the speed, sophistication, and targeting of cyber and physical attacks on energy infrastructure, the Commission is determined that these threats require special treatment. For the security to be effective, the authority of the Commission should be exercised in conjunction with the states, other agencies such as the Department of Energy (DOE), and with the protective actions of owners and operators of the infrastructure as well as the industry stakeholders. This is especially true when considering the increase in frequency and intensity of these events.

Mr. McClelland read a few excerpts to highlight the importance of being prepared in event of cyberattack. He quoted from the Task Force on Cyber Deterrence, a report from February 2017 by the Department of Defense: "First, major powers (e.g., Russia and China) have a significant and growing ability to hold U.S. critical infrastructure at risk via cyberattack 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 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 quoted a few excerpts from the Worldwide Threat Assessment of the U.S. Intelligence Community, issued in January 2019:

- "China has the ability to launch cyberattacks 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."
- "Russia has the ability to execute cyberattacks 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.”

- “Iran has been preparing for cyberattacks against the United States and our allies. It is capable of causing localized, temporary disruptive effects—such as disrupting a large company’s corporate networks for days to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks.”
- “North Korea poses a significant cyber threat to financial institutions, remains a cyber espionage threat, and retains the ability to conduct disruptive cyberattacks.”

Mr. McClelland said that the Commission uses a dual-fold approach. This means that the Commission employs both mandatory standards and established foundational practices and works collaboratively with industry, states, and federal agencies, such as DOE and the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to identify and promote best practices to address advanced threats. He said that all of the Commission’s efforts on the federal side come down to three questions:

- How aware and informed are the utilities about the specific adversaries and campaigns that they are facing? What tools can be used to defend against these adversaries?
- What practices should be put into place to protect against these threats?
- Have the utilities identified facilities that should be considered for best practices versus foundational practices?

Mr. McClelland said that the Commission modified the Critical Infrastructure Protection (CIP) standards to increase reporting capability. The reporting goes to the Department of Homeland Security (DHS) and the North American Electric Reliability Corporation (NERC) Information Sharing and Analysis Center (ISAC). The copy of the report is distributed on an annual basis. In addition, the Commission modified the NERC CIP standards to address supply chain risks. This standard is valuable as it establishes the foundational practices that everyone in the electric sector should be aware that an issue exists and have a process in place to evaluate it.

Mr. McClelland said that OEIS uses a cyclical approach. First, OEIS identifies the adversaries and their techniques, and looks at best practices that can be used against these adversaries. Second, OEIS informs state officials, state commissioners, and utilities through threat briefings so that the entities being targeted understand their threats. Last, OEIS sends representatives to the utilities for about two or three days to assess the cybersecurity vulnerabilities and help mitigate the threats. He said that OEIS has subject matter experts that assist program offices at FERC but do not bring back any of the information that is gathered in the voluntary reviews.

Mr. McClelland said that the Commission has facilitated numerous briefings, both open and classified, in the electric sector as well as the gas sector. In addition, dozens of cyber and physical security reviews have been conducted and the Commission has compiled the best practices gathered from these reviews. Furthermore, the Commission participates in the planning and execution of tabletop exercises for cyber and physical attacks. Mr. McClelland used Cyber Yankee as an example. Cyber Yankee pulls the states’ National Guard expertise and sets up a red team-blue team exercise. The goal of this exercise is to better facilitate cooperation between the National Guard and the utilities in the event of a cyber or physical attack. He encouraged the Electricity Advisory Committee (EAC) to look into Cyber Yankee because it is an innovative

way for the states to use federal expertise. He added that the Commission has developed resource materials for states and industry to help evaluate their cyber and physical programs. There is a cyber checklist, which is completely unclassified. The Commission has been working with states to come up with recovery plans as well. He said that it is important to have cyber contractors in case of a cyberattack. In addition, the Commission has collaborated with private sector efforts to broadly disseminate threat information and best practices. The Commission is looking for products and services to provide that would be useful in event of a cyberattack. He said that they have partners in the private sector and will start writing papers on topics such as cloud security. He said the Commission assists with security clearances as well.

Before wrapping up his presentation, Mr. McClelland mentioned the technical conference taking place on March 28, 2019. FERC and DOE are the co-hosts of this conference on Security Investments for Energy Infrastructure, which will focus on security practices to protect energy infrastructure. He said he will be available to answer any questions during the panel.

Mr. Heyeck introduced Assistant Secretary Karen Evans of the Office of Cybersecurity, Energy Security, and Emergency Response (CESER). Assistant Secretary Evans was sworn in on September 4, 2018. Before leading the Department's cybersecurity efforts, Assistant Secretary Evans served in the public sector as a top IT official at the Office of Management and Budget during the George W. Bush administration in the position that is now known as the Federal Chief Information Officer. Mr. Heyeck thanked Assistant Secretary Evans for joining the EAC meeting.

Assistant Secretary Evans said she appreciates the opportunity to be speaking at the EAC meeting and provided information about CESER. She said DOE is a sector-specific agency and works with a whole-government approach. DHS has overall authority on critical infrastructure. DOE is very specifically focused based on the authorities that have also been extended to the Department under the Fixing America's Surface Transportation (FAST) Act of 2015. After Secretary of Energy Rick Perry was sworn in, he looked at DOE's structure. Assistant Secretary Evans noted that CESER focuses on the energy sector from a national security perspective. She said that keeping in mind the responsibilities that the sector-specific agency has, the Secretary has no higher priority than energy security and the national security aspect of the energy sector. She added that CESER came out of the Office of Electricity (OE) but functions closely with OE because it is integrated into several offices across the Department. She noted that to achieve all the goals in the energy sector, it is important to analyze the associated risks and to reduce that risk by deploying solutions.

Assistant Secretary Evans then talked about the energy security aspect of CESER. She said they did a notice of intent from the Office of Energy Efficiency and Renewable Energy (EERE) for an advanced manufacturing innovative energy institute. This institute is a cybersecurity institute. For manufacturing, with all of the renewable types of information, there needs to be a concern about supply chain risk management. She said that while using microgrids and integrating solar into the grid, they need to make sure these components have been manufactured to reduce the risk. She noted that her office is working toward stimulating innovation and helping reduce the risk so that these technologies can be integrated into the grid for greater efficiencies.

Assistant Secretary Evans then discussed the emergency response framework that CESER is responsible for. When the national response framework is in place, CESER is part of the Federal Emergency Management Agency (FEMA) team and the whole government. She said that Puerto Rico is a good example of how their offices would function in that type of case. When the hurricane comes in, the Energy Support Function (ESF) #12 team mobilizes. She noted that CESER works with FEMA, Scott Aaronson and his group at the Electricity Subsector Coordinating Council (ESCC), the Oil and Natural Gas Subsector Coordinating Council (ONG SCC groups), and DHS. She mentioned that Assistant Secretary Walker is currently working on a longer term sustained recovery activity in Puerto Rico. She added that the Secretary is pleased with the progress the office is making and how they are functioning with the other offices within the Department.

Assistant Secretary Evans provided an overview of the cybersecurity activities that CESER is involved in. She said that the administration released its National Cyber Strategy, which is the first one in 15 years. CESER is responsible for pillar 1, which is, “Protect the homeland, the American people, and American way of life.” The very first activity that is supposed to happen is clarifying roles and responsibilities. In a cyber incident, DHS has the overall responsibility for critical infrastructure. DOE has responsibility for energy infrastructure as the sector-specific agency, as established in the FAST Act. In order to meet the national strategy outcome, DOE is clarifying roles and responsibilities and going through a policy process. There is a sense of urgency because of the worldwide threat assessment. She said that the industry and stakeholders need to have information that has been informed by intelligence to be able to take actions and be proactive about their defenses.

Assistant Secretary Evans then talked about two initiatives: the trisector initiative and the pipeline initiative. The three components of the trisector initiative are (1) DOE for energy and power, (2) DHS for telecommunications, and (3) Department of Treasury for the financial sector. She noted that the National Infrastructure Advisory Commission (NIAC), which advises the president, recommended these as three critical areas that map up to the national strategy. Power, telecommunications for power, and financial management are crucial. Health, safety, and IT are other areas. The ESCC is leading the effort for the energy sector from the industry side. On the telecommunications side, AT&T is leading the effort. The CEO of J.P. Morgan is leading the effort on the financial management side. The other initiative is the pipeline initiative, which was announced in October 2018 and is a joint initiative with the DHS. A joint exercise with FERC highlighted the interdependencies in the energy sector of oil and natural gas and the electricity group, so they could see where those interdependencies were, work on their plans, and discuss what they need to do. She added that this is another example of how her office works with its partners.

Assistant Secretary Evans highlighted three major areas CESER is working on. She said they have outreach to their industry partners because none of these initiatives will be successful without partnership from industry. Based on these initiatives, CESER is working to see how these solutions need to be in place to minimize the risk and manage infrastructure as it relates to cyber security, energy security, and emergency response.

- The Cyber Analytics Tool and Techniques (CATT) initiative is designed to provide the energy sector with situational awareness and information to help detect and mitigate

advanced cyber threats to the U.S. energy infrastructure and information enriched with classified threat information by the U.S. government. The DHS is working with DOE on this initiative.

- The Cybersecurity for the Operational Technology (OT) Environment project (CyOTE™), focuses on advancing situational awareness in the OT networks.
- The Cybersecurity Testing for Resilience of Industrial Control Systems (CyTRICS) program focuses on supply chain risk management.

Assistant Secretary Evans said the goal is to continuously provide information while working with their industry partners. DOE works with three ISACs, along with sector coordinating councils and a government coordinating council. She added that any feedback from the EAC would be very valuable.

Mr. Heyeck asked how the EAC could help CESER. Assistant Secretary Evans responded that it would be helpful if the EAC members think about questions such as “Has CESER thought about this issue?” or “Is CESER working on this issue?” She noted that CESER works closely with the defense critical infrastructure, as well as with state and the local governments.

John Adams asked if Assistant Secretary Evans could provide him a checklist of some sort that he could take back to his cybersecurity manager at Electric Reliability Council of Texas. Assistant Secretary Evans said that she could provide him a checklist but she is leery of checklists because people then tend to work just toward a checklist. She said they are working with the National Laboratories to see how much risk can be reduced for every dollar invested. CESER is currently working on a tool that will answer these questions. Even though there will be a lot of advanced mathematics involved, the interface will be simple so that the cybersecurity manager can sit with the engineers and work through how much money is going to reduce what amount of risk.

Paul Cicio said that in his organization, there are large energy-intensive manufacturers and they are doing their best to protect themselves from cyberattacks. He asked if there should be a role for these energy-intensive manufacturers as part of the programming and if cyber problems could originate in an industrial facility and then back into the electric grid or natural gas pipelines that can only make things worse. Assistant Secretary Evans responded yes to both of Mr. Cicio’s questions. She noted that the Department has announced a notice of intent on advanced manufacturing and they are very specific about the areas they will focus on.

Wanda Reder said that cybersecurity is a moving target and the Department cannot be fully transparent on what they are working on. She asked Assistant Secretary Evans how they separate public information and classified information and how they engage to the extent that is needed in order to convey information to the industry without revealing classified information. Assistant Secretary Evans said this is a major challenge because she is focused from a national security perspective but needs to work with industry and associations to achieve success. She said she will not be able to fix the clearance process because of about 800,000 people backed up in the clearance process. They are working to distribute mitigating strategies without making it known how they arrived at those strategies. She added that they are trying to have as much information unclassified, but her team works with the intelligence community, so it is a challenge. She noted

that the best thing that happened to CESER was the Director of National Intelligence's worldwide threat assessment because it is a public document. She said they bring in leadership from their coordinating councils and provide them the top-secret Sensitive Compartmented Information (SCI) briefings. They also provide Congress with the SCI briefings. They are in the process of doing those so that they understand the sense of urgency.

Anda Ray said that the Electric Power Research Institute (EPRI) is looking at operating technologies and cyber associated with operating technologies, as well as supply chain. She asked if they have looked at the intersection of OT and blockchain. Assistant Secretary Evans said that they are looking at the intersection of OT and blockchain, but she is moving more toward quantum key distribution because it is a purely physics-based approach whereas blockchain is collaborative and more subjective.

Mr. Heyeck thanked Assistant Secretary Evans for her remarks.

Panel: Electric Sector Cybersecurity Preparedness: Separating Facts From Fear, Uncertainty, and Doubt

Richard Mroz provided well wishes to Ann Delenela, who organized and was supposed to chair this panel. He then described his background over the last five years, first as president of the New Jersey Board of Public Utilities where he came to know the emerging issue of cybersecurity. He described his oversight of issuing a cybersecurity order to the regulated utilities of New Jersey to adhere to the NERC CIP standards, undertake training, review the workforce, and report on how companies were dealing with the issue of risk management. He continued to describe his work with the NARUC infrastructure committee to advance issues around cybersecurity in an active way. His committee held panels, developed a resource repository for state commissioners, and participated in an ongoing collaboration with federal partners. Mr. Mroz continued that he was the NARUC designee to sit at the ESCC with a security clearance and was able to hear about some of the threats directly. He added that he is now an independent consultant and advisor to a nonprofit, non-industry-funded organization called Protect Our Power to represent the private sector on continuation and focus on cybersecurity in this sector, identification of best practices, and supporting industry and regulators to confront the threat. He has worked with members of the panel or their organizations, and the work is important not only to this sector but the wider economy. He said the Conference Board surveyed CEOs across the country and results showed that cybersecurity was the top concern of the coming year. A comparable worldwide survey of CEOs similarly showed that the fear of cybersecurity was greater than fear of a global recession.

Mr. Mroz then introduced the panel: Sam Chanoski from the Electricity Information Sharing and Analysis Center (E-ISAC) to talk about information sharing; Mr. Aaronson from EEI where he is a Vice President and supports the ESCC; Lynn Costantini, Senior Director at NARUC covering an overview of activities from the states; and Robert Lee from Dragos to talk about how the private sector is supporting these efforts in the electric sector.

Mr. Chanoski began his remarks stating that this was his first time at an EAC meeting, and he

recognized the deep technical and business expertise of the EAC in the electricity sector. He said cybersecurity is another case of dealing with risk, and it is similar to handling other risks. He added that the technical challenge is only one aspect and it is more straightforward. However, the difficult part comes from organization governance and information sharing. He then described his running assessment from the past several years on electric cybersecurity. In trying to understand who attacks power grids, what those actors need for a successful attack is capability, intent, and opportunity. His greatest concerns are with nation-states that sponsor this type of activity as was discussed in the worldwide threat assessment. Mr. Chanoski was happy to see DOE, DHS, and other governmental organizations significantly increase their focus in the last 18 months to talk about these activities and get more of this information out there. He added that this will allow the right people to recognize the threat and understand what steps they can take to mitigate those risks.

Mr. Chanoski continued with the example that if an adversary takes an action in the physical world, the intention is to cause a physical effect. The next-level effect is in the information space where the quality of information changes, which impacts the decision-making cycle. He said the understanding of the situation will change by either a lot or a little, immediately or over time. He added that these changes would then have cognitive effects that alter your understanding and perception of a situation. This process is deliberately engineered in a threat from the physical to the informational and up to the cognitive effect. He concluded that it was really the cognitive effects that can be used to amplify cyber warfare and information attacks on the power grid. It is well-documented that the threats are real, but we do not really have a good understanding of threats. This leads to fear of the unknown, which gets amplified in media outlets. In some cases these psychological effects can distort our decision-making abilities.

Mr. Chanoski followed up with comments on the E-ISAC programs that Assistant Secretary Evans mentioned. He was interested in hearing the state perspective on these programs, particularly the CATT, CyOTE™, Neighborhood Keeper, and Cybersecurity Risk Information Sharing Program (CRISP). He added that E-ISAC is a clearinghouse of information with recommendations and seeks to get that to industry in a timely and actionable manner to improve their understanding of the situation. He added that E-ISAC operates with great support from industry and DOE.

Mr. Aaronson began his remarks by summarizing Ted Koppel's book *Lights Out*, as stating that government is inept, industry is profit-motivated, and everyone should buy freeze-dried foods. He said he disagrees with all of that and outlined why. He said first, government is integral to our ability to protect critical infrastructure and the safety and lives of customers. He added that, in fact, industry is profit-motivated, and must protect the system within which it operates. He added that preparedness is very important because you cannot protect everything from everything all of the time. It is mature to recognize the potential for failure and the need to do security the right way, using the whole community to protect critical infrastructure.

Mr. Aaronson added that cybersecurity is risk management. The key is how to prioritize something that you have to protect all the time. He said Assistant Secretary Walker identified the defense critical electric infrastructure and that is the best way to protect the Nation. He added that there are two ways that you can deter an attack. The first is to ensure that the attack

does not have the intended consequence. The other is to have a response for the attack. That response is solely the responsibility and purview of the government.

He continued that it is important to make the distinction between information technology and operational technology. Most cyberattacks attack the business systems and IT systems, but it is very different from the threat from attacking operational technology.

Mr. Aaronson followed that while we talk about cybersecurity, we consider all hazards with a measure of consequence versus likelihood. Combined cybersecurity and physical security attacks sit somewhere in the middle. He described the industry's way of protecting their systems in terms of the three legs of a stool. The first "leg" is checklists of mandatory and enforceable standards, citing examples for cyber, physical, and geomagnetic disturbance (GMD); however, checklists are not adequate on their own. The second leg is partnerships and the ESCC. Much of the work comes together to protect critical infrastructure. That work includes a number of initiatives that have advanced security posture, and includes many partners outside of industry and the federal government. He added that there are many ways to attack the grid and cited many interdependent sectors including water, transportation, and financial services. The last leg of the stool is our Nation's ability to respond and recover from these attacks.

Dr. Costantini began her remarks by thanking the organizers and citing the interests of state regulatory commissions, which are often overlooked in these venues. She added that the state regulatory community bears some of the responsibility for this. She wanted to use her time today to discuss the fears and uncertainty of threats and how this led to keeping state regulatory commissions on the outside of these conversations. She also planned to discuss the unclear position commissions play in the role, authority, and capability of addressing threats. Industry generally looks at regulators as simply economic regulators, responsible for safety and reliability at cost-effective customer rates. She added that until recently the focus of cybersecurity in the electric sector was exclusively on the bulk power grid with extensive federal doctrine discussing mitigation of risk to the bulk power sector. Dr. Costantini said that when talking about the uncertainty and focus on economics versus the bulk power system, state regulatory commissions have been excluded from the conversation. However, participants of the meeting today have underscored the importance of the state perspective.

Dr. Costantini continued that the threats have become more dire. Interdependencies of critical sectors have become more obvious, and the industry has evolved so rapidly that the distinction between bulk power and distribution grids does not matter anymore, which is why NARUC is at the meeting. NARUC's role is to identify policy challenges and alternatives and bring them into policy discussions. Cybersecurity has been part of these discussions. The Center for Partnership and Innovation (CPI) conducts analysis, resource development, education, and awareness of cybersecurity challenges from a policy perspective. Dr. Costantini said that over the last year, she has been focused on educating her constituents on cybersecurity threats, policy implications, and resilience at the distribution level. She has done that by using decision-support tools that individual commissions can also use. The tools support state policymakers on how to engage utilities on cyber risk management.

Dr. Constantini continued that NARUC developed a mini Cybersecurity Capability Maturity

Model (C2M2), which is not technical, to identify gaps and incentivize investment. Her team is also creating a tabletop exercise and testing it with a broad community of stakeholders. She continued that some of the challenges NARUC is grappling with include supply chain risk, incident recording, and information exchange.

Mr. Lee began his remarks by describing his role as CEO at Dragos. He planned to discuss where the industry is today, what concerns him, and what gives him optimism. He said the community has never been better, more reliable, or more resilient, but the threats are getting far worse. One thing he sees is a misunderstanding of the threats. He often hears people discussing the Ukrainian power grid attacks, but less so the attacks in Saudi Arabia that targeted petroleum facility safety systems with the intent to kill. He is concerned that discussions often cite the location of these attacks as being somewhere else or in a different sector, which diminishes the reality of the vulnerabilities in the United States and that these same groups are already targeting U.S. locations. He added that the media often takes the issues out of context. It is hard to have the right conversation on the risks.

Mr. Lee said his company is a technology company with a large services and intelligence arm. His background is from the National Security Administration. This community has never been more active with its response teams and last year responded to attacks on seven large manufacturers, which led to a total \$300 million in damages. He added that he is not worried about the grid going down. He is concerned that the fear of the threats will have a negative effect on the industry of an overreaction to an attack. His company is less concerned with the IT and enterprise environments, and focuses solely on industrial and operational technology environments, which is where most of the damage can occur. He added that many companies feel that they are protected, but they do not have great visibility into their environments. He found that close to 80% of environments that they have reviewed already have some kind of issue. While the U.S. has the most defensible networks on the planet, there is still considerably more training that the workforce needs. He added that a company like Dragos could not have existed five years ago, but there have been major shifts in the development of the community to providing defense of systems and that adversaries are disadvantaged. He said that one of his greatest concerns is a trend among industrial vendors to move toward common operating platforms and homogenous environments for the sake of cost savings and skills standardization. Maintaining heterogeneous infrastructure, such as having different types of substations in different areas, makes scaling an attack like the Ukraine attack difficult. He likes that there is a community goal to avoid this entirely. He added that DOE's Cyber-Informed Consequence-Driven Engineering Program is to look at more purpose-driven systems.

Mr. Mroz then prepared the panels for a Q&A session and asked Mr. McClelland from FERC to join the panel to provide a federal prospective.

Mr. Mroz then asked Mr. Chanoski and Mr. Aaronson what happens during an incident, how they handle the information flow, who talks, and who takes action. Mr. Chanoski responded that generally a company will start its own incident response plan and in some cases will institute certain NERC-CIP standards. He continued that companies should have a plan for what to do when recognizing a potential incident and know the legal requirements for what they need to tell certain organizations, including the E-ISAC. Companies should then identify, based on

contacts and including smaller electric cooperatives, whether the problem is within their system or if other broader organizations in the industry are affected. These companies can be a liaison to a larger audience that should be engaged to monitor and prepare for wider information-sharing as it comes available. Mr. Mroz followed up and asked if the E-ISAC has cross-sharing processes in place. Mr. Chanoski responded that the other ISACs do share across sectors. For example, the staff member of the Downstream Natural Gas IASC comes to their office with a multistate ISAC memorandum of understanding to share information. Mr. Aaronson added that the ESCC's first response when an incident occurs is: Who do you call? A call to one is a call to all. The calls support a unity of effort and unity of message. Entities then extrapolate how to convene the community to help each other during an incident and after an incident has occurred.

Mr. Mroz asked how the industry knows what entities to engage and when. Mr. Aaronson responded that there was fundamental distrust years ago. The FERC security organization has now incorporated support within the nonregulatory portion of the Commission. He tells people all the time that states deal with the consequences. Dr. Costantini followed that in states, the relationships are in the building stage. There is not a lot of trust in regulators. They are bringing subject matter experts together with public regulators in forums to talk about the state environment during an incident, and when a governor may decide what action to be taken.

Mr. McClelland briefly described as background his experience with Allegheny Energy for over 20 years before joining FERC. He said that standards establish baseline practices. The importance of the process is deliberative and slow to ensure there is full input. Then, when working on issues for national security, adversaries can read standards and execute based on those standards. He continued that when the industry understands a threat, they take action. He has never seen an assessment where the decision-makers did not direct immediate action. The regulator has all this context, and the companies always respond. He added that actions and activities can be represented by a pyramid, with standards on the bottom and best practices at the peak.

Mr. Mroz followed that this is a threat like no other because the threat is evolving rapidly. He asked Mr. Lee how his community of advisors is helping industry incorporate best practices. Mr. Lee responded that he has a bias that a lot of the communications that the cybersecurity community distributes are at a high level and that they are not necessarily reducing risk. He was concerned that patch fixes were not that valuable. His company researched the issue and found that 64% of all patches for industrial equipment introduced zero risk—no adversary had ever exploited a known patch. He added that sometimes companies undertake actions that seem correct but have no bearing on the security posture. The way to counter that issue is an intelligence-driven approach to assess threats. The concern is how the Ukraine or Saudi Aramco subsidiary attacks happened and what should be done to prepare for them. He added that the cost to protect systems is not cheap and that the technology his company utilizes is not affordable for smaller entities. Programs like Neighborhood Keeper that was started by DOE try not to overlap with the private effort to scale the technology to electric cooperatives and municipal-based utilities.

Mr. Mroz then asked Mr. Aaronson to discuss supplemental operating systems. Mr. Aaronson responded that if an incident occurred in the United States as it did in Ukraine, where 225,000

people lost power for a few hours, there would be a major overreaction from U.S. regulators. The community was still able to learn from the Ukraine incident and the importance of information sharing. Four of the Ukrainian companies had experienced an attack before, and one took action and the other three did not. The first company was able to get back up and running in a manual state. Mr. Aaronson said that they have found that utility CEOs say they can only run in a manual mode without digital infrastructure. He described the importance of operating a utility in a degraded state through supplemental operating strategies to get up and running as soon as possible. The North American Transmission Forum (NATF) took up this task. GE is working on it and other manufacturers are following suit. NATF came up with 13 recommendations that include the need for people to be able to operate the grid in a manual state. Mr. Aaronson added that operating a system manually includes the ability of people in the control center to communicate to people in the field. This confluence of engineering must be built out during blue-sky conditions.

Mr. Mroz turned the conversation to Dr. Costantini, asking how states are dealing with these issues and where they are in these efforts. She responded that there is a little bit of everything, depending on the state. No state is left that will say it has not done anything. States recognize that they have a role and responsibility to do something. Often the question is, as economic regulators: What should regulatory commissions be doing? She added that they should be talking to their utilities about what they are doing, how they are doing it, and the need from the public utility commission to do it faster and better. A vexing problem for engaging the wider community is workforce. Public utility commissions are not the first place where people with cyber skills seek to go and they need more technical expertise to accurately inform the policy conversation.

Mr. Heyeck asked Mr. Lee about the homogenous nature of utilities, and whether DOE can provide standards or recommendations to help assure technologies are not homogeneous beyond the utility space. Mr. Lee responded that, as the community collectively looks at building out infrastructure systems, it would be great to incentivize that the control and physical process for one is not the exact same as for another. He cited the example of one heavy industry that already is technologically homogeneous, for which an adversary would have to do minimal research to get to the next stage of the attack. Mr. Lee added that he believes utilities should get tax credits to invest in smart processes to train their workforce and secure their systems. He concluded that DOE is starting down the right path, but there is work to be done.

Ms. Reder followed that when thinking about the 16 critical infrastructures, eight of which are enabled by energy, how can we think about how the infrastructures converge and how can DOE make it easier to work across the other infrastructures? Mr. Mroz responded that that has been happening more at the state and federal levels. He then directed the question to Mr. Chanoski.

Mr. Chanoski used the term “seam” for where organizations or systems touch and the prime place in the system that can be exploited. He said there may be a gap in visibility, capability, and coordination. We need to identify those areas, strengthen connections, and watch those areas very closely. Mr. Aaronson agreed and cited Assistant Secretary Evans’ reference to the recent NIAC report that described the need for better cross-sector coordination. Government plays an important role in looking across sectors and identifying the seams, but because

administrations necessarily change over time, the private sector becomes the continuity across administrations. The private sector is the “supported command” responsible for identifying and filling gaps in their systems, and asking the government in its capacity as the “supporting command” for help when the private sector is unable to fill the gaps themselves. DOE has been good about not duplicating effort and is working in support of things that the private sector needs. Mr. Aaronson added that the NIAC report had a recommendation about bringing together the five lifeline sectors—electricity, water, telecommunications, finance, and transportation. Transportation is very diverse, with seven modes of transportation, none of which are the same. Water is important, but there are 168,000 water and wastewater utilities across the country. So what his team has done is create the trisector work to bring together telecommunications, electricity, and financial services as the lifeline of the country to protect seams and gaps.

Mr. Mroz asked Dr. Constantini and Mr. McClelland about the seam between the state and federal levels. Dr. Constantini responded that there is a strong seam, but there is a recognition to invest time and effort to build capability within state regulatory bodies with support from DOE. The relationships are being formed, but now that the recognition is there, they have been invited with open arms to fully participate in the conversation. She added that NARUC does not focus solely on one industry, so they are building relationships across sectors as well. Mr. McClelland said that when his office was set up, they knew that the adversary pivots across sectors but there are some fundamental concepts to understand. It is not just zero-day exploits that are the issue when phishing techniques are very successful. Operators want to maintain maximum administrator rights to system functionalities they never actually use, so when a phishing attack takes those operators’ credentials, the adversary gains access to that broad set of functionalities. In states that have moved to full scale on automated metering reading, questions need to be asked about how safe the equipment will be over time and where it comes from. If the functionality of that meter is limited then the risks are lowered.

Tom Bialek asked the panel about customers making choices about systems on their homes, including solar panels, where security is often an afterthought. Mr. Aaronson responded that it is similar to the concept of the least shippable product or minimal viable product, and whether you want that impacting critical infrastructure. There needs to be further incentives and requirements that have an impact on critical infrastructure. Mr. Mroz added that there is no manufacturing seal of approval for these types of products and that creates an issue.

Lola Infante then asked if distributed energy resources (DERs) can be part of a resiliency plan while still addressing these (security) issues. Mr. Aaronson responded that in Puerto Rico, people wanted to re-engineer the grid with microgrids and DERs are part of the solution. But the grid is the enabler or platform for security and resilience. Mr. Chinoski added that if you are going to connect to a utility, there needs to be some tariff contract that includes a minimum standard. There needs to be an understanding of what the grid is plugging in to.

Kimberly Denbow pointed out to media in attendance that the worldwide threat assessment is not news to the industry or the operators. She continued that the industry and operators work well with the government to prepare for these threats. Mr. Lee added that the natural gas pipeline industry got unfairly called out, and when his company asked about that they heard that there is no significant additional risk. Ms. Denbow followed up that the federal government has

a sense that there is a gap and nothing is being done. She thanked NARUC for responding to the challenge and bringing states to the table and educating them. She continued that the conversation needs to happen between the state and its regulated entity, the operator. The conversation also needs to happen between states and the federal government. She then asked the panel to respond about whether owner-operators are often held accountable for the cyber integrity of the equipment they buy.

Mr. Lee responded that utilities can be an easy target for blame, but there is still some negligence on their part as well. Mr. McClelland added that companies are accountable for what they are aware of. He has seen equipment that utilities were not aware of that had issues. The hard part is that sometimes the state regulators are not aware of these issues and may not approve a rate request to replace equipment. He knows DOE is working on this essential issue. He concluded that if there is at least a procurement restriction, that is probably a good reason to examine the topic.

Chris Ayers then asked about what regulators should look for when evaluating utility cybersecurity readiness plans. Dr. Constantini responded that is the entire purpose of the cyber manual, which builds off the cybersecurity primer to articulate processes, which was released in 2012. The manual includes questions for regulators to ask their utilities about preparedness. She continued that commissions did not have a way to evaluate the quality of answers they were getting. There was no structure to how the questions were asked. A new edition was organized, using National Institute of Standards and Technology (NIST) risk management steps, with specific, content-sensitive questions to ask and more questions depending on certain answers. When commissions have raw data, they can create an evaluation tool to filter answers and assess maturation of cyber preparedness. The goal is to have those conversations in a trusted environment that they are not out to overregulate but to understand and mitigate gaps. Mr. Mroz added that the factual foundation is also important for rate recovery.

Mladen Kezunovic then asked the panel to reflect on why the concept of cybersecurity is often separate from resilience. He said that within his studies, he does not differentiate attacks from any malfunctions that can deteriorate resilience and that could have an impact on how DOE addresses these issues. Mr. Lee responded that they should be distinct and that the discussion of resiliency does not take into consideration an adversarial response. He continued that a resiliency-based response may be the adversary's intention, whereas looking at the same incident through a defensive lens may lead to different actions that could prevent further damage. Mr. McClelland added that adversaries look for resiliency problems. If there is a single point of failure, we are agnostic in evaluation; but the applications to solve those issues include cyber assessments.

Clay Koplin said he is codeveloping a municipal water supply with electric generation for a FERC regulatory electric cooperative with extra costs for security as you stack costs on consumers to regulators. Dr. Constantini responded that a regulator would ask why those security requirements are needed. The regulators would look for alternatives if possible, but it is best for the regulators to know these issues in advance before even being asked that question.

Bryan Olnick then addressed the panel from an employee awareness and training standpoint. He

commented that while the panel has largely discussed external threats, his company also focuses on the threats from insiders, including external vendors who may have access to their systems.

Laney Brown asked about the maturity of the mutual assistance framework and workforce training requirements. Mr. Aaronson responded that cyber mutual assistance is 2 years old and that there is urgency after the GridEx 3 meeting to deal with cyber incidents. The ESCC Secretariat set out to develop and build out a cyber surge capacity. Three meetings were held to build out the concept, a legal structure and a playbook for utilizing it, and now there are more than 150 companies across the United States onboard with the cyber mutual assistance. The future state of this project is similar to traditional mutual assistance, in which a company can incorporate contractors, consultants, and experts as well as the National Guard in addressing future cyber episodes. Mr. Lee added that he wrote a course for industrial control, threat assessment, and response, which is effectively everything from IT security and physics. There are different mission requirements and different threats. For example, an IT person may not know how to talk to operating engineers, which is often a culture issue.

Mr. Heyeck thanked the panel and Mr. Mroz.

EAC Smart Grid Subcommittee Update

Mr. Adams, EAC Smart Grid Subcommittee Chair, provided an update on the Subcommittee's activities that are currently underway. Mr. Adams said that the Smart Grid Subcommittee is requesting EAC approval on its "Policy and Research Opportunities for Grid Resilience" work product. He said that the Subcommittee made four minor corrections to the work product, none of which were about substance. This work product came out of the panel "Perspectives on Grid Resilience," which was moderated by Sheri Givens during the October 2018 EAC meeting. The working group captured recommendations from the panel and sent it to the Subcommittee members for additional comments.

Mr. Adams then summarized the recommendations that came out of the work product on "Policy and Research Opportunities for Grid Resilience." These include:

- Develop a comparison of resiliency standards and methodologies.
- Modify the Interruption Cost Estimate (ICE) calculator tool.
- Make resiliency tools known to state organizations.
- Develop a resiliency handbook.

Dr. Kezunovic commented that the summary of the recommendations does not reflect the title because it does not talk about research. Ms. Denbow suggested adding "R&D" to the second recommendation, which is "DOE should direct Lawrence Berkeley National Laboratory to modify its Interruption Cost Estimate (ICE) calculator tool to evaluate costs of power outages beyond 24 hours and make evaluation of alternative resiliency investments more appropriate." Dr. Kezunovic said that ICE covers only certain aspects of this issue. He said that implying that the modification is in the R&D effort does not cover the methodologies, which require further research. Ms. Givens said there are numerous research opportunities, such as research into the different methodologies that are used to calculate the benefits, research into the different types of resilience measures used across the country, and research into what states are doing to effectuate

resilience opportunities for their grid systems. She added that research is needed to find subject matter experts who are responsible in their respective states. Tom Weaver said that the detailed recommendation section asks for research to help modify resiliency standards and the ICE calculator. He said that even though those recommendations do not specifically use the word “research,” research is in the detailed recommendations. It was decided to not add the word “research” in the summary. Mr. Adams moved to approve the work product. Drew Fellon seconded the motion. The EAC unanimously approved the work product.

Mr. Adams then moved on to discuss the work in progress. He said that the two panels under discussion for the June EAC meeting are about eliminating or reducing spinning reserve requirements and the EPRI Electromagnetic Pulse Technology/Geomagnetic Disturbance (EMPT/GMD) report. He noted that there might not be enough time for both panels in the next meeting. He will work with the EAC leadership about when each of these panels can be scheduled. In addition, the Subcommittee is considering a panel on grid planning for the October EAC meeting. Another topic under discussion involves the coordination of state and federal governments on the smart grid and resiliency. Mr. Adams said DOE has volunteered to help with some of these topics. A Smart Grid call will be scheduled before the end of March to discuss the panel topics. Mr. Adams noted that it is possible that work products will stem from the panels on “Value Proposition for Big Data Analytics” and “Energy Sector Cybersecurity Preparedness: Separating Facts from Fear, Uncertainty and Doubt.” He added that DOE has asked the EAC to provide recommendations on the 2018 DOE Smart Grid System Report by June 2019. Mr. Heyeck said that everyone should have received this report. He said that DOE has asked the EAC to review the 2018 report and provide comments for the 2020 report. He asked EAC members to send their comments to Chris Lawrence.

Mr. Lawrence said that DOE will organize a webinar to review the 2018 DOE Smart Grid System Report to make recommendations for the 2020 report. He added that calls will be scheduled after the webinar for further discussion.

Mr. Adams said would like to schedule a planning call to discuss the panels and the upcoming activities for the Smart Grid Subcommittee.

Public Comments

There were no public comments.

Adjournment of Day 2 of the March 2019 EAC Meeting

Ms. Reder said she was impressed with the dialogue and interaction during both the panels and appreciated the effort that went into putting them together. She wondered how discussions during the EAC meetings will get communicated to the rest of the world, including effective communication with stakeholder groups. She looked forward to hearing from OE Deputy Assistant Secretary Katie Jereza about DOE efforts to engage with stakeholders. Ms. Reder said that the state regulator involvement is very healthy but there is a lot of opportunity to bring in

more tools, knowledge, and collaboration. She said that the EAC has great thought leaders who can be leveraged more to make even bigger differences. Even though the technology is present, evolution and transformational changes are occurring simultaneously—and require education. Ms. Reder challenged DOE and the EAC to think about what can be done to enable the transformational aspect. She noted that the EAC brought in more talent than ever before on both the panels. She said it was a great meeting and thanked everyone for their participation.

Ms. Jereza said it is important to look at how the EAC works and how EAC members can know how their work impacts and influences DOE. DOE will work on making the EAC members understand how, when, and where they can engage and how DOE can get back to EAC to let them know they have made a difference. Ms. Jereza thanked everyone for approaching her and letting her know what DOE can do.

Mr. Heyeck said that the next EAC meeting would be held June 19 and 20, at the same location, starting at 1 p.m. and ending the next day at noon. He noted that there is a lot of activity happening within the two Subcommittees. He added that the EAC is trying to bring back a panel on energy storage because energy storage is going to be the disrupter in the electric sector in the coming years.

The meeting was then adjourned.

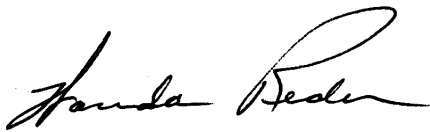
Respectfully Submitted and Certified as Accurate,



Michael Heyeck
The Grid Group, LLC
Chair
DOE Electricity Advisory Committee

06/10/2019

Date



Wanda Reder
Grid-X Partners, LLC
Vice-Chair
DOE Electricity Advisory Committee

06/10/2019

Date



Christopher Lawrence
Office of Electricity
Designated Federal Official
DOE Electricity Advisory Committee

06/10/2019

Date