S. HRG. 116–378

FEDERAL AND INDUSTRY EFFORTS TO IMPROVE CYBERSECURITY FOR THE ENERGY SECTOR, INCLUDING HOW TO IMPROVE COLLABORATION ON VARIOUS CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION INITIATIVES

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

AUGUST 5, 2020

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

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

U.S. GOVERNMENT PUBLISHING OFFICE

41–402 WASHINGTON : 2021

COMMITTEE ON ENERGY AND NATURAL RESOURCES

LISA MURKOWSKI, Alaska, *Chairman*

JOHN BARRASSO, Wyoming
JAMES E. RISCH, Idaho
MIKE LEE, Utah
STEVE DAINES, Montana
BILL CASSIDY, Louisiana
CORY GARDNER, Colorado
CINDY HYDE-SMITH, Mississippi
MARTHA MCSALLY, Arizona
LAMAR ALEXANDER, Tennessee
JOHN HOEVEN, North Dakota

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

BRIAN HUGHES, *Staff Director*
LUCY MURFITT, *Chief Counsel*
JAKE MCCURDY, *Professional Staff Member*
ROBERT IVANAUSKAS, *FERC Detailee*
RENAE BLACK, *Democratic Staff Director*
SAM E. FOWLER, *Democratic Chief Counsel*
NICOLE BUELL, *Democratic Professional Staff Member*

CONTENTS

OPENING STATEMENTS

WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

FEDERAL AND INDUSTRY EFFORTS TO IMPROVE CYBERSECURITY FOR THE ENERGY SECTOR, INCLUDING HOW TO IMPROVE COLLABORATION ON VARIOUS CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION INITIATIVES

WEDNESDAY, AUGUST 5, 2020

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

The Committee met, pursuant to notice, at 10:07 a.m. in Room SD–366, Dirksen Senate Office Building, Hon. Lisa Murkowski, Chairman of the Committee, presiding.

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

The CHAIRMAN. Good morning, everyone. The Committee will come to order. We are here this morning to examine federal and industry efforts to improve the cybersecurity of the energy sector, including efforts to improve collaboration on various cybersecurity and critical infrastructure protection initiatives. It has been more than a year since we last held a hearing on cybersecurity for the energy sector, but I think it is fair to say that this is always a timely topic. It is also a critical priority that we cannot lose sight of, even as we grapple with COVID–19, lest it become the source of our next national crisis.

There have been a few noteworthy developments since our last hearing. Earlier this year, the President issued an Executive Order focused on securing the bulk power system from both cyber and physical threats posed by hostile nation-state actors. This is an effort that will be led by the Department of Energy (DOE). Meanwhile, the Federal Energy Regulatory Commission (FERC) has published a paper detailing a potential structure for providing incentives to utilities to make cybersecurity investments following up on a technical conference examining the same issue in 2019. I am pleased this morning to be able to welcome our witnesses from DOE and the FERC and to look forward to hearing the latest from them. I also welcome the witnesses representing industry which will play an equally significant role in how these initiatives unfold.

The threat of cyberattacks by foreign adversaries and other sophisticated entities is real, and it is growing. As I mentioned on the Senate Floor earlier this week when we confirmed Mark Menezes,

cyberattacks are near constant and only growing more sophisticated. According to the latest worldwide threat assessment from the Office of the Director of National Intelligence, China, Russia and other foreign adversaries are using cyber operations to target our military and our critical infrastructure. Those near-peer adversaries already have the capability to launch cyberattacks against our electric and gas infrastructure. The COVID–19 pandemic has created a unique opportunity for cyber criminals to attack our networks, including critical energy infrastructure. The Department of Justice (DOJ) recently issued a press release announcing the indictment of two individuals backed by the Chinese Ministry of State Security. DOJ noted these two individuals not only targeted portions of our energy sector, including DOE's Hanford site, but also entities conducting research on a Coronavirus vaccine. We cannot allow hostile foreign nations to disrupt our way of life.

Energy is the lifeline for all critical infrastructure sectors, and protecting our critical infrastructure is the first step in ensuring its continuity. Unfortunately, we have already seen the real-world ramifications of cyberattacks on the energy infrastructure, and this is most vividly seen in Russia's attacks on Ukraine. In December 2015, Russian hackers cut off power to nearly a quarter million people in Ukraine in an attempt to disrupt and intimidate. In the summer of 2017, Russian hackers infiltrated the industrial control system of a Saudi Arabian petrochemical plant and disabled the plant's safety systems. More recently, an advanced Russian government-backed hacking group is alleged to have probed a U.S. energy entity's network, according to a release the DOE issued in January. We all know the stakes here. A successful hack could shut down power impacting hospitals, banks, gas pumps, military installations and cell phone service. The consequences would be widespread and devastating and only more so if we are in the midst of a global pandemic.

The Federal Government and industry focus on cybersecurity is a major reason why the United States has not experienced an attack like Ukraine's. Protection of our critical assets is a shared responsibility demanding that federal, state and private sector partners work together to improve cyber defenses and coordinate responses to cyberattacks. The FAST Act of 2015 contained provisions authored by our Committee to codify the Department of Energy as the sector-specific agency for the energy sector and to provide the Secretary with authority to address grid-related emergencies. We also sought to facilitate greater information sharing by protecting sensitive information from disclosure. Our American Energy Innovation Act also has numerous sections to enhance government industry partnerships in this space and establishes programs to enhance the cyber posture of smaller utilities. Most recently, I introduced a new bill, the Energy Infrastructure Protection Act, to update provisions in the Federal Power Act and restrict federal disclosures of certain sensitive energy information. I know that there are a few who may disagree with that approach, but the alternative, disclosing and displaying our vulnerabilities for our enemies, will hardly make us any safer.

I am pleased to welcome a distinguished panel of witnesses who are truly at the front lines of the effort to protect our energy infra-

structure from cyber threats. I thank you again for being with us this morning.

I will now turn to my colleague and Ranking Member, Senator Manchin, for his opening remarks.

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

Senator MANCHIN. Thank you, Chair Murkowski, for convening this hearing today, and thank you to our witnesses for making yourselves available to join us and discuss efforts to improve the cybersecurity of the electric sector. As a Ranking Member of both this Committee and the Senate Armed Services Cybersecurity Committee, I am intensely focused on the security of our energy infrastructure. We just had a meeting yesterday on that, and it was quite enlightening. And the importance of our discussion today against the backdrop of a global pandemic is not lost on any of us, I believe, in this room.

The COVID–19 crisis has made our nation, the world, acutely aware of the consequences of being underprepared for a catastrophic event. The pandemic has forced the energy industry to adapt to new challenges and vulnerabilities with more employees working remotely. There are certainly lessons to be learned from this moment in history about the need to invest in protections to avoid, to mitigate and respond to events that challenge our grid's resilience and thereby our national resilience. You all know well that threats to critical infrastructure are serious and increasing daily. In recent months, federal officials have warned of rising cybersecurity threats from China, and recent reports indicate Russia has shown renewed interest in targeting the U.S. power grid. Then last month, a national security agency and the Cybersecurity and Infrastructure Security Agency (CISA) issued an alert urging critical infrastructure operators to take immediate action to secure their operation technology assets. Legacy grid systems are/were not designed to defend themselves against modern cyberattacks, and as they grow more and more connected to the internet, our electric systems grow more and more vulnerable. On top of that, IBM recently issued a report that showed that the energy sector suffers particularly high costs from state-sponsored cyber threats. Compared with the previous year, the costs of cyber breaches are up 14 percent because of the increased number of attacks targeting power grid infrastructure and the magnitude of the damage caused.

There is a lot of work being done across the sector to address these cybersecurity challenges. I would like to highlight the good work of my colleague, Senator King, who recently co-chaired the Cyberspace Solarium Commission. This Commission issued a report this spring identifying a number of recommendations to reduce the probability and impact of cyberattacks of critical infrastructure which he presented to the Senate Armed Services Committee yesterday, and it was truly quite enlightening. Although the report is broad in scope, many of the Commission's recommendations affect the electric industry, and I look forward to hearing about the impact to the electric sector today.

A few months ago the President issued an Executive Order directing the Department of Energy to identify foreign-made grid

components that pose an unacceptable security risk to the U.S. power grid. While I support this action, I was concerned that vendors and manufacturers of the grid equipment the order targets were not being adequately consulted. Senator Risch and I sent a letter to the DOE about these concerns and are eager to see DOE utilizing the valuable knowledge and experience of manufacturers as they implement this Executive Order. Having both DOE and industry representatives here today, I look forward to hearing how these engagements are going. There are certainly opportunities for Congress to facilitate action in this space as well, and I am proud that the American Energy Innovation Act included several pieces of legislation that support investments in programs that are of vital importance to securing and protecting our critical energy infrastructure. The bill would strengthen public-private partnerships like those I know our witnesses will discuss today and included my and Senator Murkowski's PROTECT Act which would establish incentives for electric utilities to invest in advanced cybersecurity technologies.

I am still committed to passing this comprehensive bipartisan energy package so that these important programs can be put into action. We have lots to do to protect and secure our electric grid. I look forward to hearing from our agency and industry witnesses today and what efforts are working and what work still remains to be done.

Thank you, Madam Chairman.

The CHAIRMAN. Thank you, Senator Manchin, and you mentioned the work of Senator King on the Cyberspace Solarium Commission. Senator King, as a member of the Committee, has asked for a brief moment here to introduce just that and, as you have mentioned, he has had an opportunity before the Senate Armed Services. It is important to acknowledge that work.

Senator King, if you would like to make any brief comment about that before we turn to our distinguished panel, you are certainly welcome to proceed.

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

Senator KING. Absolutely. Thank you, Madam Chair. You outline very eloquently the danger, so I don't really have to spend a lot of time on that. Everybody in this hearing knows the level of risk that we have before us.

Just let me tell you a bit about the Solarium. It was created in the 2019 National Defense Authorization Act (NDAA). It was a national commission whose mission was to establish a comprehensive strategy to defend this country in cyberspace. The structure of the Commission was somewhat unique. It had 14 members including 4 sitting Members of Congress: myself; Senator Ben Sasse; Congressman Mike Gallagher, a Republican from Wisconsin; and Jim Langevin, who is a Democratic member of the House and a member of the Armed Services Committee from Rhode Island. We also had four members from the Executive Branch and six members from the private sector. One of the most valuable members of the entire Commission was Tom Fanning, who is the CEO of the Southern Company, which I think is the second largest electrical

utility in the country. We had over 30 meetings. We had about 90 percent attendance at all of our meetings, and we talked about a whole range of cyber issues.

Our report really boils down to three simple points. One is reorganization. Reorganizing and organizing our government to be responsive to this problem and not operate in silos. Secondly is resilience. How to strengthen our resistance to cyberattacks and how to build up our defenses, if you will. And the third is response. How do we develop a deterrent doctrine so that our adversaries have to feel that they will pay a price for attacking this country, even if it is below the level of the threshold of the use of force?

Energy, of course, is a major target. One of the challenging parts of this problem, which you and Ranking Member Manchin mentioned, is that this really has to be a partnership between the Federal Government and the private sector. Eighty-five percent of the target space in cyberspace is in the private sector, a lot of that is the energy sector. And if there is one thing we learned from the pandemic, it is that the unthinkable can happen and a significant cyberattack is not unthinkable. We know that it is being planned, and we know that it is happening today. I spoke recently to a utility executive who told me that his system is attacked three million times a day, now, today. So this is not an abstract issue. This is something that we have to address, and the Commission made a number of legislative recommendations, more than two dozen of which we hope will be included in the final National Defense Act that is now headed to conference. I want to thank the Committee and the Chair and the Ranking Member for their cooperation on assisting us in getting those provisions into the National Defense Authorization Act. There will be others that we will be discussing over the next few months in this Committee.

But I want to thank you for having this hearing. It is incredibly important. This is one of our prime issues, and I look forward to the testimony of our witnesses. Again, thank you for your work on this and if we work together, we can defend this country.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator King. Thank you for that brief summation and to those of you, including Senator Sasse, who were part of that very, very important Commission.

Let's turn to our panel this morning.

We have one of our witnesses that has joined us in person. We thank you for that. Mr. Alexander Gates, who is the Senior Advisor at the Office of Policy for Cybersecurity, Energy Security, and Emergency Response. It is a long name. We call it CESER there at the U.S. Department of Energy. We welcome you to the Committee, Mr. Gates.

With us virtually today are Mr. Joseph McClelland, who is the Director of the Office of Energy Infrastructure Security at the Federal Energy Regulatory Commission. We welcome you, Mr. McClelland.

Mr. Steve Conner is the President and CEO for Siemens Energy, and we thank you for being part of this panel this morning, Mr. Conner.

Mr. Thomas O'Brien is the Senior Vice President and Chief Information Officer at PJM Interconnection. We appreciate that you

have joined us as well and look forward to your input to today's discussion.

With that, we will go in the order that I have introduced you. We will begin here in the Committee room with Mr. Gates. We would ask you all to try to keep your comments to about five minutes. Your full statements will be included as part of the record, and then we will have an opportunity for questions from those of us present and those of us online.

Mr. Gates, welcome, and again, thank you for your leadership there at the Department of Energy. Please proceed.

STATEMENT OF ALEXANDER GATES, SENIOR ADVISOR, OFFICE OF POLICY FOR CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE, U.S. DEPARTMENT OF ENERGY

Mr. GATES. Thank you, ma'am.

Chairman Murkowski, Ranking Member Manchin and members of the Committee, thank you for the opportunity to appear before you to discuss the Department of Energy's important work to protect the energy infrastructure from cyber threats. A reliable, resilient and secure energy infrastructure is critical to U.S. economic competitiveness, national security and, to put it frankly, our way of life. As an organization responsible for safeguarding the nation's nuclear stockpile and as a member of the intelligence community, the Department of Energy is keenly aware of threats to our national security. Today that includes cyber threats to the energy sector. In the 2019 and 2020 worldwide threat assessment, the Director of National Intelligence stated, "Our adversaries and strategic competitors will increasingly use cyber capabilities to seek political, economic and military advantage over the United States and its allies and partners. China, Russia, Iran, North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways, to steal information, to influence our citizens and to disrupt critical infrastructure."

Within the Department, CESER and the Office of Electricity form a nucleus that provides products and services that improve the energy sector's cybersecurity and resilience. Whether it's electricity, oil, natural gas or renewables, CESER endeavors to increase the security of the United States' energy infrastructure against all hazards through the following priorities: improving emergency response and recovery, expanding cyber discovery activities, creating high fidelity situational awareness, providing more focused research and development, further solidifying our partnerships and increasing workforce development efforts. The Office of Electricity, on the other hand, is focused on long-term research and development to build a secure and resilient power grid. The Office has four strategic priorities: building advanced modeling capabilities, innovating in the field of megawatt scale grid storage, improving grid operations and performance through advanced sensing technology and securing defense critical electric infrastructure.

Some key DOE initiatives that come out of those groups of priorities include the Cyber Risk Information Sharing Program, or CRISP, which is a public-private data sharing and analytic platform that facilitates the timely, bidirectional sharing of threat information amongst energy sector stakeholders. The North Amer-

ican Energy Resilience Model (NAERM), which is a modeling capability that analyzes risk and threats to the grid and other interdependent infrastructures, provides operational situational awareness. The Cybersecurity Testing of the Resilience of Industrial Control Systems, or CyTRICS, tests critical components to identify and mitigate embedded cyber vulnerabilities in industrial control systems within the energy sector. And, of course, Executive Order (EO) 13920, Securing the United States Bulk Power System in response to the growing threat the EO authorizes the Secretary of Energy, working with other federal departments and agencies and the private sector, to quickly and proactively protect the bulk power system.

Cybersecurity in the energy sector is a complex endeavor that will require more authorities, laws, and in some respects, an extreme level of collaboration to achieve. As a sector-specific agency, the Department of Energy relies on strong collaboration with FERC, NERC, and CISA, in order to make progress. Utility owners, coordinating councils, and trade groups are all very effective partners in this fight. Collectively these entities form the fabric of a public-private partnership that everyday serves to protect the nation's energy infrastructure. Despite all the progress made to date, the cyber threats to the sector are real and outpacing our collective solutions. Still, more action is needed to make the energy sector more resilient and cybersecure.

Thank you for this opportunity to appear before your Committee. I look forward to working with you to address the nation's cyber and physical security challenges to the energy sector.

[The prepared statement of Mr. Gates follows:]

Testimony of Alexander Gates

Senior Advisor in the Office of Policy for
Cybersecurity, Energy Security, and Emergency Response
U.S. Department of Energy

Before the

Committee on Energy and Natural Resources
United States Senate

August 5, 2020

Introduction

Chairman Murkowski, Ranking Member Manchin, and Members of the Committee, thank you for the opportunity to appear before you to discuss the Department of Energy's (DOE) important work to protect the critical infrastructure of the energy sector from cyber threats. A majority of the efforts in this regard are led by the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) with support from the Office of Electricity (OE).

The DOE and its numerous partners in the Federal, State, local governments, private sector and national laboratory community are keenly aware of the numerous and complex cyber challenges that the energy sector faces. One of the most noteworthy challenges is that our adversaries are conducting an increasing number of malicious cyber activities against our nation's infrastructure, which poses a persistent threat to our nation's security and economy. These ongoing campaigns demonstrate the continued need to use the full range of legal authorities and technological capabilities afforded to the U.S. Government, including strengthening our national resilience through cyber defense and close cooperation with the private sector.

Given the Nation's growing dependence on the energy sector to power every aspect of our lives, and the increasing interdependencies of the sector on communication systems and other critical infrastructures, a major attack could cause wide-ranging national security and economic impacts. Our Nation's electricity and fuel delivery systems are complex and interdependent. There is a great potential for negative and cascading impacts when operator error, software upgrades, and equipment failures occur in formerly isolated environments. As a result, energy cybersecurity and resilience are among the Nation's most urgent security challenges.

A reliable and resilient energy infrastructure is critical to U.S. economic competiveness, national security, and the American way of life. The DOE is continually seeking to increase this reliability and resiliency by ensuring engagement with all stakeholders, particularly those in the energy sector. We also seek to take advantage of DOE's considerable strengths such as the national lab complex and our relationships across industry and State and local governments.

Within the DOE, CESER and OE work together to provide products and services to improve the energy sector's cybersecurity and resilience. The close collaboration between the two offices

improves the seamless nature and impact of the solutions that the Department offers to the energy sector.

Office of Cybersecurity, Energy Security, and Emergency Response

The mission of CESER is to improve the security of the United States energy infrastructure against all hazards via two main divisions of the Office: Cybersecurity for Energy and Delivery Systems, and Infrastructure Security and Energy Restoration. CESER's mission to improve the security and survivability of the Nation's energy infrastructure cannot be achieved without both near- and long-term activities that strengthen the cybersecurity of the energy infrastructure across the Nation. In order to achieve these outcomes, the DOE has developed and prioritized CESER's goals as follows:

- **Build a Superior Workforce** – CESER will recruit, hire, retain, train, and organize resources with a focus on deepening and sustaining technical knowledge in Industrial Control System Cybersecurity across the Department, and will help enable industry to do the same.
- **Modernize Emergency Response & Recovery** – CESER will continue efforts in modernizing DOE's capabilities to respond to all hazards in close coordination with Federal interagency partners, infrastructure owners and operators, and State and local governments by expanding skills and using new and different technologies and products – informed by lessons learned from current and recent incidents.
- **Develop Cyber Discovery** – CESER will enhance sector-wide situational awareness and cultivate multi-faceted threat intelligence to support timely and appropriate action. CESER will convene stakeholders to jointly establish operational cybersecurity processes and apply technology and products to enhance predictive capabilities to prevent cyber incidents in the energy sector.
- **Improve Situational Awareness** – CESER will continuously improve energy sector situational awareness capabilities through development of consensus driven stakeholder requirements, application of predictive analytics, integration and optimization of technology platforms, and closely linking R&D investments and sector needs.
- **Focus Research & Development** – CESER seeks to accelerate the impact of the world-leading capabilities resident in the DOE Labs and partners by: constantly evaluating the current portfolio, ensuring that R&D advances other strategic goals, addressing emerging vulnerabilities, and sizing resources and organizational structure appropriately.
- **Strengthen Partnerships** – CESER will heighten its collective impact through streamlining communication and outreach, providing products and expertise to support timely risk and threat information sharing, and training to build sector capacity.

Office of Electricity

OE works to provide a secure and resilient power grid which is vital to our national security, economic security, and the services Americans rely upon. Working closely with private and public partners, OE acts to ensure the nation's most critical energy infrastructure is resilient and

able to recover rapidly from disruptions. Under the leadership of the Assistant Secretary for Electricity, the organization is focused on long-term research and development to build a secure and resilient power grid. OE has four strategic priorities:

- **Build Advanced Modeling Capability** - Working with the national labs and relevant stakeholders, OE is developing an integrated North American Energy Resiliency Model (NAERM) to conduct planning and contingency analysis to address vulnerabilities in the North American energy system.

- **Advance Megawatt Scale Grid Storage** - OE is pursuing megawatt scale storage capable of supporting frequency regulation, ramping, and energy management for bulk and distribution power systems.

- **Improve Grid Operations and Performance through advanced Sensing Technology** - OE is pursuing integration of high-fidelity, low-cost sensing technology for predictive and correlation modeling for electricity.

- **Secure Defense Critical Electric Infrastructure** - OE is implementing the authorities provided under the Fixing America's Surface Transportation Act (FAST Act) to define and secure Defense Critical Electric Infrastructure (DCEI). DCEI is defined as any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary of Energy to be: 1) critical to the defense of the United States, and 2) vulnerable to a disruption of the supply of electric energy provided to such a facility by an external provider, but is not owned or operated by the owner or operator of such facility..[1] Similarly, these two conditions also constitute the definition of critical defense facilities.

Key DOE Initiatives

Further Understanding and Testing the Resilience of Our Industrial Controls

CESER's Cybersecurity Testing for Resilient Industrial Control Systems (CyTRICS™) program serves as a central capability for the DOE's efforts to increase energy sector cybersecurity and reliability through the testing and enumeration of critical components to identify and mitigate embedded cyber vulnerabilities across the energy sector. Analysis of test results will identify systemic and supply chain risks and vulnerabilities to the sector by correlating collected test data and enriching it with other pertinent data sources and methods. The DOE has signed multiple agreements with energy sector partners to grow the CyTRICS™ program from a proof of concept to a robust supply chain cybersecurity program for the sector. We will continue collaborating with other Federal partners, the DOE Labs, and industry to identify key energy sector industrial control systems components and apply a targeted, collaborative approach to these efforts.

[1] *See* 16 U.S.C 824o-1(a)(4).

Bulk Power Executive Order

The bulk-power system (BPS) is the backbone of the U.S. electric grid, which is critical to our national security, the economy, and way of life. As outlined in the *Office of the Director of National Intelligence 2019 Worldwide Threat Assessment* and the *2020-2022 National Counterintelligence Strategy*, foreign adversaries continue to develop new ways to compromise the BPS and the supply chain of critical components, thereby undermining national security.

To confront this increasingly sophisticated threat, the President signed Executive Order (EO) 13920 "Securing the United States Bulk-Power System" on May 1, 2020, authorizing the Secretary of Energy, working with other Federal departments and agencies, and private industry, to quickly and proactively protect the BPS.

The DOE is in the process of operationalizing EO 13920 through four "pillars" of implementation:

1) prohibiting particular foreign adversaries from supplying particular BPS electric equipment;
2) establishing a list of pre-qualified vendors of BPS electric equipment;
3) developing advisory recommendations for the identification, isolation, monitoring, and replacement of at-risk equipment currently on the system; and
4) presiding over the Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security.

Immediately after the May 1st signing of the EO, OE and CESER began an extensive outreach campaign, which ultimately resulted in 50 briefings with more than 2,300 participants from more than 900 organizations. With the intent of being as inclusive as possible, briefing participants included representatives from industry, associations, and the Federal family.

Many practitioners within the cybersecurity field often have accurately asserted that you cannot protect what you do not know you have. This was one of the rationales behind EO 13920. Accordingly, through the efforts of the DOE and its stakeholders in implementing the EO, we will unlock a new degree of critical visibility into how best to prioritize our collective efforts to address the threats.

North American Energy Resilience Model

The DOE, in accordance with its responsibility and authority to identify, minimize, and respond to risks facing the United States energy sector, has begun development of the NAERM. The NAERM is best defined as a set of modeling capabilities for the analysis of risks and threats to the grid, and other interdependent infrastructures. Unlike the status quo, the NAERM will equip the DOE with the capabilities needed to quickly assess the resilience of the electrical grid and inform the Secretary with the real-time holistic situational awareness required to address emergencies as they unfold.

Developed in coordination with eight DOE Labs, the NAERM is the first of its kind, and the foundation for analyzing the North American electric power system and its interdependencies with other infrastructures in real-time, such as natural gas and communications. When complete, NAERM will address both long-term energy planning and energy planning and operational studies with real-time data streams, national-level situational awareness for both infrastructure and threats, and analytic and decision support capabilities to anticipate threats and mitigate their impacts.

Developing and Identifying the Energy Cybersecurity Workforce of Today and Tomorrow

Cybersecurity workforce development is a national priority outlined in the President's National Cyber Strategy and Executive Order on America's Cybersecurity Workforce (Executive Order 13870). Through its CyberForce Competition, the DOE seeks to identify and develop the next generation of cybersecurity professionals who will secure the nation's critical energy infrastructure. In November 2019, the DOE held its fifth CyberForce Competition hosted by 10 National Laboratories and featured a professional-level pilot which included scoring that will be considered to identify highly qualified individuals for potential employment with the DOE. In 2019, 105 collegiate teams from 32 states and Puerto Rico participated in the CyberForce Competition, a nearly 67% increase in participation over the prior year's 63 teams from 24 states and Puerto Rico. CyberForce 2020 will be held virtually on November 14th and will focus on assessing the skillsets of individual competitors representing their respective academic institutions.

Key Partnerships

The Departments of Defense and Homeland Security and the Intelligence Community are crucial partners in the effort to protect the nation's energy infrastructure from cyber threats. The DOE holds regular discussions with energy sector Information Sharing and Analysis Centers (ISACs) to share emerging and potential threats and disseminate information. A critical DOE role is our work with State officials to facilitate state-industry preparedness and response coordination, encourage response plans that help prepare for any potential consequences of a cyber-attack, and to offer training and exercises to ensure that the States are ready and able to mitigate incidents and respond, if needed.

The DOE also works closely with our public and private partners to support and bolster the actions that are needed to help ensure the reliable delivery of energy. We continue to coordinate with industry through the Sector Coordinating Councils to synchronize government and industry cyber incident response playbooks.

Conclusion

The President recognized the threat to the energy sector, and through EO 13920 "Securing the United States Bulk-Power System", is empowering the DOE to take bold action. The Secretary of Energy has proven his continued commitment to reliable and resilient energy infrastructure, and through CESER is bolstering the DOE's collaboration with industry and State and local governments to protect our Nation's critical energy infrastructure from all hazards, including the growing cyber threat. Our long-term approach will strengthen our national and energy security and protect the American way of life.

I appreciate the opportunity to appear before this Committee to discuss cybersecurity in the energy sector. I look forward to working with you and your respective staffs to continue to address physical and cybersecurity challenges to the energy sector, and welcome any questions you may have. Thank you.

The CHAIRMAN. Mr. Gates, thank you very much for that testimony.

We will now go online to Mr. McClelland, with the Federal Energy Regulatory Commission. Welcome.

STATEMENT OF JOSEPH MCCLELLAND, DIRECTOR, OFFICE OF ENERGY INFRASTRUCTURE SECURITY, FEDERAL ENERGY REGULATORY COMMISSION

Mr. MCCLELLAND. Thank you, Chairman Murkowski, Ranking Member Manchin and members of the Committee. Thank you for the privilege to appear before you today to discuss potential threats to the bulk power system in the United Sates. My name is Joe McClelland, and I am the Director of the Office of Energy Infrastructure Security at the Federal Energy Regulatory Commission. I come before you as a Commission staff witness, but I should note that my remarks do not necessarily represent the views of the Commission or any individual Commissioner.

In the Energy Policy Act of 2005, or EPACT 2005, specifically Section 215 of the Federal Power Act, Congress entrusted the Commission to approve and enforce mandatory reliability standards for the nation's bulk power system. Section 215 requires the Commission to certify an electric reliability organization or ERO that is responsible for proposing FERC Commission review and approval, reliability standards or modifications to existing reliability standards help protect and approve the reliability of the nation's bulk power system. The Commission certified the North American Electric Reliability Organization or North American Electric Reliability Corporation, or NERC, as the ERO. Section 215 of the Federal Power Act provides stakeholder input in the ERO's development of reliability standards for a bulk power system. This process works relatively well to develop standards to address traditional operations and planning related reliability events that may cause grid failures or blackouts such as from improper vegetation management or failures associated with the operation of protective equipment.

The nature of national security threats by adversaries intent on attacking our nation's electric grid significantly differ from the reliability of vulnerabilities that have caused regional blackouts and reliability failures that we have faced in the past. Widespread disruption of electric service can quickly undermine the U.S. Government, its military and the economy, as well as endanger the health and safety of millions of our citizens. To help mitigate these advanced, persistent and rapidly evolving threats, the Commission uses a two-pronged approach regarding grid reliability employing mandatory reliability standards to establish foundation of practices while also working collaboratively with the industry, with states and other federal agencies to identify and promote best practices.

While NERC reliability standards are the foundation of the Commission's work to address cybersecurity, there are additional measures that can and should be taken to further improve industry's cybersecurity posture in light of these rapidly evolving threats. That is why the Commission established our office, or OEIS. OEIS partners with industry, states and federal agencies to develop and promote best practices for critical infrastructure security. Working with these organizations, OEIS helps identify new and emerging

threats, inform the private sector of them and then assist with mitigating action. One example of OEIS' work is that we conduct voluntary architectural assessments of utility computer networks, reviewing everything from the configuration of legacy equipment to the application of state-of-the-art protection systems. Another example is OEIS works with the Office of the Director of National Intelligence and the Department of Energy, specifically CESER, to conduct briefings and exchange information with state and industry officials about the current threats industry is facing and what can be done to address them. More broadly, OEIS works with the NERC Electricity Information Sharing and Analysis Center (E-ISAC) to rapidly issue bulletins and alerts informing industry of specific vulnerabilities and threats as well as best practices that can defend against them. And as a final example, OEIS assists with the planning and execution of tabletop exercise and participates in joint security programs with other government agencies. In fact, just last week, OEIS assisted the National Guard units and participating utilities in the New England states to conduct Cyber Yankee, a simulated cyberattack on utility networks. Exercises such as this are critical to maintaining readiness and ensuring our ability to respond to cybersecurity events.

In conclusion, cybersecurity threats pose a serious risk to the bulk power system and its supporting infrastructures that serve our nation. These are complex, persistent and fast-evolving issues. Therefore, the Commission has adopted this two-pronged approach to best address the important security matters. Thank you again for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Mr. McClelland follows:]

Testimony of Joseph McClelland
Director, Office of Energy Infrastructure Security
Federal Energy Regulatory Commission
Before the Committee on Energy and Natural Resources
United States Senate
August 5, 2020

Testimony

Chairman Murkowski, Ranking Member Manchin and Members of the Committee:

Thank you for the privilege to appear before you today to discuss potential threats to the bulk power system in the United States. My name is Joe McClelland, and I am the Director of the Office of Energy Infrastructure Security at the Federal Energy Regulatory Commission (Commission). I come before you as a Commission staff witness, but I should note that my remarks do not necessarily represent the views of the Commission or any individual Commissioner.

I'd like to begin today by briefly describing the Commission's work regarding the reliability and security of the bulk power system. I'll then describe the Commission's two-pronged approach to these issues. This approach includes, first, our role in establishing and enforcing mandatory reliability standards (or standards), which are administered by the Commission's Office of Electric Reliability. The second prong of the Commission's approach is our role in addressing advanced, persistent threats with best practices and mitigation mechanisms by partnering with other federal agencies, the states and the industry on a collaborative basis. The Commission's Office of Energy Infrastructure Security, or OEIS, is charged with oversight of this second prong.

In the Energy Policy Act of 2005 (EPAct 2005) -- specifically through section 215 of the Federal Power Act (FPA) -- Congress entrusted the Commission to approve and enforce mandatory reliability standards for the nation's bulk power system. Section 215 requires the Commission to certify an Electric Reliability Organization (ERO) that is responsible for proposing, for Commission review and approval, reliability standards or modifications to existing reliability standards to help protect and improve the reliability of the nation's bulk power system. The Commission certified the North American Electric Reliability Corporation (NERC) as the ERO.

The reliability standards apply to the users, owners and operators of the bulk power system and become mandatory in the United States only after Commission approval.

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

Section 215 of the Federal Power Act provides for stakeholder input in the ERO's development of reliability standards for the bulk power system. Consistent with the FPA, NERC uses an accredited process, approved by the American National Standards Institute, which is intended to develop consensus among stakeholders on both the need for, and the substance of, a proposed standard. This process works relatively well to develop standards to address "traditional" operations and planning-related reliability events that may cause grid failures or blackouts, such as from improper vegetation management or failures associated with the operation of protection equipment.

The nature of the national security threats by adversaries intent on attacking our nation's electric grid significantly differ from the reliability vulnerabilities that have caused regional blackouts and reliability failures we faced in the past. Widespread disruption of electric service can quickly undermine the U.S. government, its military, and the economy, as well as endanger the health and safety of millions of citizens. These threats originate from a variety of new and quickly emerging sources, such as from supply chain compromises, insider attacks, targeted phishing attempts, ransomware campaigns, internet-of-things vulnerabilities, and many more.

To help mitigate these advanced, persistent, and rapidly-evolving threats, the Commission uses a two-pronged approach with regard to grid reliability: employing mandatory reliability standards to establish foundational practices while also working collaboratively with industry, the states and other federal agencies to identify and promote best practices.

For instance, regarding mandatory reliability standards, the Commission has approved Critical Infrastructure Protection, or "CIP" Reliability Standards, to establish a baseline to address such critical and fundamental matters as security

management controls, protection of removable media, patch management, personnel training, and cyber incident reporting. These Reliability Standards are updated over time to address emerging issues. As one example, the Commission modified the CIP Reliability Standards in 2018 to help address supply chain risk management for cyber assets. The supply chain risk management standards are scheduled to take effect before 2021.

While the NERC CIP Reliability Standards are the foundation of the Commission's work to address cybersecurity, there are additional measures that can and should be taken to further improve industry's cybersecurity posture in light of these rapidly-evolving threats. That is why the Commission established OEIS.

OEIS partners with industry, states and other federal agencies to develop and promote best practices for critical infrastructure security. Working with these organizations, OEIS helps identify new and emerging threats, inform the private sector of them, conduct voluntary cybersecurity assessments, and then assists with mitigating actions. I would like to provide you with a few examples of the work OEIS does for the Commission. One example of OEIS's work is that OEIS conducts voluntary architecture assessments of interested Commission-jurisdictional utilities' computer networks that control the operations of their facilities. Conducted onsite, these assessments are specific to the organization, reviewing everything from the configuration of legacy equipment to the application of state-of-the-art protection systems.

Another example is OEIS works with the Office of Director of National Intelligence, specifically the National Counterintelligence and Security Center, to conduct briefings and exchange information with state and industry officials about the current threats industry is facing and what can be done to address them. More broadly, OEIS works with the NERC Electricity Information Sharing and Analysis Center to rapidly issue bulletins and alerts, informing industry of specific vulnerabilities and threats as well as best practices that can defend against them.

And as a final example, OEIS assists with the planning and execution of table-top exercises and participates in joint security programs with other government agencies. In fact, just last week OEIS assisted the National Guard units and participating utilities in the New England states to conduct Cyber Yankee, a simulated cyber-attack on utility system networks. This exercise helped the utilities and National Guard units to prepare for these threats including practicing government assistance to the utilities as part of the defense and recovery efforts. Exercises such as this are critical to maintaining readiness and ensuring our ability to respond to cybersecurity events.

In conclusion, cybersecurity threats pose a serious risk to the bulk power system and its supporting infrastructures that serve our nation. These are complex, persistent, and fast-evolving issues. They won't be solved easily, and they require a great deal of coordination and communication. Therefore, the Commission has adopted this two-pronged approach to best address the important security matters. In addition, to effectively address these threats, the Commission will continue this important work with our federal, state, and industry partners on a collaborative basis.

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

The CHAIRMAN. Mr. McClelland, thank you for that. We appreciate it.

Let's next go to Mr. Conner from Siemens Energy. Mr. Conner, welcome.

STATEMENT OF STEVEN C. CONNER, PRESIDENT, SIEMENS ENERGY, INC.

Mr. CONNER. Thank you, Chairwoman Murkowski, Ranking Member Manchin and members of the Committee, thank you for the opportunity to testify today. My name is Steve Conner. I'm the President of Siemens Energy, Inc., which is the U.S. regional entity of Siemens Energy. We have more than 11,000 employees in the U.S. supporting the country's grid operations at 21 power equipment and manufacturing service and innovation sites. Our headquarters is located in Orlando, Florida. The United States is our company's largest market worldwide, and Siemens Energy equipment provides secure, resilient technologies that support one-third of America's total daily energy needs. We have been working with our customers on solutions for the evolving demands of industry and society for more than 150 years. We have been a partner to the United States Government, America's energy producers and its energy providers for decades. We have a deep understanding of the safest and most resilient infrastructure technologies and processes necessary to secure one of our most essential national assets, America's power grid.

Industrial cybersecurity is at the core of our Siemens Energy business. Our products and solutions have industrial security functions that are built in by design and turned on by default. They support the secure operation of plants, systems and machines and networks of our customers. We use this experience and expertise to establish partnerships that advance cybersecurity efforts. I would like to share with you some example of those collaborations with both the public and private sectors.

In 2018, we created the Charter of Trust which is now a leading global initiative of companies and organizations focused on securing critical infrastructure. We're a founding member of the Energy Cybersecurity Alliance, a partnership of energy companies, manufacturers and service providers. We have a dedicated team of seasoned security experts which we call our ProductCERT team that manages the receipt, investigation, internal coordination and public reporting of security issues related to the Siemens products solutions and services. Any vulnerabilities discovered are shared with our governmental partners. And just last week, the New York Power Authority (NYPA) and Siemens Energy announced a new collaboration to develop an industrial Cybersecurity Center of Excellence. It will bring the public and private sectors together to develop innovative cybersecurity best practices that will serve as a model for deployment at other utilities. This first of its kind Industrial Cybersecurity Monitoring Research and Innovation Center will focus on detecting and defending against cyberattacks on critical infrastructure owned and operated by NYPA, the largest state-owned electric utility in the nation. Successful solutions have potential to be deployed and commercialized at other public and pri-

vate organizations that operate critical infrastructure across the U.S.

Supply chain security is just as important as cybersecurity. By ensuring the security of our supply chain, we enhance the reliability, security and resilience of America's energy infrastructure. This depends on close collaboration and involvement with our customers, partners, suppliers and governments around the world to secure for our supply chain. Some examples of our supply chain security policies and best practices include a supply chain management standard that performs regular supplier audits to address technical, commercial and cybersecurity risks and opportunities. We manage, track and control access to confidential data, chronic development and source code, both physically and virtually. We don't share any overall product development information with the suppliers. And utilizing select components from qualified suppliers only, which includes testing their hardware, software and security, only then including them in an approved components database. And lastly, we perform civil, criminal and governmental-sanctioned background checks as necessary.

As you can see, Siemens Energy takes its responsibility to secure our country's critical energy infrastructure by collaborating with the public and private sector very seriously. We are constantly looking for additional ways to engage the public sector, including supporting vendor-driven forums that would improve industry involvement and promote wider discussion on the vulnerabilities and supply chain risks.

Thank you again for inviting me to testify, and I, along with the 11,000+ U.S. employees of Siemens Energy, look forward to the continued collaboration necessary to "keep the lights on" in the U.S. energy infrastructure.

[The prepared statement of Mr. Conner follows:]

Statement of Steven C. Conner
President
Siemens Energy, Inc.

United States Senate
Committee on Energy and Natural Resources

An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives

Wednesday, August 5, 2020

Introduction

Chairman Murkowski, Ranking Member Manchin, and Members of the Committee, thank you for the opportunity to testify today. I look forward to sharing the views of Siemens Energy on industry efforts to improve collaboration on various cybersecurity and critical infrastructure protection initiatives with the energy sector.

My name is Steve Conner, President of Siemens Energy, Inc., the U.S. regional entity of Siemens Energy. We have more than 11,000 employees in the United States supporting the country's grid operations at 21 power equipment manufacturing, service and innovation sites. Our headquarters is in Orlando, FL. The United States is our company's largest market worldwide, and Siemens Energy equipment provides secure, resilient technologies that support one-third of America's total daily energy needs.

Siemens Energy has been a reliable partner to the United States government, America's energy producers and its energy providers for decades. We have a deep understanding of the safest and most resilient infrastructure technologies and processes necessary to secure one of our most essential national assets, America's power grid. I appreciate the opportunity to share with you our cybersecurity and supply chain management expertise and how collaboration on these issues, both within our own company and with the public and private sector, is critically important in our efforts to help secure our nation's energy infrastructure.

Siemens Energy Overview

Siemens Energy is the global energy business of the Siemens group, which has been working with its customers on solutions for the evolving demands of industry and society for more than 150 years. With planned stock listing, Siemens' energy business will operate independently as Siemens Energy in the future.

It will offer broad expertise across the entire energy value chain, along with a comprehensive portfolio for utilities, independent power producers, transmission system operators, the oil and gas industry, and other energy-intensive industries. With its products, solutions, systems, and services, Siemens Energy will address the extraction, processing, and transport of oil and gas as well as power and heat generation in central and distributed thermal power plants, and power transmission and technologies for the energy transformation, including storage and sector-coupling solutions. The majority stake in Siemens Gamesa Renewable Energy will round out its future-oriented portfolio. With its commitment to leading the way in decarbonization of the global energy system, Siemens Energy will be a partner of choice for companies, governments, and customers on their path to a more sustainable future. With approximately 90,000 employees worldwide, Siemens Energy will help shape the energy systems of today and tomorrow.

As a highly experienced partner and advisor, we will enable our customers to achieve their ambitious goals and will actively assist them on their way to a more sustainable future – no matter where they are in their journey at the moment. That's because the transformation of the energy sector will be starting out from a wide range of different points and will proceed at different speeds – depending on individual countries' economic development and political agendas, as well as their access to energy sources. Accordingly, we will deploy the entire range of our products, solutions and services to shape this transformation together with our customers and partners. Step by step, but consistently and in the right direction. This requires the courage to accept interim solutions, such as increased efficiency or the use of clean fuels.

In this sense, we see ourselves as the partner of choice for government, business and society. Together, we energize society worldwide, and thus enable successful and sustainable growth. That is our promise and our purpose.

Industrial Cybersecurity and Siemens Energy

Industrial cybersecurity is at the core of Siemens Energy's business. We have pioneered cyber solutions to meet the rapidly evolving needs of the utility industry by enhancing visibility, monitoring, and asset management capabilities across critical and energy infrastructure networks. Our products and solutions have industrial security functions that are built-in by design and turned on by default. They support the secure operation of plants, systems, machines, and networks by our customers.

The energy sector has become a primary target for cyber attacks. In this environment, owners and operators need to be certain that cybersecurity solutions will meet the need for operational technologies (OT). Siemens Energy has worked to develop OT-native cybersecurity for the energy sector with the insights gained from long experience developing equipment and weathering attacks ourselves.

In strengthening their cyber defenses, we navigate our customers through the complex relationship between their information technology (IT) and operational technology (OT) environments. We deliver clarity and focus to help our customers make better decisions. We keep our customers safe with our in-depth market knowledge and comprehensive set of solutions along the full value chain.

Cybersecurity Leadership through Collaboration and Information Sharing

Siemens Energy leverages its experience and expertise by establishing partnerships that advance cybersecurity efforts outside of its own walls in the U.S. and beyond. I would like to share with you some examples of those collaborations with both the public and private sectors.

Charter of Trust. Siemens is a leading contributor in the industry push toward continually advancing cybersecurity. In 2018, at the Munich Security Conference Siemens brought together global organizations to create the Charter of Trust – an initiative to build a foundation for a more secure digital world with a focus on the critical infrastructures essential for national functions. Today, its members have transformed it into a unique initiative of leading global companies and organizations working together to make the digital world more secure. For example, the initiative has been driving this by establishing, piloting and adopting global baseline cybersecurity requirements and concepts.

Energy Cybersecurity Alliance (ECA). Siemens Energy is a founding member of the Energy Cybersecurity Alliance (ECA), a partnership formed to enhance the security and resiliency of the North American energy grid by providing a forum for energy companies and service providers, manufacturers and suppliers of equipment and software to discuss and share potential safety and security-focused solutions.

Siemens ProductCERT. The sharing of information across industry and with the government happens via our ProductCERT team – a dedicated team of seasoned security experts that manages the receipt, investigation, internal coordination, and public reporting of security issues related to Siemens products, solutions, or services. ProductCERT cultivates strong and credible relationships with partners and security researchers around the globe to advance Siemens product security, to enable and support development of industry best practices, and most importantly to help Siemens customers manage security risks.

Cyber Emergency Response Team (CERT) Collaboration. Our product security teams maintain a strong collaboration with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) run by the Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security. This collaboration includes pre-release of our Siemens Security Advisories subject to a non-disclosure agreement. A listing of these advisories disclosing vulnerabilities concerning Siemens products is available dating back to 2011. Siemens has direct contact with 535 teams/CERTs worldwide with 98 of them in the United States that also may be notified in advance. This network allows for the globally coordinated release of information to all stakeholders.

ISACs/ISAOs. For applicable products/industry, Siemens Energy participates in select sector-based Information Sharing and Analysis Centers (ISACs) and the Information Sharing and Analysis Organizations (ISAOs) established by the Department of Homeland Security. Siemens Energy maximizes its engagement with ISACs /ISAOs by leveraging experts across our organization. Siemens Energy is constantly looking for additional ways to engage the public sector, including supporting vendor-driven forums that would improve industry involvement and promote wider discussion on vulnerabilities and supply chain risks.

Cybersecurity Partnership with NYPA. And just last week, the New York Power Authority (NYPA) and Siemens Energy announced a new collaboration to develop an industrial cybersecurity Center of Excellence. The partnership is intended to bring the public and private sectors together in order to develop innovative cybersecurity best practices that will serve as a

model for deployment at other utilities. The first-of-its-kind industrial cybersecurity monitoring, research and innovation center will focus on detecting and defending against cyberattacks on critical infrastructure owned and operated by NYPA, the largest state-owned electric utility in the nation.

The announcement is the first step in bringing together a coalition of public sector, private industry and academic partnerships that will build core capabilities needed to identify new and existing cyber threats, adopt new technologies to protect digital infrastructure and close the industry's talent-gap. Successful solutions have the potential to be deployed and commercialized at other public and private organizations that operate critical infrastructure systems in the state of New York and beyond.

Working Together to Secure the Supply Chain

To secure our supply chain Siemens Energy depends on close collaboration and involvement with our customers, partners, suppliers, governments, and standards bodies around the world. I would like to share some of our supply chain security policies and best practices to give the Committee a better understanding of the steps Siemens Energy takes to secure America's energy infrastructure.

Supply Chain Management and Risk Assessment Processes. As part of the Siemens Supply Chain Management (SCM) Standard, all suppliers are evaluated and qualified with respect to a supply chain risk management process. This process aims to safeguard and consistently improve strategic supplier performance by ensuring that the potential of our best and most innovative suppliers is utilized in full. Regular supplier audits are an active part of Siemens' governance of our vendors. Evaluations address technical, commercial, and cybersecurity risks and opportunities.

Binding Cybersecurity Requirements for Suppliers in All New Contracts. We have standard contract language with dedicated sections to address cybersecurity in the supply chain to ensure that related organization, processes, physical and information assets used for design, development, manufacturing and distribution of deliveries conform to applicable standards, such as ISO/IEC 27001, ISA/IEC 62443, ISO 27034, NIST 800-series, NERC CIP or similar.

Secure Access to Data, Product Development and Source Code: Siemens has research, product development, and manufacturing facilities located in multiple countries. These facilities are protected using a defense-in-depth approach that uses both physical and IT-based access controls to protect Siemens assets. We decide where to deploy Siemens technology (e.g. source code, research, manufacturing, etc.) based upon the security level of the organization that will use it. Access to confidential and strictly confidential information is carefully managed, tracked and controlled. Unless required as part of a co-development process with a supplier, Siemens does not share overall product development information with suppliers.

Vulnerability Testing for Components. Our project teams select components from qualified suppliers and review its technical qualifications. The supplier's components are further checked as part of the respective hardware, software, and security testing required by the applicable development process. Pilot builds are carefully reviewed by engineering and initial production units go through a thorough inspection and test process prior to final release. Test results and vulnerability information are aggregated into an approved components database.

Vulnerability Monitoring of Components. We constantly monitor the vulnerability information and potential security issues of the suppliers' components that become part of our products. We use multiple information sources or vulnerability information providers such as the NIST National Vulnerability Database. In the event security issues are identified, corrective action is taken, including disqualification of suppliers. IT Security requirements are cascaded to suppliers through contractual terms.

Asset and Services Classification. Siemens Energy conducts an Asset Classification Process based on the ISO/IEC 27001 standard on information and technology assets and services utilized to develop, manufacture, engineer and/or deliver products and services. The Asset Classification Process defines the security level based on a risk assessment, which results in various methods applied to protect the assets or services at an appropriate level. Additionally, Siemens Energy applies a threat and risk analysis that is based on ISA/IEC 62443 and ISO/IEC 27005 to our product portfolio.

Personnel Risk Assessment. For other products that apply, Siemens Energy complies with the NERC CIP-004-6 standard for personnel risk assessment during the on-boarding process and adheres to customer security policies and procedures prior to accessing assets at customer locations. Siemens performs civil, criminal, and government-sanction background checks for both installation and maintenance personnel where required.

Security During Installation. To secure our products during installation, Siemens Energy provides information regarding the secure configuration of the applicable products and systems within the Operational Guidelines for Industrial Security and by following the recommendations in the product manuals. This provides the capability for the systems integrator and asset owner to support multiple policies and practices as required. Siemens Industrial Security Services can also contribute expertise and support including security consulting, implementation and optimization.

Existing Standards and Established Best Practices. Siemens Energy participates in different standards organizations and has selected as a guiding security standard ISO/IEC 27001 and ISA/IEC 62443 to enhance the protection of our hardware, firmware, and software. We consult with other standards (e.g. IEC 62351, NIST 800 series, NERC CIP, etc.) depending upon the critical infrastructure or vertical market where our products are applied, including IEC 62351 for the energy sector. Where applicable supply chain risk management is recommended to follow the ISO/IEC standards that address supplier risk management, contractual requirements, policies, qualification and monitoring.

Penetration Testing. The independent Siemens Corporate Technology department conducts penetration testing on products that often comprise enterprise systems. This information is provided as a report back to the requesting project manager. Penetration test results requiring follow-up actions are recorded in an issue management system where they are tracked to resolution. Siemens also has an internal audit department with a team for products and solutions testing. They also perform component and penetration testing of enterprise systems.

Vulnerability Detection and Mitigation. Any vulnerability identified by an internal or external party is treated equally according to its criticality. Siemens investigates and reproduces the vulnerability upon receiving the report. Siemens handles the vulnerability in collaboration with the responsible development groups. After the issue is successfully analyzed and handled

and if a patch is necessary to resolve the vulnerability, corresponding updates are developed and prepared for distribution. Siemens will notify the customer directly or publicly release a Siemens Security Advisory with information on the vulnerability and corresponding mitigation measure.

Conclusion

Siemens Energy takes its responsibility to secure our country's critical energy infrastructure very seriously. We do this by collaborating with the public and private sector. I hope the sharing of our current supply chain security and cybersecurity efforts will further strengthen the solid partnerships already in place and create new opportunities to collaborate. We all need to work together to "keep the lights on" in America.

Thank you for the opportunity to present the views of Siemens Energy today. I look forward to answering any questions that you may have.

The CHAIRMAN. Thank you, Mr. Conner. We appreciate your time before the Committee this morning.

Finally, let's go to Mr. O'Brien with PJM Interconnection.

STATEMENT OF THOMAS O'BRIEN, SENIOR VICE PRESIDENT AND CHIEF INFORMATION OFFICER, PJM INTERCONNECTION, L.L.C.

Mr. O'BRIEN. Chairman Murkowski, Ranking Member Manchin and Committee members, thank you for the opportunity to speak to you today on this critical topic. I appreciate the opportunity to represent PJM. I also appreciated the opening comments from the Chairwoman and some of the things that she covered specifically around the Energy Information Protection Act which is something that's very important to us at PJM and the industry.

I'd like to thank my fellow panelists for their insights and contributions. I've worked with some of them in the past, and I really appreciate everything that you do.

My written testimony covered a broad range of topics, including PJM's current approach to managing cybersecurity, partnership and collaboration, cybersecurity supply chain considerations, workforce and training and longer-term considerations. In my brief remarks, I will build off of some of the key points from my fellow panelists and leave you with three things for consideration and let the written testimony speak for itself.

First, and this was highlighted by everybody, is collaboration and partnership is essential between and amongst government, industry and our service providers. It is essential and no one can do it by themselves. I'd like to share a couple of examples. DOE and DHS lead the charge on both classified and non-classified briefings, and this is critical to industry for managing priority and risk management. The Electric ISAC, which is part of NERC, is the hub of information sharing for the electric industry. They continue to evolve their information sharing programs and the industry relies on that significantly. The E-ISAC coordinates the cyber risk information sharing program which is just one way to get intelligence on what the adversaries are doing. DHS has a program for sharing threat indicators with industry and something that we use at PJM.

I'd like to echo some of what Joe McClelland said. We work with FERC on things like risk management, best practices, and we appreciate their support. And again, I would emphasize the importance of protecting critical information, which again, was highlighted in the opening by Chairwoman Murkowski.

Now let's talk about compliance for a second. Just because the electric industry is on the forefront of compliance, NERC sets standards but they don't do it blindly. They do it with industry engagement, and regional entities lead the audit process which essentially drives transparency and allows for consistency. I also wanted to speak to just one example that PJM is involved with around fuel security. We're looking at a phase three fuel security study at the moment. It's looking at major interstate pipelines, modeling, both physical and cyber scenarios and we've had great support from DOE, from FERC, and we'd like to thank them for that.

The second takeaway that I'd like to leave with you is that risk management must be informed by clear understanding and appre-

ciation of the adversary is informed by threat intelligence, likelihood on impact and requires adequate investments. On October 1st of 2020, the NERC cybersecurity supply chain management standard will go into effect. That's an excellent starting point for advancing controls to mitigate risks and associated threats, and I'm sure that will continue to evolve. Previously mentioned, we're looking at the impact of the Executive Order and that has potential sweeping and broad implications for the procurement of electrical equipment as well as legacy equipment. And while ISOs and RTOs do not own the assets, the order will have significant operational planning and marketing impacts. Consistent with the feedback from Bruce Walker from DOE, we agree that it should be a surgical approach.

The final point that I'd like to leave you with is that metrics and key performance indicators are critically important to security operations. You can't improve what you don't measure, and you need to establish key targets so you can see how your progress is going. That will allow you to focus on transparency and continued recruitment.

I'd like to thank you for the opportunity to appear before this Committee. I look forward to your questions, and I appreciate the opportunity to leave you with my three takeaways: collaboration and partnership between government, industry and our service providers is essential and no one can do this alone; risk management must be informed by clear understanding, appreciation of the adversary; and finally, metrics and KPIs are necessary for a clear security operating picture. Thank you for this opportunity.

[The prepared statement of Mr. O'Brien follows:]

United States of America
Senate Energy and Natural Resources Committee
Full Committee Hearing to Examine Efforts to Improve Cybersecurity for the Energy Sector

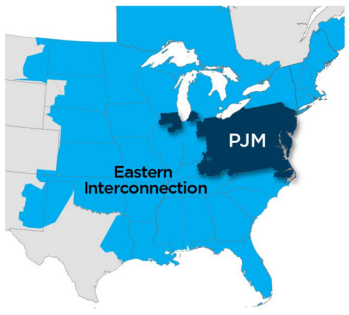
Testimony of Thomas O'Brien, Senior Vice President and Chief Information Officer
PJM Interconnection, L.L.C.
August 5, 2020

For Public Use

Thank you for the opportunity to testify before this Committee on efforts to improve cybersecurity within the energy sector.

My name is Tom O'Brien, Senior Vice President and Chief Information Officer for PJM Interconnection. I appreciate the opportunity to appear before this committee as a representative of PJM. As a reminder, PJM is the regional transmission organization (RTO) serving all or parts of the states of Illinois, Indiana, Michigan, Ohio, Kentucky, Tennessee, West Virginia, North Carolina, Virginia, Maryland, Delaware, Pennsylvania, New Jersey as well as the District of Columbia.

Key Statistics	
Member companies	1,040+
Millions of people served	65
Peak load in megawatts	165,563
MW of generating capacity	186,788
Miles of transmission lines	84,236
2019 GWh of annual energy	787,307
Generation sources	1,446
Square miles of territory	369,089
States served	13 + DC



As a regional transmission organization, we ensure the reliability of the grid in our footprint, operate electricity markets and plan the expansion of the grid. We also have a critical role to play in ensuring the cybersecurity of the grid, as I will explain below.

I serve as the CIO of PJM. In this role, I am responsible for all activities related to PJM's Information Technology Services Division and its Enterprise Information Security with a key focus on security operations, Critical Infrastructure Protection (CIP) compliance, software development, architecture, infrastructure operations and production support in all facets of information technology and cybersecurity.

Prior to joining PJM, I was employed by GPU Energy and First Energy. In those roles, I led and participated in deregulation, energy trading, retail sales and marketing, system operations and information technology activities.

In my testimony today, I want to cover a few topic areas:

- A high-level overview of PJM's approach to addressing cybersecurity threats to the grid
- How we work with other industry players and our federal partners on information sharing, testing and addressing cybersecurity threats to the grid
- Our coordinated efforts with the other RTOs and the industry as a whole to address supply chain issues from foreign adversaries
- Workforce and training
- The next generation of issues we as RTOs and our federal partners seek to address

PJM takes cybersecurity very seriously, and it is critically important to fulfilling our mission of reliably serving 65 million people. There are many risks facing the electric power grid, and it is core to our mission to prioritize and focus on the highest risks.

PJM's Approach to Addressing Cybersecurity Threats to the Grid

PJM utilizes the Cybersecurity Framework, developed by the National Institute of Standards and Technology, as our approach to managing cybersecurity. The framework focuses on the principal functions to identify, protect, detect, respond and recover. Cybersecurity best practices begin with protecting our assets, detecting bad actors, responding to events and recovering from events. We establish key performance indicators (KPI's) and metrics for each of the principal functions. We utilize metrics that allow us to measure the life cycle of an attack. In simple terms, we look at measures for each phase of an attack, from adversaries scanning our external environment looking for vulnerabilities, to all the way through exploiting vulnerabilities and taking action. You cannot control the reconnaissance that an adversary is doing, but you can control the layers of defense and the action you take to avoid or mitigate a breach.

The KPIs and metrics begin with risk management. Like managing any risk, understanding and getting visibility to the threats are important. Threat information is critical to managing and preventing breaches and is foundational to prioritizing daily operations.

PJM and the electricity industry have a great start through industry compliance efforts, which focus on best practices. The CIP standards provide a strong baseline for protecting and defending our critical assets.

Incident response for cyber and physical events has been a high priority of the electricity subsector and has resulted in a number of vital efforts that have prepared us for coordinated response to high-consequence events. One of the

most important programs that the electricity industry has engaged in is the NERC GridEx program. This program exercises extreme events occurring across multiple electricity utilities, and includes both cyber and physical injects. It exercises coordination between utilities, the Electricity Information Sharing and Analysis Center (E-ISAC), and participating state and federal government entities. Lessons learned from these exercises improve the ability of utilities and government entities to work through unforeseen future events by having ready plans that have been tested through hypothetical, extreme scenarios. PJM also performs drills with the members in our footprint, building off the NERC GridEx experiences. Incident response is critical and requires preparation and practice.

How We Work With Other Industry Players and Our Federal Partners on Information Sharing, Testing and Addressing Cybersecurity Threats to the Grid

Partnership and collaboration are essential to any cybersecurity or physical security program. The importance of working across the industry, and with our state and federal government partners – and even across other critical infrastructures like telecom, finance, water and gas – to share threat information and best practices cannot be overstated. Threat intelligence and learning from others in relation to threats and prevention is critical to managing any cybersecurity program.

PJM continues to advance the security and resilience of our system through engagement with industry and government efforts, as well as internal work designed to address a variety of challenges. PJM has supported initiatives such as the North American Transmission Forum (NATF) Spare Tire Project, the ESCC Resilient Communications Working Group (RCWG), Cyber Mutual Assistance (CMA), the Department of Energy North American Energy Resilience Model (NAERM), and the Defense Advanced Research Projects Agency (DARPA) RADICS program. All of these are examples of mechanisms to improve the security and resilience of the grid through industry and government collaboration on topics of shared interest.

Our government partners do a great job of sharing threat information as appropriate. We rely on our government partners to share relevant information that we can use to protect our systems. The Electricity Information Sharing and Analysis Center (E-ISAC) is the hub of information sharing for the electric industry and continues to evolve its information-sharing programs. In addition, we receive threat indicators from the Department of Homeland Security and government-informed analysis from the Cyber Risk Information Sharing Program (CRISP).

Our industry relies on the leadership of the DOE to coordinate both classified and unclassified briefings to keep the industry informed on the threat landscape. These briefings are important to supporting risk management programs and establishing priorities. DOE and the National Laboratories have been instrumental in cybersecurity research. The ESCC Research & Development Committee hosted a National Lab roundtable in 2019 that included all of the National Labs and industry participants highlighting cybersecurity and resilience research. Advancing that research to the private sector through technology transfer programs is an important next step.

NERC and the regional entities continue to work with the industry to improve our compliance programs and fully support industry engagement in the development and evolution of standards. NERC sets standards to improve our

security fundamentals, and the audit process helps to drive transparency and consistency in meeting our security requirements.

PJM works with FERC to look not only at compliance, but also, through the Office of Energy Infrastructure Security (OEIS), PJM has collaborated on best practices in cybersecurity to help combat nation-state threats.

The Department of Defense looks at the electricity subsector as vital to its mission of national defense. As a result, technology transition programs that make cyber defensive tools and technologies available to private industry have proven to be helpful and have promoted positive public/private partnerships.

PJM continues to work with the DOE on fuel security. At PJM, we also recognize that the security of fuel supply chains that support the generation of electricity are critical to ensuring a strong physical and cybersecurity environment. We have been working with the major interstate pipelines that serve electric generation in our footprint on modeling both cyber and physical scenarios as part of our Fuel Security Phase III analysis. Although the analysis is still underway, I do want to recognize the great support we have had from each of the federal agencies that have a role in this process, including FERC; the DOE; the Transportation Security Administration (TSA), which oversees cybersecurity of the interstate pipeline system; and PHMSA, which also is charged with overseeing pipeline safety and security.

Our Coordinated Efforts With the Other RTOs and the Industry as a Whole to Address Supply Chain Issues From Foreign Adversaries

The current version of the NERC Cybersecurity Supply Chain Risk Management standard will go into effect on Oct. 1, 2020. This standard provides an excellent starting point for advancing controls to mitigate the risks associated with threats and vulnerabilities in the supply chain. Through the ISO/RTO Council, the nine North American ISOs worked together to provide joint feedback to the standard. NERC has fully supported industry engagement and feedback in the development and evolution of this standard.

Supply chain standards and best practices need to evolve continuously. The breadth and depth of the supply chain creates unique and significant challenges. Coordinated and prioritized actions between industry and government are critical success factors. Reliable and secure supply chain management will require broad cross-sector engagement, broad government engagement and a significant shift in how vendors and service providers deliver products and services to substantially mitigate supply chain risks. There is a role for our government partners to provide clear direction about vendors who put national security at risk. Additionally, the DOE and other government partners are in a position to develop testing and certification programs and will need to find the balance between government programs and competitive third-party programs.

A key success factor in security supply management is to ensure an equitable allocation of liabilities and costs. Eventually, vendors and service providers will differentiate themselves by how well they manage cybersecurity risks and meet these customer needs in a fair and responsible manner. While the differentiation will come at a cost, it is likely that market share and revenue will increase for vendors and service providers that lead with excellence in cybersecurity.

The recent executive order on supply chain has the potential for sweeping and broad implications to the procurement of electrical equipment for critical transmission, generation and control systems used to operate the bulk power system. The executive order also has potential implications for legacy equipment and technology installed in the field. While the ISO/RTOs do not own many of the electric assets, the order could have significant operational, energy market and planning implications. Consistent with the feedback from Bruce Walker, Assistant Secretary for the Office of Electricity (OE) at the U.S. Department of Energy (DOE), PJM agrees that a surgical approach to the executive order must be utilized.

We should carefully establish a scope that will allow the DOE and the electric industry to be successful. Industry and government should establish the process for identifying the critical bulk power assets that are the most vulnerable, focusing on the subset of devices and technology that present the greatest risks. From a cybersecurity perspective, it will also be important to assess the compromise of less critical equipment that may allow lateral movement to more critical equipment. In some cases, it will be the equipment with the least protection that will become the entry point. We will need better architectures and protocols that protect our most critical assets and prevent compromise by attacks from less secure equipment.

Additionally, we should work collaboratively to ensure the security of critical information shared between industry and government partners. Along these lines, we and many other utilities with CEII information, have continued to urge our regulators to view the dissemination of CEII on a 'need to know' basis with an adequate demonstration of that need.

Workforce and Training Issues

The future success on the electricity industry depends on the development and leadership of the next generation of utility employees, including cybersecurity analysts. Even as the threat landscape transforms and we achieve advances through automation, machine learning and artificial intelligence, it will be imperative to develop that next generation of cybersecurity expertise.

Collaborating with academia at all levels is an important step to addressing the long-term workforce and training issue for the electric industry. Participation in local communities focusing on Science, Technology, Engineering and Math (STEM) is just one way to do that. Introducing students to the electric industry and our critical role in supporting society and sharing our critical mission can motivate future employees. Internships with universities serve as another opportunity to introduce future workers to the industry before they make long-term career choices.

It is also important to ensure that we can retain employees and support the development of new skills as the industry continues to transition. We are finding that by investing in the early careers of recent college graduates through our rotational development programs, we are building the next generation of the cybersecurity workforce. Public and private partnerships that foster training and collaboration will also help to strengthen the private industry workforce.

We must value diversity and inclusion in the workplace. Not only is it the right thing to do, but the business case is clear that people with different backgrounds and experiences will drive competitive advantage leading to better solutions. This focus and priority will support attracting and retaining top talent and utilizing significant untapped potential.

The Next Generation of Issues We as RTOs and Our Federal Partners Are Seeking to Address

We need to continue to build on the momentum that industry and government have already achieved in protecting the nation from adversaries. We need to strike the right balance, including: i) understand the nature of the threats including risks and likelihood; ii) leverage and expand mitigating controls and positive actions underway; iii) identify new key focus areas for new actions based on risks and gaps; and iv) further develop relationships between the electricity sector and other critical infrastructures.

As we look forward, the protection of our nation's critical infrastructure must continue to evolve. We must capitalize on the strengths of government and industry partners with clearly defined roles that allow for a powerful force of teamwork. Management of cybersecurity will need to adapt to changes on the electric grid, including the increased focus on distributed technology. Distributed technology introduces a large attack surface for adversaries, and we must plan and prepare for that.

Innovation will continue to fuel the electric grid and the Internet of Things (IoT) creates tremendous opportunity and interconnectedness of devices leading to creative solutions. It will be important to consider the operational and security impacts that come with the integration of heterogeneous devices. Sensor technology has opened the door for increased automation with less human interaction. We must acknowledge the new attack vectors and areas of compromise as we share more information that is sensitive.

Advances in cloud computing will provide opportunities for faster advancement of new technologies, improved resilience and economies of scale. It will be important to address the cybersecurity and compliance opportunities and challenges leveraging the scale of the cloud.

Conclusion

In summary, PJM and the electricity industry take cybersecurity seriously. We apply best practices, measure performance and address evolving threats like supply chain risks. We collaborate with government and industry partners to share threat information and best practices. We are investing in the workforce of the future and applying advances in technology to improve our reliability. Finally, we are taking advantage of opportunities to enhance the resilience of electricity by actively collaborating to understand and address the supply chain of electricity, to ensure that interdependent critical resources are available to serve the needs of the 65 million people in the PJM footprint.

The CHAIRMAN. Thank you, Mr. O'Brien, and we thank each of the panelists that have appeared before us this morning.

Mr. Gates, I want to start with you in terms of my questions. I think everyone on the panel this morning has mentioned the need and the necessity for collaboration and partnerships, but we all know that it is one thing to say I am going to partner with you, I am going to collaborate with you, but you have to trust one another. And sometimes when we are operating in a world of cybersecurity, you are not quite sure who to trust.

So, as several have mentioned, the Executive Order on the bulk power system is going to require enhanced information sharing between the government and the entire energy sector, including our utilities, our vendors and our manufacturers. If you can speak to how, within DOE, we can improve the protection of sensitive data that it receives from the industry and then also, how can DOE improve its trust of the private sector when sharing sensitive government information? I know, oftentimes, what we will hear is the industry is required to give the information, but they don't feel like they have been fully read into the situations. And so, again, collaboration and partnership are key and important, but that is also built on trust. So can you speak to both sides of that, please?

Mr. GATES. Thank you, Senator. I'll address the protection of the sensitive information from industry. That's always a challenge. Certainly, as it relates to collecting data from the Executive Order and the RFI that will allow us to implement the Executive Order, the RFI went out in July and ends in August. Protecting that information is, kind of, central to the program. The Department, when you look at information sharing, when you look at analysis and data gathering programs, not only CRISP but the CATT program that you may have heard of, the Cyber Analytics and Technical Techniques program. Those types of initiatives are central to understanding what's going on and then sharing information in a way that's protected. Liability protections for companies, for example, is part of that equation. The other part of that equation is the Department and the government protecting less than classified but very sensitive information. So we are designing systems and programs that the Department of Energy protects secrets and sensitive information in a number of endeavors from our science and research initiatives with the national labs to our nuclear stockpile and weapons protection programs, and cybersecurity is another aspect of that.

As it relates to the sector trusting us, that's a tough one, but if you just look at what's happened in the last four or five months and our response to the pandemic, the sharing that we've had with the different coordinating councils, the use of the ISAC to share information, we think the trust in the sector is growing, that the Government is actually figuring out how to take even classified information through a process, sanitize it in a way that it can quickly be distributed through either CISA or the E-ISAC but out to the sector in timely enough fashion that it actually makes a difference. We haven't totally solved the problem, ma'am.

The CHAIRMAN. Right.

Mr. GATES. It's a work in progress, but we think the trust issue, the trust equation is improving in favor of both the Government and the sector.

The CHAIRMAN. Well, and I think we recognize that it has to in order for this all to work.

Let me ask you one more question. Hopefully this one is relatively brief. Many of us on this Committee have electric co-ops and municipal utilities that have benefited from the DOE initiative that is focused on improving the cyber and physical security posture of the electric sector. In Alaska, we are primarily served by our rural electric co-ops and our municipal utilities. Last year, Congress agreed to appropriations report language that encouraged CESER to continue this initiative. Our energy bill also includes language that encourages these types of public-private partnerships. We also established a grant program to improve the cyber posture of our smaller utilities. Can you give us any update on the status of this initiative? Has any funding been released in this regard?

Mr. GATES. Ma'am, I'll get the exact details of the status of the program to you after this session. But we are working very hard to make sure that money flows to the sector and even outside of that program, the small utilities are, they're a soft, in some respects, a soft underbelly of the grid and we take great pride in, you know, certain research and development programs, like the Essence program that we think are going to be valuable in providing those entities the same level of protection as some of the larger utilities. So I'll get the detailed answers to you.

The CHAIRMAN. Well I appreciate that and, again, that is something that, I think, we recognize there is a vulnerability. They may be small, but once you work your way in, you can do a lot of damage there and recognizing the cost then to these small, rural electric co-ops and our municipal utilities, this is something that we have been focused on.

Let me turn to Senator Manchin.

Senator MANCHIN. Thank you, Madam Chairman.

First of all, to Mr. McClelland. As you are aware, Senator Murkowski and I introduced the PROTECT Act last year. The bill would establish incentives for electric utilities to invest in advanced cybersecurity technology. FERC's recent staff white paper exploring cybersecurity incentives considers several options that could work to achieve some of the objectives laid out in our bill. What are the next steps for FERC in considering cybersecurity incentive options, and can you share what some of the public comments have been in the docket?

Mr. MCCLELLAND. I think I found the unmute button. Thank you, Senator, for the question and also I just want to thank you for your work on the bill and your continued support and interest in cybersecurity. The, as you're aware, the white paper was a FERC staff white paper. It went out on June 18th as a 60-day comment period. And the white paper proposes two mechanisms of incentives. One is to exceed the current obligation within the CIP, the NERC, Critical Infrastructure Protection, or CIP, reliability standards, that would be, say, for instance, if an entity went from a low designation to a medium or a high designation.

The other is to follow the NIST framework. The NIST framework was established by Executive Order in February 2013 and its purpose was to create a set of best standards that all critical infrastructure sectors could share, all 16 sectors could share. So the industry collaborated with government to produce that NIST framework. It was revised, subsequently it was revised twice. So it was produced in 2014 and revised in 2018. So the white paper proposes either or both of those alternatives. We're awaiting comment. I don't have the status of what the current comments are to that proceeding, but we'd be happy to follow up with you.

Next steps would be to consider those comments and then use that within the Commission as a mechanism to better understand how, where industry would like, where the most effective place to apply the cyber incentives might be.

Senator MANCHIN. Thank you, sir.

I only have a few minutes here, so I want to go through some things very quickly, if I can.

Mr. Conner, we have talked about deterrents. How do we deter other nations from hitting us, especially in our grid system which would be very vulnerable and very harmful to our country? I guess, retaliation. How do you believe the retaliation—what we should do when we know these perpetrators are continually trying to do all the damage they can—what type of deterrents do you think that we, as the United States Government, should take against these perpetrators? Should we hit back? Should we hit back at their critical infrastructure or just give them a warning or what is the recommendation?

Mr. CONNER. Well, I think, as was mentioned earlier, we can't have, we can't have something that really has no meaning, but you know, it's true from our standpoint that, you know, the technology that's out there, we have to continue to fight this. This is not a matter of a "nice to have," it's—or a "needs to have." This is a "needs to have" and it changes daily. So as far as deterrents, you know, we don't really look at that from Siemens Energy Inc.'s viewpoint, but I do—but I believe there is something that we have to do to make it crucial for people who want to come in and attack our grid system.

Senator MANCHIN. Yes. I would like to get some of you all's input to try to make sure that we are not out of sync with the rules of engagement, if you will, but we have used retaliation from our nuclear response to let them know that we would hit and hit hard. I think in order to stop this type of attack, we have to make sure that they understand that we will use every means that we have to come back at these countries who are going at us, to hinder us, really, and harm us. I would love to hear from you all in the industry, if you will.

Mr. Gates, if I can follow up real quick? Presidential Policy Directive 21 designated responsibilities to different, to various federal agencies, departments and agencies, to serve as sector-specific agencies and support the private sector in managing the risk and respective critical infrastructure sectors. This recommendation was incorporated into the House version of NDAA and will likely come up in conference. I support these discussions and hopefully they ac-

knowledge and preserve the important role that DOE plays in protecting the electric grid.

Mr. Gates, do you agree that DOE provides specific capabilities and expertise as a sector-specific agency (SSA)? Is there additional clarification that DOE needs to fulfill its responsibility in this regard, and how do you all interact with the sector-specific agencies to ensure their coordination, but not duplication?

Mr. GATES. Thank you for the question, Senator Manchin.

I think in many respects the Department of Energy is a unique SSA. Not only does the sector know us, but we know the sector and, in many respects, we're part of the sector. As you know, we're, we manage PMAs. We manage the SPRO. We're, in some respects, an operator and those kinds of requirements are important to us understanding what's going on, sharing information with our partners. So I think that unique aspect of DOE is important. It gives us credibility in the sector, and I think it allows us to go at the cyber problem and other problems really aggressively because, you know, you add our——

Senator MANCHIN. Yes.

Mr. GATES. ——our national lab complex and just the talent and expertise we can bring to the problem. We think it's important for us to serve a strong SSA role.

Senator MANCHIN. Thank you.

Thank you, Madam Chairman.

The CHAIRMAN. Thank you, Senator Manchin.

We will next go to Senator Cassidy, who is with us online.

Senator CASSIDY. Hello, gentlemen. Thank you, Madam Chair.

Mr. Gates, last year we heard that one of the problems of information sharing was getting security clearances for partners in the private sector. Can you give us an update? Have we been able to better gain those security clearances, which is to say, better able to share this information?

Mr. GATES. Senator, I do not have an answer, a specific solution. Clearing, you know, the thousands of owners in a way that allows us to share highly sensitive information is an incredibly difficult challenge. We've taken the, I think the approach that is more historic in trying to make the information still useful but not sensitive, so in a way that is useful to the sector but doesn't threaten sources and methods. It's a difficult challenge. It's been a difficult challenge clearing just individuals who actually work in national security. It's one that we need to tackle, but I'll give you an update offline on the status of that action.

Senator CASSIDY. I would appreciate that because, again, it was identified as an issue a year ago and it does seem as if it was highlighted a year ago as, kind of, the Achilles heel. And so, however we can address that, that would be great. I will accept that it should be offline.

Mr. Conner, as an equipment manufacturer, how do you feel that this information sharing has progressed because it does seem as if there is a threat. It seems, again, as an equipment manufacturer, you need to be actively involved with the nature of the threat.

Mr. CONNER. Yeah, as I mentioned earlier, we have a number of tools, you know. Collaboration, I think Mr. O'Brien talked about, nobody can do it alone. So we have a number of tools that we go

out with our partners and our customers on/with, when we take a look at, for instance, the DOE talking with them. We just had a meeting end of June with Secretary Brouillette and talked about what we can do on the order to help, kind of, guide this along. But again, I think it's hey, the collaboration, I think is good. We can always improve things, and we need to continue to improve things to keep this moving forward.

Senator CASSIDY. Mr. Conner, I am also very interested in counterfeit goods and the ability of counterfeit goods to basically serve as a sabotage instrument, and you mentioned the quality control that you have in order to prevent that from occurring. Can I ask, does any of your supply chain go through China? I say that because we know that the People's Liberation Army has allegedly inserted chips into servers that would allow information to go back, chips that were only found with forensic engineering. So again, to what degree do your supply chains go through China and do we have such a risk?

Mr. CONNER. Very minimal, very minimal supply chain usage for us out of China. We do have facilities in China, and we do serve that market. That's not on Siemens Energy Inc. side, my side in the U.S., but that's on the larger part of Siemens Energy as a whole. What we actually go through, as I mentioned in my testimony, we actually have preapproved vendor lists and these vendors have to go through rigorous testing. We take a look at all their products and then——

Senator CASSIDY. Let me ask, because I heard your testimony. I have also become aware that having a network of vendors represents a security challenge for actually the parent company, if you will. If it is a vendor to the Department of Defense (DoD) that they can, kind of, work their way up the information chain into a prime contract. Similarly, since we are concerned about the cybersecurity of our grid, the cybersecurity of Siemens itself, I am sure that you have a number of cyberattacks as well. With this network of providers/vendors, how does Siemens avoid cyber espionage upon what you are doing and on cyber sabotage?

Mr. CONNER. Well, we actually have a significant group both in the U.S. and globally that goes through and tests every day. We get attacked thousands of times a day. I think somebody mentioned earlier, 300 million times a day. I don't think it's that much, but again, ours is, we have the, our approved vendor list. We go through and we have, to the extent we find something or from a compliance standpoint somebody doesn't meet that requirement, we kick them off. So it's almost, it's a significant amount of business that they would lose. And we also do, as I mentioned earlier, we do background checks and even through governmental, even the U.S. Government on who we're going to utilize as vendors, et cetera, to make sure they meet all the requirements to avoid having any counterfeit parts in our systems.

Senator CASSIDY. Okay.

Thank you, Madam Chair. I yield the floor.

The CHAIRMAN. Thank you, Senator Cassidy.

Senator King.

Senator KING. Thank you, Madam Chair.

There is one subject that we have not touched on today. It is not really within the jurisdiction of this Committee, but I just mention it in this context and that is the vulnerability of water systems. There was a recent alleged attack by Iran on an Israeli water system. Fortunately it was defended against successfully, but we have something like 50,000 water companies, separate water companies, in this country and that is a risk that the Congress needs to address.

Secondly, an issue that has not come up yet today is the gas pipeline system, and in New England about 60 percent of our electricity comes from natural gas and all the natural gas comes through the pipeline system. So at least in our region, and I suspect in other areas of the country, the pipeline system is part of the energy grid. You can protect the energy grid, but if the gas can't get through for some reason, the lights are still going to go off. My concern is TSA, in 2005, was given the authority to regulate the pipeline system. They were given the authority to issue regulations which they never have, and I am reminded of Lincoln's famous letter to McClellan, "If you're not gonna use the army, perhaps you could lend it to me for a while." If TSA is not going to use this authority, perhaps we should give the authority to somebody who will use it because this is an enormously important part. They are relying entirely on voluntary self-regulation. I just don't think that is adequate given the level of risk. And I know that FERC has an interest in this. This is something I very much want to follow up on.

A couple more specific questions to our panelists. Mr. O'Brien, do you red team your system? Do you do pen testing to see whether you have vulnerabilities? Do you have hackers for hire to test the security of your system?

Mr. O'BRIEN. Yes, thank you for the question, Senator King. We do a couple things. One is we do continuous red teaming, and we partner with an outside firm that's constantly probing our system and looking for issues. Secondly, we do what we call compromise assessments. We've brought in a top forensics company, Mandiant, to comb through our network looking for issues. And finally, we do internal audits, penetration testing and all that. So yes, we do. Thank you.

Senator KING. That is very reassuring.

I want to ask Mr. Gates and Mr. McClelland the same question. I was very disturbed a year or two ago when we had a hearing on this subject when I asked the fellow from NERC, do you red team? Do you pen test? And the answer was, I don't think so or something to that effect. Do you, as the agencies that are looking after this incredibly important infrastructure, do you do penetration testing and red teaming on the networks that you are responsible for?

Mr. Gates?

Mr. GATES. Senator King, thank you for that question.

In the context of the federally-owned assets, the PMAs, the SPRO, there is a red teaming of other, kind of, security measures that are taken to verify certain aspects of the defenses of the system and——

Senator KING. What about the private systems that are part of your responsibility?

Mr. GATES. So in that respect, and that's where the ESCC, the ONG, SCC and other forms are important where we can advise and consult and recommend defensive services such as red teaming, such as pen testing.

Senator KING. So the answer is no, you don't do this yourself. Is that correct?

Mr. GATES. So we don't do it ourselves and we're not, we're not designed, CESER wasn't designed to provide that service.

Senator KING. But wasn't CESER designed to protect the grid?

Mr. GATES. It's designed to protect the grid, yes, sir, but through using——

Senator KING. Isn't protecting the grid determining whether it is safe?

Mr. GATES. It is, but using the authorities and the resources that have been allocated to do that mission which we believe we're operating in, we could do more, perhaps we should do more. I don't know if it gets to the level of pen testing or red teaming. There are certain people on my staff who would love to take that on. But again, right now, in the role with the responsibilities and authorities we have and the partnerships, it's an advisory service that we're providing at this point.

Senator KING. Well, if you need additional authorities, I hope you will take for the record a question to let us know what additional authorities you need. I don't see how you can carry out a mission of protecting the grid without testing the grid's vulnerability.

Mr. McClelland, I did not get a chance to follow up, but I want to ask, I want you to think about the same question.

Finally, Madam Chair, I just hope that we could follow up this hearing with a hearing on the natural gas pipeline system, because I think it is a crucial part of our energy system and I am very concerned that we don't have the level of standards, testing and examination on that system that we have on the grid.

Thank you very much, Madam Chair, I appreciate it. I yield the floor.

The CHAIRMAN. Thank you, Senator King, and know that I certainly agree in terms of our energy infrastructure as it relates to our pipelines.

I don't see Senator Gardner on—I know he is popping in between three hearings this morning—so let's go to Senator Hyde-Smith.

Senator HYDE-SMITH. Thank you, Chairman Murkowski, and thank you, panel, for appearing today because your testimony is very valuable to this Committee. Your insight is very important, and I certainly appreciate you guys taking the time and being with us today.

My question is for all of you. It is well known that our nation's critical infrastructure is under constant threat of attack from our adversaries as we have been discussing. Couple this with the aging and fragile nature of systems running critical energy delivery systems and you have a potential recipe for disaster with our aging infrastructure. I know a lot of time and resources are dedicated to implementing the best practices and standards to secure these assets; however, best practices and standards do not often stop increasingly sophisticated bad actors for long. In your judgment, how much more should we be investing in time and resources recruiting

private or government entities that specialize in protecting the energy sector and counteracting these threats?

We will start with whoever wants to go first.

Mr. GATES. Thank you for the question, Senator Hyde-Smith.

Investment is always a tricky and difficult question, particularly from the government perspective when you have, you know, so much private ownership of an entity. So finding the right balance is a challenge. I think I can say, as you've stated, we're not investing enough, but how much of that should be public or private investment is a fair question. As Senator King mentioned regarding the pen testing, there are other security services that can be provided to identify threats. I think what we're doing in the Department to create products like the NAERM, the North American Energy Resilience Model, DCEI, CRISP—I think those are things that are helping, but more can be done on the ground to help sense more, to provide more analysis to identify threats more quickly and mitigate them.

What that investment looks like, I can't say, but I know it's not enough. The system is so large and expansive and you have such a different kind of stakeholder—stakeholders that can invest a lot on their own—and then you have communities that are on limited budgets. So it's a complicated problem that needs to be addressed, but it will require more investment.

Mr. O'BRIEN. Yeah, Senator Hyde-Smith, this is Tom O'Brien and I would add to what Alexander Gates discussed is, you brought up a really good point that there are legacy systems and there's older systems that are out there and we need to protect our systems. And I would go back to what we talked about earlier around the cybersecurity framework. We know how sophisticated the adversaries are. We still need to be able to protect our assets. We need to be able to detect when a bad actor is getting into our systems and we need to be able to recover and respond when that happens. That will require increased investment by everybody and I think it needs to scale based on the risks that you have. So just as a short answer, that would be my feedback.

Thank you.

Senator HYDE-SMITH. Thank you.

Mr. MCCLELLAND. If I might add, Senator, just add one other perspective?

Our office conducts individual assessments at utility networks. In many cases, these networks are large and complex. They're having tens of thousands of points. One of the recommendations we make, because it is so difficult, the challenges so sophisticated, and it's so rapid as far as its movement, one of the recommendations we make is that the utilities consider hiring outside expertise, contractors, that would assist during an emergency. So if their systems were breached, if they were having difficulty, they would bring in the outside contractors who have already helped preconfigure and arrange those networks so that they could be more resilient, better able to come back online and then it wouldn't be a matter of scrambling to try to find a contractor that could provide some assistance at the last minute.

So we actually focus this more toward the private sector to say FERC can provide cost recovery. We can provide incentives. We're

seeking comments about how those incentives and that cost recovery structure would best benefit the private sector, but at the same time, we are offering recommendations to address the issue that you raised.

Senator HYDE-SMITH. Thank you very much.

My second question——

Mr. CONNER. Yes, Senator——

Senator HYDE-SMITH. I am sorry.

Mr. CONNER. I was just going to respond.

Senator HYDE-SMITH. Oh.

Mr. CONNER. You know, as I mentioned earlier, Senator, in my responses, companies of all sizes need the technology workforce and the resources to manage these attacks and critical infrastructure. Cyberattacks are not going to be going away and we need to defend against them and make it a priority. And you know, I talked about the latest collaboration that we have with NYPA, New York Power Authority, to put together a state-of-the-art cyberattack and critical infrastructure group there. So, you know, the intent is that as we learn things in industry, as the governments learn them, as the states learn them, that we all collaborate and then we actually can filter that down and share that, those solutions, amongst the other utilities, not only energy, but I think we had mentioned water earlier, Senator. So things that we can learn there as well.

Senator HYDE-SMITH. Thank you very much.

Madam Chairman, I have a second question, if we have time for that? We will be brief.

The CHAIRMAN. Go ahead.

Senator HYDE-SMITH. It is on the cybersecurity defense, just the collaboration. Mr. Gates, this will be to you. With respect to protecting our nation's critical energy infrastructure, please provide the Committee with your primary recommendations on how the Department of Energy, the intelligence community and the private sector can collaborate better to defend against these cyber threats from, obviously, foreign adversaries, more effectively? Just on the collaboration.

Mr. GATES. Well, fortunately, we're working from a decent base with the CRISP program, the briefings that we provide the sector and our collaboration with the IC. The IC is, of course, the Intelligence Community, is critical. It is better to engage the adversary outside of our networks instead of inside. That shouldn't be the first point of an engagement. And so, the IC's role in that is critical and that's not just my bias because that's where I sort of grew up, but the collaboration is getting stronger. It needs to get better. It needs to be seamless, and it needs to be real time.

The Solarium Commission proposed some things that kind of speak to that, but I think more can happen. Information sharing and, ma'am, you mentioned the trust issue earlier, when you're talking about the Intelligence Community, sensitive information and sharing it rapidly, that those are oxymorons in some respects. We need to do more to figure out how to get useful, kind of, sensitive information into the hands of network operators so they can make decisions and take actions. It's a work in progress. I will be—I would gladly provide you a list of recommendations on how to improve that process.

Senator HYDE-SMITH. Thank you very much.

The CHAIRMAN. Thank you, Senator.

Let's go to Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you. Gentlemen, thank you so much for this important conversation. I want to thank the Chair and Ranking Member for holding this hearing.

Let's talk a little bit about workforce. I know, Mr. Gates, in your testimony you highlighted one of the priorities for CESER is to build a superior workforce. And then Mr. O'Brien, in your testimony, you also highlighted that the future success on the electricity industry depends on the development and leadership of the next generation of utility employees including cybersecurity analysts. So let's start with both of you and, Mr. Gates, I will start with you. Can you speak more about DOE's efforts and methods to deliver on your goals of building a superior workforce? And then Mr. O'Brien, I would ask you to also talk about the importance of the need for building that cybersecurity workforce across both the public and private energy sectors. Mr. Gates.

Mr. GATES. Thank you, Senator.

This is a challenge for the country. Most of the estimates are that even, you know, at current rates we're going to be short of not only IT cybersecurity professionals, but it's even starker when we talk about industrial control systems. We started a number of initiatives from CyberForce, for example, to help with training of those who are inclined to enter this space as a profession. We think there's more that can be done. Certainly we're looking at models, similar to the Center of Academic Excellence that DHS and NSA run for cybersecurity and intelligence programs. We think there's a carve-out possible for those who are inclined to go into defensive industrial control systems. Using our national lab complex, we actually started this year a collaboration with one of the military academies to do internships to get them training with one of the national labs in this area and we think there's just more. This is something where it's not just the Department, but the government and the private sector will need to invest to get the experience, the senior and junior engineers more training, those who are in the business and build on ramps for those coming out of college or in college to enter the business so we can build that, not only cybersecurity workforce, but one that's, kind of, geared toward the energy sector.

Senator CORTEZ MASTO. Thank you.

Mr. O'Brien, your thoughts on what more we can be doing?

Mr. O'BRIEN. Yeah, thank you for the question and I think you're highlighting a really good point that the supply and demand on cybersecurity resources is somewhat problematic, and from our perspective we're looking at growing talent from the inside where we can and we've established things like rotational development programs and really teaching people the business, teaching people the different technologies so that they can fight the cybersecurity issue. I think the other thing that we've done, and it's yielded some pretty good results, is we have some great partnerships with, you know, academia. We've had great partnerships with DoD, DOE and really engaging our workforce on that. The E-ISAC has done a very

nice job with workshops and you've really got to commit to getting your people to those so that they can learn.

And then the other thing that I referenced in my testimony was I think we need to look at the diversity inclusion as an opportunity for untapped potential and that's something that we're doing at PJM.

Thank you.

Senator CORTEZ MASTO. Thank you. I cannot stress that enough, and we have had hearings in other committees where the diversity inclusion is key to increasing that workforce and it is a power that has not been tapped into. So thank you for that.

Mr. Gates, I want to also highlight the fact that just in June of this year the University of Nevada Reno, where I graduated from, their Cybersecurity Center and DOE's Nevada National Security Site announced a partnership for cybersecurity research and collaboration. I cannot thank you enough for that, but most importantly, I am excited because it gives the opportunity for a number of graduate and undergraduate students to engage in and have hands-on research, on research, education, training and career development. I think more of that needs to occur. I applaud you on taking advantage of that, so thank you.

I know my time is almost up. I will submit the rest of my questions for the record.

Thank you.

The CHAIRMAN. Thank you, Senator.

Continuing on Senator Cortez Masto's questions regarding the workforce, Mr. O'Brien, I know that—and we have had conversations here this morning about supply chain security—you have spoken to this issue as well as Mr. Conner. But not only does PJM purchase from around the world, so when we think about supply chain there, you also hire employees, contractors and consultants that come from other places around the world. How can you be certain that you are not hiring an insider threat? How do you address that challenge?

Mr. O'BRIEN. Well, first and foremost, that's very difficult because, you know, a foreign adversary that has intent may very well find ways to get in, but the things that we do is, you know, we have pretty good security background checks and that's both for, you know, contractors and for employees. The other thing that we do is, you know, and obviously I wouldn't get into the details, but we have an insider threat program where we're looking at, you know, the activities of what's happening inside our walls and those are things that are very important because if you put your head in the sand around the insider threat, it can be problematic. But I will just summarize it with good background checks, good interviewing, good references and making sure you have the solid insider threat protocol. Thank you.

The CHAIRMAN. Thank you.

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

Mr. CONNER. Yes, thank you for the question.

No, I think we actually make sure we do the background checks here as well and we also, because this is relatively new, you know, have actually been setting up programs with universities to try to run a curriculum to how do we get the training there. So more

homegrown, we don't like to bring in people from the outside to be doing some of this work for us. So I think if you take a look at the programs we've put in, along with the universities for the training, it's gone a long way for us.

The CHAIRMAN. I appreciate that.

Let me go to you, Mr. McClelland, and this is with regards to how we protect sensitive data. On an annual basis FERC requires our electric utilities to submit detailed data on their power grid operations. Form 715 requires utilities to submit maps and diagrams of the grid as well as actual grid data in electronic format. We acknowledge, FERC acknowledges, that this data is critical energy infrastructure information and treats it as such. The first question here though goes to FERC's policy of releasing the data to the public on the basis of the public's right to know. I think we are all in favor of levels of transparency, certainly. In general, the public does have a right to know, but when it comes to schematics of critical energy infrastructure information, it seems reasonable to me to be, perhaps, a little more circumspect here. Should FERC consider changing its policy regarding the release of this critical energy infrastructure information to a need to know basis?

Mr. MCCLELLAND. Thank you, Chairman, I appreciate the question.

FERC has to balance or must balance the right to know with the sensitivity of the information. The CEII program that we conduct provides necessary but limited release of that information. In addition, all requesters are required to submit in writing their need for, to attest to and demonstrate their need for this information. FERC then verifies that request. It can do so with business references and online tools and after verification, FERC does require the execution of a non-disclosure agreement. That non-disclosure agreement carries with it sanctions if that non-disclosure agreement is violated and those sanctions can include a loss of access to CEII as well as criminal prosecution.

To date, FERC is not aware of any individual that's violated, intentionally violated, that non-disclosure agreement.

The CHAIRMAN. So Mr. McClelland, how does FERC audit how members of the public use that CEII information that they have received? Is there a follow-on? You mentioned the non-disclosure, they then receive the information. What then happens next in terms of just ensuring that there has been that level of compliance?

Mr. MCCLELLAND. Well, FERC doesn't actively monitor those that sign non-disclosure agreements and receive the information, but FERC, however, has investigated allegations that non-disclosure agreements have been violated and followed up appropriately.

The CHAIRMAN. So is it your view that perhaps FERC should look to strengthening the provisions in the non-disclosure agreements?

Mr. MCCLELLAND. Well, to date, the non-disclosure agreement process has worked for FERC. As I said, we're not aware of any intentional violations of that non-disclosure agreement for those that have received CEII information.

The CHAIRMAN. Okay.

Let me ask, I know Senator Manchin had asked about the white paper that FERC recently did. In the white paper, there is an ob-

servation that the standards-making process—for the mandatory reliability standards—the standards-making process "does not lend itself to addressing rapidly evolving cybersecurity threats." Does Congress or does FERC need to change the development process for these standards?

Mr. MCCLELLAND. Well——

The CHAIRMAN. If you recognize that it is that cumbersome.

Mr. MCCLELLAND. I'm sorry, I'm glad you asked the question, Chairman.

That's why FERC uses a tool called Approach. And the reliability standards, although they can be, they aren't required to be best practices. And in the context of these advanced persistent threat adversaries that are specifically targeting our most critical infrastructure facilities with precision and with advanced tools and techniques, the Commission has found that it's necessary to use a dual-pronged approach. It's not to say that the standards development process isn't working because it's providing excellent foundational standards that really are a shining example across all of the infrastructure types, but those are foundational practices.

The Commission, and we've heard this earlier from several Senators, the Commission's—it's recognized the need to convey this most sensitive information to our utility partners so that they can quickly react to it. In that context, and I just want to highlight one small example. We do work very closely with the Director of National Intelligence, the National Counterintelligence and Security Center. They convey one day read in clearances. So a process that could take a year or more to conduct, we can get and we have, we've gotten state officials and industry officials quickly cleared and then brought them in for group classified briefings and working sessions to make sure they understand the threat that's before them. We identify the best practices to mitigate against them and then they go out and take care of that. In the meantime, FERC then considers whether it would be appropriate to follow on with actions and activities pursuant to the reliability standards.

The CHAIRMAN. Let me ask you one more question on the white paper as well. Do you think that the white paper's proposal of financial incentives for the industry will be helpful or will it just serve to increase rates because, you know, you have the potential for a tradeoff here between higher rates or better protection? And so, is that the answer there in terms of that protection, is the financial incentive?

Mr. MCCLELLAND. Well, we hope so. We did solicit two separate mechanisms by which industry can react and then propose comments back to the incentives. But it really, the fundamental, it's really just three questions that I think summarize this issue very succinctly. The third question is do you know where best practices belong because not all facilities are created equally. Some facilities are extremely strategic in nature and you can bet that's where our adversaries will be targeting. So we hope or believe that the white paper that we developed, the application of those incentives can be used to target those critical facilities to deny the adversary access and then in the future even exploit of those facilities.

So, and that would be also cost-effective. So instead of requiring everyone to establish a best practices and follow those best prac-

tices through a mandatory requirement, we can strategically select those facilities and then apply these best practices to them. And we're hopeful we get great comments back on that incentives white paper. We're very hopeful about that.

The CHAIRMAN. I am sure you will get comments.

[Laughter.]

I appreciate that, Mr. McClelland.

I am going to give my colleagues an opportunity for a second round, but Senator Risch has just joined us. Senator, if you would like to ask a question before we turn to Senator Manchin.

Senator RISCH. Thank you very much. Thank you, Madam Chairman.

Cybersecurity is really important, and obviously this Committee has overlapping jurisdiction with a number of other committees.

The CHAIRMAN. With everybody.

[Laughter.]

Senator RISCH. Yes, with everybody, I guess that is right.

In Idaho, we are particularly sensitive to all this because of the Idaho National Laboratory (INL). The Idaho National Laboratory, as everyone knows, is the birthplace of nuclear energy in America and it is now, it has been the flagship for nuclear energy, really, in America and in the world. Now the flag is going up for cyber because at the INL they have some unique capabilities that really call out for them to be the flagship lab also for cybersecurity. This is the result of their decades of experience in control systems. Obviously since it was the birthplace of nuclear power, control systems played a very, very important role as they went forward building the 52 different experimental—or some experimental, some actual—nuclear reactors that were built at the laboratory. Those control systems were critical. They have great expertise in that regard, plus they have some test beds that are important. So the result of that is the INL is moving forward very rapidly in the cyberspace.

I have a question for Mr. Gates I would like to ask and have him talk to us a little bit about the role that the INL and the other labs are playing in this regard. And as we know, earlier this year the Cyberspace Solarium Commission released dozens of recommendations to better secure the nation from cyberattacks—very important because this is so critical in our infrastructure and everything else. The Department of Energy national laboratories are playing a key role in this effort to move these recommendations forward. In Idaho we have the Idaho National Lab, as I said, which is the only national laboratory explicitly mentioned in this report and that, of course, is because of its expertise that I just described and also because of their outsized role and growing role in cybersecurity.

So again, the question I have for you, Mr. Gates, is that as Congress looks as we all, in Congress, look to implement many of the recommendations in this report, can you please talk a little bit about what you think the INL, the role the INL can play in that regard and the role that any other of the labs might play in that regard? INL certainly has a unique place and unique capabilities, but I would like to hear your observations in that regard.

Mr. GATES. Thank you, Senator Risch.

INL, it's in many respects, particularly in the area of control systems, it's a first among its equals. Certainly, CESER and the De-

partment, the sector, relies on many labs. If you look at what we are doing with NAERM, you know, there are eight national labs that are collaborating on that project that will allow us to obtain high-fidelity situational awareness on the grid. INL is one of them. But INL has really taken a leadership role on some of our critical programs, CyTRICS, for example, where we're going to be testing systems down to the component level to look for and eliminate vulnerabilities. That program, I mean, INL is best suited for it. It was, CyTRICS, was designed with INL in mind and what that is going to allow us to do is push the adversary further out of the infrastructure using that and other programs. CyTRICS, centered at INL, is also going to allow us to execute the Executive Order. It's a key component to DOE's ability to implement 139920.

There are other programs. Just this year, I mentioned earlier that we sent a few Coast Guard cadets to INL for an intern program and we think that's a model for how to get training into the hands of those who will be helping us defend control systems, whether they're controlling a weapon system or whether they're controlling part of the critical infrastructure. So that's just one of many programs. We rely on INL's expertise, even in classified settings. There's work that's just uniquely suited for INL, but many of our other national labs, it's almost a superpower for the Department of Energy, our ability to rely on national labs to help us solve problems and then get them into the sector.

Senator RISCH. Thank you very much, and I appreciate your reference there to the national security matters and also the classified nature. Sometimes when I am home in Idaho I try to explain to people what they do at the INL. I can tell them about some things and I can't tell them about others. Even the ones that are classified are incredibly important. So thank you for your work, I sincerely appreciate it.

Thank you for holding this hearing, Madam Chairman. I appreciate it.

The CHAIRMAN. Thank you, Senator Risch. As you know, I have been out to INL, have seen it, can't talk about it.

[Laughter.]

Senator Manchin.

Senator RISCH. Some of it.

The CHAIRMAN. Some of it.

Senator MANCHIN. Thank you, Madam Chairman.

To Mr. Gates and Mr. Conner, I mentioned earlier I am pleased to see DOE taking steps to ensure that we have safe and secure supply chains for bulk power systems. However, in moving forward with identifying grid equipment that is at risk or equipment that could be part of a prequalified list, it is of credible importance that the manufacturers of electric equipment are utilized for their knowledge and expertise. I know the Executive Order established a task force to engage with the energy industry, but manufacturers were not specifically included in that process.

Mr. Gates, has the DOE considered establishing a task force equivalent for the manufacturers to the electric equipment to inform DOE to get response back for them and how is DOE fully engaging with these stakeholders?

Mr. GATES. Thank you for that question, Senator Manchin. You know, since the issuance of the Executive Order, DOE has held over 90 calls, not only to the asset owners, but that also includes manufacturers. So they're part of the equation. And even in part of the CyTRICS program which is a key element of executing the Executive Order, we've already signed two companies. We're engaging others directly and having a conversation. A lot of those discussions are in the context of the broader vulnerability identification and elimination aspect, but we're also talking about implementation of the Executive Order.

So over 3,000 individuals have engaged the Department since the issuance of the Executive Order. Some of them are manufacturers, a lot of utility owners, suppliers, and we're comfortable, though we've taken the letter to heart and we're making sure that we're covering all our bases, we're comfortable with our engagement strategy so far and we seek to do more of that because we do want to be thorough and it requires a partnership. We can't go it alone. So, you know, your letter was taken to heart, sir.

Senator MANCHIN. Thank you, sir.

Mr. O'Brien, as the largest grid operator in the country, I appreciate that PJM takes cybersecurity seriously. The states and utilities that make up PJM service territory which includes my State of West Virginia vary a lot in their ability to address and get ahead of the cyber grid threats leaving an important role for PJM to make sure the system is not made vulnerable by any one actor who does not get it up to the standards that you are asking for. So my question would be, what are the biggest risks in the PJM territory that you are concerned about and what can other grid operators learn from what you have been able to address with these threats?

Mr. O'BRIEN. Yeah, thank you, Senator.

I think from my perspective, certainly from an operating control aspect, is the biggest risk to PJM is that there's significant compromise of our members. I mean, we rely on information and data that comes into PJM and we're running all types of real-time analysis to keep the lights running. But if there is any case where the telecommunications system is down, we can't get that data, that information. I think it's a really high risk——

Senator MANCHIN. Let me ask you this, Mr. O'Brien. Are you all able to run scenarios that you can test to see if they are up to your standards, even if they are reporting they are? Do you do, kind of, cyber test, if you will, to see if you are able to get into their system or basically show they have, still, some vulnerabilities?

Mr. O'BRIEN. No, we don't do that. I mean, that's something that we don't, you know, feel is in our jurisdiction based on how we operate. We do collaborate a lot with the members, but no, we don't do, you know,——

Senator MANCHIN. Well, let me ask Mr. Gates. Let me ask him then.

From the DOE, Mr. Gates, does any, I mean, if our systems are telling you, whether it be in West Virginia or any other of the PJM states or any other areas of our country, if they are not, if they are actually not really hardening their systems to protect against the cyberattacks, how are you able to detect it? Do you just have to

wait until something happens or are you all checking to see if they are doing it?

Mr. GATES. We're not. There is a reporting mechanism in place.

Senator MANCHIN. No one is checking, I can tell right now. No one. No one is testing to make sure. If I wanted to find out if you did what you told me you did, I would have one of my smart people try to hack into that and see if I show the fallacy there. So we are not doing those types of tests?

Mr. GATES. I think that's fair, though if you look at what CISA is doing, some of the work they're doing in the sector and the Department and the advice from FERC and NERC, there are mechanisms to engage them, but as far as overseeing the implementation of certain things in a private utility, again, there are some limitations in the current——

Senator MANCHIN. Well, again, I would ask PJM. Mr. O'Brien, how do you all plan to continue monitoring these evolving risks if you really can't check to see if they have been hardened? It can't be done. Has the risk been eliminated?

Mr. O'BRIEN. Yeah, I think, Senator, the thing that we rely on, relative to our members, is, you know, the NERC compliance and they're all held to a standard, they're held to an audit and we're counting on that. Now we do a lot of collaboration and discussions on best practices, but it's not within our jurisdiction to actually red team or try to hack into their systems right now.

Senator MANCHIN. Well, we will have to check with NERC then. We have to check with somebody to see if somebody is checking anything.

Alright, thank you.

Thank you, Madam Chairman, and thank all of you. I am very, very appreciative.

The CHAIRMAN. Thank you, Senator.

Senator Hoeven has joined us.

Senator HOEVEN. Thank you, Madam Chairman.

My first question is to Mr. McClelland. As consumers we have benefited from centralized baseload generating assets and our ability to [inaudible]—to provide power, especially during extreme weather events, polar vortexes and so forth. And we now see more centralized, intermittent generation on the grid and so forth which creates opportunities, but also, risks. Mr. McClelland, what measures has [the company] taken to manage liability and cybersecurity risks in these new technologies?

Mr. MCCLELLAND. So as users, owners and operators of the power grid, these facilities may be subject, would likely be subject to the NERC reliability standards if they reach a certain threshold and they are interconnected to the bulk power system. So that's where the Commission's jurisdiction is, under the Federal Power Act, Section 215. If these facilities interconnect to the bulk power system, they'll be held to that minimum standard. And in addition, Senator, we do have a program, a collaborative program that is available to any entity where we will, for instance, do an onsite assessment of their facilities, identify vulnerabilities and then assist them with mitigating action. So it's the same level of accountability that all generation resources under the Commission's jurisdiction would have.

Senator HOEVEN. Does Congress need to provide the FERC with any additional tools or capabilities to make sure that FERC is continuing to protect and improve the reliability of the bulk power system?

Mr. MCCLELLAND. Well, the Commission now is using a dual-fold approach. So we're establishing baseline standards and they're good, the reliability standards for cybersecurity through the NERC process, but this process is open and deliberative and it's not necessarily reflects best practices. On the other side, we're collaborating very closely with the intelligence community. That'd be our friend, Alex Gates at the Department of Energy, Department of Homeland Security and other agencies to stay current on those threats. And then we're actively engaging with industry to push out this information so that they can be aware of the threats. This bill would actually add to that authority. It would add to our voluntary assistance work with industry, providing us with additional authorities.

Senator HOEVEN. For Mr. Conner, how do we continue to strengthen the relationship between the public and private sectors to ensure that information is shared and also protected from inappropriate disposal?

Mr. CONNER. Yes, thank you for the question.

I think, as we mentioned earlier in my testimony, if I just take a look at the partnership that we've done with NYPA. That's more on the public side. That was just last week, and it's to develop the new think tank with them. I also take a look at all the partnerships that we have in the private sector with some of our vendors and our supply chain management. And as I also testified earlier, we make sure that despite all of that, that we actually do testing on hardware, software, security testing of everything that we get out of our suppliers as well to cover that side.

So I think it's collaboration. We talked about it earlier. Nobody gets there by themselves, but it's continue to collaborate and communicate across the board.

Senator HOEVEN. And then for Mr. Gates. Do you believe that the Department of Energy has sufficient ability over the nation's energy delivery system to properly address the attacks and vulnerabilities——

Mr. GATES. Thank you for the question, Senator.

I'm not sure anyone has the visibility to address all the threats. If we had that visibility, whether it was the Department, whether it was in the private sector, we would be doing more to develop solutions and push the adversary further away from our infrastructure. But that's why investments like NAERM and developing other tools and why information sharing through the ISACs and other mechanisms, the intelligence briefings, are so important. But we do need better tools. We need better sensors, and we're investing in that. We need better analytics which we're developing at the national labs. Pulling all that together to have better situational awareness, high fidelity is the answer. We haven't achieved it yet, but it is a goal and it's a pressing goal for the Department.

Senator HOEVEN. Is there additional assistance Congress can provide or resources, in your opinion, at this time that would be critical to test?

Mr. GATES. There's always room for additional support, sir. Targeted support at specific programs that allow us to develop some of these solutions more rapidly is always effective, making it easier for us to fund pilots and work with the national labs, with the private sector. There are pretty interesting developments in private industry, tools that are useful for us, but even that requires integration and testing. So clearly, the whole sector, including the Department could use more support.

Senator HOEVEN. But you don't have a specific in mind?

Mr. GATES. I do have specifics in mind, sir, and I would gladly provide those to you offline.

Senator HOEVEN. Alright. Thank you very much.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator Hoeven.

Gentlemen, we appreciate the discussion that we have had here this morning. I know Senator Manchin and I have no further questions.

Senator King, did you have anything further that you wanted to add?

Senator KING. Yes, just two things.

The first, Senator Manchin, in your usual commonsense way, you put your finger on something very important which we talked about earlier which is red teaming or hackers for hire or penetration testing, whatever you want to call it. We need more of it. We need authority to do it in Mr. Gates' agency and perhaps at FERC. People can certify that they are secure but there is no way to really test that until you have really tried to penetrate their network. So I have asked Mr. Gates to supply us with what he feels he needs in the way of additional authorities to make that happen. So I want to associate myself with that question.

One other question that has not come up today, and I don't know whether this should be to Mr. McClelland or to Mr. Gates, but isn't distributed energy, that is, generation at the home or in the neighborhood which is now available to us in part through the use of solar, isn't that part of a national security solution to try to avoid the risk of the giant grid with the giant generating plant that if it goes online, everybody goes down? Is anybody thinking about that? Mr. Gates, is that something that you all have looked at?

Mr. GATES. Senator King, it is something the Department is concerned with, particularly when we look at some of the grid modernization initiatives, you know, baking security into that modernization, whether they're microgrids and so forth is an important aspect of it. But there are those who also believe that if we don't bake in security that we're distributing the problem. Those systems still are dependent on technologies that, you know, could be vulnerable and just change the nature of an attack, make it a——

Senator KING. But if you have a solar array on your house that supplies your needs, you don't care if something happens to a generating plant 200 miles away. That is my point. It seems to me that there is a resilience redundant kind of effect here, and I realize integration into the grid and all those are technical questions, but the decentralization, I mean, the whole history of our electrical system has been centralization. We are now in a place where technology allows us to decentralize, and it seems to me that could be

an important advantage in terms of securing electric supply to individuals and businesses.

Mr. McClelland, are you guys looking at that at FERC?

Mr. MCCLELLAND. Thank you, Senator, for the question.

In some ways, and to add to Mr. Gates' point, in some ways the addition of new technologies, new systems, especially supply chain concerns can complicate security. However, to your point, there's a vast reduction of interdependencies associated with a self-sufficient plant. So I think that so long as the facility, and I am speaking for myself, so long as the facility is secure, has/is abiding by best practices to counter those adversarial attacks, it certainly makes it easier to protect a self-contained, fuel secure facility, such as renewables versus a facility that depends on many other types of infrastructure to produce generation.

Senator KING. Thank you.

Thank you, Madam Chair, I appreciate it.

The CHAIRMAN. Thank you.

This has been a really instructive hearing, again, and I appreciate the input that we have received, not only from those within the Department, the agencies, but also the private sector. I think it was important to have that.

Senator MANCHIN. Can I say one thing?

Senator King, Angus, are you still on?

The CHAIRMAN. Yes.

Senator MANCHIN. Angus, the only thing I wanted to ask, I know you asked directly with DOE if they could check, you know, by basically hiring the real smart people we talk about that are able to find out if we are on our game or not.

Senator KING. Right.

Senator MANCHIN. But how about with PJM? Are they not responsible then, basically if they are the carrier, I mean, they are one of the largest in the country? They are all over my state. Should they not be——

Senator KING. I asked PJM that question and I think the response was that they do do pen testing and red teaming. Isn't that correct, Mr. O'Brien? I thought that was what you said.

Mr. O'BRIEN. Yeah, thank you. Let me clarify. We do extensive red teaming on our own systems. We do extensive penetration testing on our own systems. What we don't do is red teaming and penetration testing on our member company systems where data flows into us. So that's the little nuance to the question.

Senator MANCHIN. So you don't have the jurisdiction for that, is what you are saying, why you don't do it?

Mr. O'BRIEN. We do not. No.

Senator MANCHIN. Okay. Angus, that gives us something else to work on.

The CHAIRMAN. Yes.

Mr. O'BRIEN. And again, I think NERC plays a role in that as well.

Senator MANCHIN. Sure.

Mr. O'BRIEN. With the—thank you.

The CHAIRMAN. But that is your vulnerability. You can be secure here——

Senator MANCHIN. Absolutely. Absolutely.

The CHAIRMAN. ——but then feed into where you are.

Senator MANCHIN. I just want to thank Angus, Senator King, and Congressman Gallagher for what they have done in the last two years. I mean, it is truly amazing and it needs to be brought—it is just common sense. It is just pure common sense. And we have to do all the checking we can. So maybe this is something that we could work on with NERC and get some of these barriers broken down for you so we really have thorough checking and thorough testing.

Thank you.

The CHAIRMAN. Well, I think we recognize that the threat from cyber, whether it is to our energy systems or any aspect of, really, our economy, there is vulnerability that we recognize and again, we are talking about collaboration, we are talking about partnership, built on the trust. And so how we can help facilitate that is important. When you can't trust, you have to test. Trust but verify. I think this is some of the conversation that we have had here today.

There are some requests that Committee members have made that, I think, Mr. Gates, you acknowledge that you would be able to provide members of the Committee a response. We look forward to that and if other members have further questions for the record, we would hope that you would be able to respond.

We appreciate the time that you have given us and the information that you have provided us as we focus on this critically, critically important aspect of protecting our energy sector.

With that, the Committee stands adjourned.

[Whereupon, at 11:53 a.m. the hearing was adjourned.]

APPENDIX MATERIAL SUBMITTED

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Alexander Gates

QUESTIONS FROM CHAIRMAN LISA MURKOWSKI

Q1. During the hearing, I asked about the Department of Energy's work to improve the cybersecurity posture of small and rural utilities. In the report to accompany the FY2020 Energy and Water Development and Related Agencies Appropriations Act (Division C of the Further Continuing Appropriations Act, 2020), the Office of Cybersecurity, Energy Security and Emergency Response (CESER) was specifically directed to continue to develop and deploy cyber and physical security solutions for rural electric cooperatives and municipal utilities.

Q1a. Can you please describe CESER's efforts in this space?

A1a. CESER is continuing to develop and deploy cyber and physical security solutions for rural electric cooperatives and municipal utilities as directed by the FY2020 Energy and Water Development and Related Agencies Appropriations Act.

Through this effort, CESER is executing two cooperative agreements with select entities to engage distribution and municipal utilities on innovative cybersecurity solutions. These agreements will total no less than $6,000,000 and are focused on innovative cybersecurity solutions in the following areas:

1. Detect and respond to cyber adversarial activity on operational technology (OT) networks;
2. Utilize artificial intelligence (AI) to identify anomalies, reduce false positives;
3. Provide for advanced analytics to identify compromised systems;
4. Increase system resilience in energy delivery control systems or components; and
5. Employ autonomous defense solutions at remote endpoints to protect against attacks.

Q1b. Has any of the funding appropriated been released to some of these smaller distribution utilities?

A1b. In September 2020, CESER made the above non-competitive awards to APPA and NRECA with the goal of providing utilities with emerging innovations at the hardware, firmware and/or software levels to protect the key operational technology components that enable the safe control of the physical systems that deliver electric power. CESER aims to deploy the solution to utility participants by 2023.

Q2. A few times during the hearing, you mentioned the Department of Energy's efforts on building a North American Energy Resilience Model (NAERM).

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Alexander Gates

Q2a. Are there any roadblocks preventing the NAERM from becoming fully operational?

A2a. There are currently no foreseeable roadblocks preventing NAERM from becoming operational, though the tool's adoption by industry will be determined by the needs of various operators.

Q2b. How can the NAERM improve our collective response to cyber threats and vulnerabilities?

A2b. NAERM enables the study and analysis of the grid under different scenarios by Federal partners and other future end-users with a need-to-know. Communications infrastructure modeling, coupled with other infrastructure models (such as natural gas and electricity), will enable the NAERM user to study and analyze infrastructure interdependencies, including identification of system vulnerabilities and mitigation approaches. With the addition of near real-time data, cyber threats can be detected rapidly and appropriate entities can be notified to support timely, coordinated response. NAERM will help effectively utilize taxpayer funding by informing the end-user of the types of investments that are prudent to increasing grid resilience and improving system restoration time following an emergency.

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Alexander Gates

QUESTIONS FROM RANKING MEMBER JOE MANCHIN III

Q1. In April, the Federal Communications Commission (FCC) voted to open up 1200 megahertz of radio spectrum in the 6GHz band for unlicensed use. I am concerned that this will impede the ability of critical infrastructure industries, who rely on the 6GHz band, to operate mission-critical communications, and that there has not been enough testing of the Automatic Frequency Coordination mitigation technology to prevent negative impacts on the current 6GHz band users.

Q1a. Have you had discussions with the FCC about how sharing the band with unlicensed users will work?

A1a. On September 3, 2019, the Department of Energy (DOE or Department) sent a letter to FCC Chairman Pai to express concerns over the unlicensed use of the 6GHz band, and NTIA is currently working with DOE to file that letter into the FCC docket. In that letter, DOE emphasized the importance of secure communications for the energy and water industries. DOE stated that these industries "do not currently have any cost effective, readily achievable alternatives to the 6GHz band if the FCC proceeds with the existing proposal and damaging signal interference is realized." DOE emphasized the importance of adequate testing of the FCC proposed Automated Frequency Coordination (AFC) system before commingling occurs on the band. DOE recommended investigating a long-term solution for dedicated spectrum for critical infrastructure users in the energy and water sectors. DOE is currently working with NTIA to coordinate a briefing with FCC to discuss this matter.

Q1b. Are you confident that the incumbent users will be protected and not experience disruptions under any scenario as this plan moves forward?

A1b. DOE cannot confidently state that incumbent users will be protected and not experience disruption during the implementation of the current plan. DOE recommends that the FCC-proposed AFC system be analyzed by field trial projects and internal lab modeling before it is placed into use. DOE also recommends investigating a long-term solution for dedicated spectrum for critical energy and water infrastructure owners and operators to prevent potential spectrum interference in the 6GHz band.

Q2. The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) recently came out with an advisory recommending the reduction of operational technology and control systems exposure.

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Alexander Gates

Q2a. Is the Department of Energy using these recommendations to inform your guidance and activities?

A2a. The Department of Energy (DOE) is using the recent advisory from the NSA and CISA, as well as other current standards and guidance to inform the ongoing development of Version 2.0 of the Cybersecurity Capability Maturity Model (C2M2) —a free, voluntary, and foundational CESER program guiding the resilience of the energy sector. The C2M2 is a common set of industry-vetted cybersecurity practices developed through a public-private partnership of energy sector experts. Organizations in energy and other sectors use C2M2 to evaluate, prioritize, establish, and improve cybersecurity capabilities and posture. CESER, in collaboration with energy industry is currently engaged in a technical sweep of the draft C2M2 version 2.0. Our goal is to validate and improve the efficacy of cybersecurity practices in the model against current threats and technologies. The C2M2 technical sweep topics prioritized by energy industry include, but are not limited to, ransomware, connected infrastructure, and recent grid attacks, which address the recently observed tactics, techniques, and procedures identified in the joint NSA-CISA advisory.

Additionally, CESER routinely provides both DOE-originated reporting and advisories from interagency partners to the energy sector to ensure maximum awareness of all sources of cybersecurity risk information. Generally, this information is provided to key information hubs such as the Electricity Information Sharing and Analysis Center (E-ISAC), the Oil and Natural Gas (ONG)-ISAC, and the Downstream Natural Gas (DNG)-ISAC, as well as our Sector Coordinating Councils.

Q2b. Do you have plans to address asset management and vulnerability management to understand in real time which assets and technologies are connected to energy networks and how organizations should be prioritizing vulnerabilities that are discovered in their networks and systems?

A2b. The C2M2 model addresses Asset Management and Threat and Vulnerability Management capabilities. These topics are two of the C2M2's 10 domains. These two domains include fundamental practices for understanding the assets (e.g., know what is on one's network) connected to energy networks and appropriately prioritizing identified vulnerabilities in networks and systems (e.g., dealing with the most consequential vulnerabilities first). As an example, an organization adopting C2M2 higher maturity practices is able to better defend its systems and networks because in case of an incident, it is prepared

with complete and timely information on asset inventories, configurations, and changes. It has also established and maintained plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities. Additionally, the organization ensures that its asset, threat, and vulnerability management actions are commensurate with the risk to its infrastructure (such as critical, IT, and operational technologies) and organizational objectives.

Q2c. Given that these issues exist around the world and not just the in United States, is there value in considering harmonizing global standards?

A2c. Guided by the Administration's Cyber Strategy to build partnerships with like-minded nations DOE supports public and private collaboration with global partners in areas of key interests. These partnerships better enable the understanding of emerging trends that can guide development of standards for further reduced risk to the global energy sector. DOE CESER led three international delegations in 2020 to cultivate information-sharing partnerships with our like-minded allies in order to better understand and characterize the threats we face. Through these partnerships, we can promote global standards that make it more difficult for threat actors to exploit our global connected energy systems. Additionally, DOE contributes to the energy sector's voluntary efforts to develop robust, open, transparent, consensus-based technical standards and best practices such as C2M2, through several different public forums, trade associations and working groups.

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Alexander Gates

QUESTIONS FROM SENATOR JAMES E. RISCH

Q1. Securing the nation's electric power grid is an essential effort to national security, but it's quite technical and complex. You have some of the brightest minds working for you at the nation's national laboratories, including the Idaho National Lab. I know this because I've toured the lab on many occasions and some of their engineers have testified before this committee in the past.

Can you tell me how the Department is encouraging collaboration among the national labs and with the private sector to meet some of the nation's most pressing energy security challenges? And can you provide recommendations on how to improve collaboration between DOE, the intelligence community and the energy sector to facilitate better information sharing and collaboration about threats to our critical infrastructure?

A1. DOE is actively encouraging and engaging in collaboration among the national laboratories and the private sector with the goal of addressing our Nation's energy security challenges. As an example, DOE has developed a multi-lab program, Cyber Testing for Resilient Industrial Control Systems (CyTRICS™) to test energy system components for cybersecurity vulnerabilities. CyTRICS features a risk-managed approach to selecting components for testing and a standardized, repeatable approach to testing and reporting results. CyTRICS involves collaborating with component manufacturers on the testing of their products to identify and mitigate key vulnerabilities. CyTRICS is at a development stage, but once fully implemented, will cover cyber vulnerability testing across the energy sector, including electricity, oil and natural gas, and renewables. The program depends on partnerships with the Idaho National Laboratory, Sandia National Laboratories, the Lawrence Livermore National Laboratory, the Pacific Northwest National Laboratory, and the National Renewable Energy Laboratory.

DOE is also working to improve collaboration with the private sector and the intelligence community via the Securing Energy Infrastructure Executive Task Force mandated by the FY2020 National Defense Authorization Act (NDAA), Section 5726. This Task Force supports a two-year pilot to collaborate with industry, the Federal government (including the intelligence community), State representatives, the national laboratories, and academia to develop a national cyber-informed engineering strategy to isolate and defend critical energy sector companies from security vulnerabilities and exploits in the most critical systems, evaluate the technology and standards used, and identify new classes of security vulnerabilities.

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Alexander Gates

DOE will also leverage the efforts of the Task Force to refine and improve the CyTRICS program and collaborate with industry partners on threats to the energy critical infrastructure.

Q2. In May, the President took decisive action against China by signing Executive Order 13920 to secure the U.S. Bulk Power System. The Department of Energy is the agency of record to implement the President's order.

Can you give the committee an update on the progress DOE has made to date on this order and a timeline for near-term actions?

A2. The Department of Energy (DOE or Department) is working closely with our interagency partners as well as with the private sector to implement Executive Order 13920 (EO 13920). DOE has held three open stakeholder calls with participation from more than 2,300 unique individuals representing over 900 organizations as part of its outreach efforts on EO 13920. These entities included vendors, manufacturers, utilities, public utility commissions, generators, and financial institutions. Additionally, the Department has held over 40 briefings with private sector companies, trade organizations, congressional offices, and Federal government entities.

As part of the rulemaking process, on July 8, 2020, DOE published a Request for Information (RFI) in the *Federal Register*.[1] The RFI seeks comments on specific equipment to enable a phased process by which the Department can prioritize the review of bulk-power system (BPS) electric equipment by function and impact to the overall BPS. The deadline for submission of comments was recently extended to August 24, 2020.[2]

Stakeholders will be able to provide the Department with comments on EO 13920 when a notice of proposed rulemaking is published, which is anticipated later this year. The Department will give full consideration to all comments we receive.

[1] 85 Fed. Reg. 41,023 (July 8, 2020), https://www.govinfo.gov/content/pkg/FR-2020-07-08/pdf/2020-14668.pdf.
[2] 85 Fed. Reg. 44,061 (July 21, 2020), https://www.govinfo.gov/content/pkg/FR-2020-07-21/pdf/2020-15848.pdf.

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Alexander Gates

The Department is also currently identifying individuals to participate in the Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security. DOE expects the first meeting of the Task Force to occur this fall.

Q3. During the FCC's 6 GHz rulemaking, I led a bipartisan letter with 11 of my colleagues expressing concerns about the sharing of unlicensed devices with protected incumbents– including electric utilities and public safety entities – in this band. Chairman Murkowski, DOE Assistant Secretary Bruce Walker, and FERC Chairman Neil Chatterjee also sent letters raising concerns.

Can you please outline DOE's work and engagement with the FCC regarding 6 GHz, and is your agency currently working with the FCC to ensure unlicensed devices will not cause interference within this critical band. Furthermore, the Idaho National Lab has unique wireless testing capabilities - has the FCC reached out to DOE to discuss the possibility of testing unlicensed devices to ensure there is no interference to incumbent electric utilities?

A3. On September 3, 2019, the Department of Energy (DOE or Department) sent a letter to FCC Chairman Pai to express concerns over the unlicensed use of the 6GHz band, and NTIA is currently working with DOE to file that letter into the FCC docket. In that letter, DOE emphasized the importance of secure communications for the energy and water industries. DOE stated that these industries "do not currently have any cost effective, readily achievable alternatives to the 6GHz band if the FCC proceeds with the existing proposal and damaging signal interference is realized." DOE emphasized the importance of adequate testing of the FCC proposed Automated Frequency Coordination (AFC) system before commingling occurs on the band. DOE recommended investigating a long-term solution for dedicated spectrum for critical infrastructure users in the energy and water sectors. DOE is currently working with NTIA to coordinate a briefing with FCC to discuss this matter.

Q4. In June, the Department of Defense released a list of Chinese companies operating in the United States that have links to the Chinese military. To no one's surprise, Huawei was included on that list. Congress and the Administration have already taken steps to ban the use of Huawei equipment from our nation's telecommunications networks, but Huawei also manufacturer's energy equipment - like solar inverters. Senator King and I led a letter to FERC in December regarding the national security threat these inverters pose to U.S. national security. To fully protect the electric grid from foreign intrusion, do you think the federal government should also consider barring Huawei equipment from being used on our electrical grid?

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Alexander Gates

A4. Several reports document Huawei's lax maintenance of routers and the possibility that vulnerabilities in communications equipment used by the power sector could be a vector for cyber threats to the grid. Recently, highlighting DOE's efforts in this space, a CESER-funded project identified activity associated with the Entity List maintained by the Department of Commerce. As supply chains are the preferred route of ingress for those seeking to attack the grid, it remains prudent for all stakeholders to employ appropriate measures that secure our infrastructure from the potentially harmful effects of malicious cyber actors.

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Alexander Gates

Question from Senator Bill Cassidy

Q1. Last year, this committee learned that one of the problems with information sharing was getting security clearances for partners in the private sector. Can you provide an update on the process to approve those security clearances?

A1. DOE sponsors clearances for appropriately vetted individuals. However, for the majority of the private sector, critical infrastructure owners and operators utilize the Department of Homeland Security's (DHS) Private Sector Clearance Program (PSCP).

DOE assists in the facilitation and streamlining of clearance processes by nominating individuals that are most likely to utilize a clearance. CESER plays an active role by nominating appropriate individuals for clearances, leveraging its understanding of the key roles and personnel throughout the energy sector. Below, are the number of active sponsored clearances that have been granted through the PSCP for our energy sector partners:

- 2016 – +37 clearance holders
- 2017 – +31 clearance holders (-8.9%)
- 2018 – +61 clearance holders (+32.6%)
- 2019 – +89 clearance holders (+18.7%)

* Percentages indicate differential from the previous calendar year throughput

Thus far in 2020, DOE has nominated 86 energy sector partners and 32 individuals, all of whom have been granted a clearance through the PSCP. Currently, CESER manages 559 clearances through the PSCP. When analyzing the number of all clearance holders for the entire PSCP, across all critical infrastructure sectors, approximately 30% are in the energy sector.

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Alexander Gates

Question from Senator Angus S. King, Jr.

Q1. What additional authorities does CESER need in order to allow the agency to carry out its mission of protecting the grid through critical vulnerability and penetration assessments (like red teaming and pen testing) of interstate grid networks, power stations and substations, dispatch centers, and other critical grid components?

A1. The Department of Energy (DOE) shares the Committee's views regarding the need to protect the U.S. energy grid and acknowledges that initiatives, such as those that involve the discovery of and assessments related to the vulnerability and penetration of critical grid components, can provide essential insights into those measures that need to be taken to ensure the security and resiliency of critical U.S. energy infrastructure.

In the event that Congress elects to authorize sufficient resources for the Department to carry out these activities, DOE believes that it possesses the necessary capabilities, expertise, and relationships required to support activities at varying levels under its current authorities. For those components of the energy system that are DOE-owned or operated assets, such as is the case with respect to DOE nuclear facilities, Power Marketing Administrations (PMA) and the Strategic Petroleum Reserve, DOE has sufficient authorities to conduct activities in accordance with existing laws and policies.

With respect to components of the U.S. energy grid that are owned or operated by private sector entities, DOE's role in this regard is more limited and is governed by a range of federal laws and policies, such as

- Section 61003c of Public Law 114–94, "FIXING AMERICA'S SURFACE TRANPORTATION ACT" (FAST Act);
- Executive Order 13636 (Improving Critical Infrastructure Cybersecurity);
- Presidential Policy Directive – 21 (Critical Infrastructure Security and Resilience); and
- Presidential Policy Directive – 41 (United States Cyber Incident Coordination).

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Alexander Gates

Questions from Senator Catherine Cortez Masto

Q1. Throughout your written testimony, you highlighted the importance of the Department of Energy's (DOE) partnerships with states. Specifically, you mentioned that this collaboration is vital for ensuring preparedness and a coordinated response, should a cyber attack occur.

Q1a. How is the federal government coordinating with state cyber offices, including the Nevada Office of Cyber Defense Coordination, to perform cyber threat analysis and report information on cyber threats?

A1a. The DOE works closely with the National Governors Association (NGA), the National Association of Energy Officials (NASEO), and the National Association of Regulatory Utility Commissioners (NARUC) to support state, local, tribal, and territorial (SLTT) energy officials. CESER collaborates with these groups to provide training, resources and technical assistance. A few recent cybersecurity focused projects include:

- Late last year, with support from CESER, NGA hosted an experts roundtable focused on energy cybersecurity coordination and information sharing among state, federal, and utility officials with a goal of drafting guidance on cybersecurity partnerships and information sharing for SLTT. Based on this expert input, DOE is supporting the development of guidance that will identify the State role in cybersecurity information sharing, demonstrate how cybersecurity information can be shared effectively, and detail how States can build and enhance relationships with industry and the federal government to ensure effective coordination before, during, and after a cybersecurity incident.

- Recently, NASEO, in cooperation with and under a work effort funded by CESER, released a report titled, "Enhancing Energy Sector Cybersecurity: Pathways for State and Territory Energy Offices." The report provides an overview of energy sector cybersecurity roles and responsibilities and identifies actions that State Energy Offices can take to enhance internal cybersecurity and support energy sector cybersecurity within their states. The report also provides contextual knowledge that will enable State Energy Offices to develop and implement cybersecurity programs and policies in partnership with federal and industry partners.

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: *An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives*
Questions for the Record Submitted to Mr. Alexander Gates

- NARUC, in coordination with CESER, holds regional in-depth cybersecurity training for public utility commissioners and staff to learn about important and fundamental cybersecurity concepts.

Q2. How important are international partnerships and collaboration with foreign allies in determining cyber threats?

A2. Cyber threats do not respect borders. The interconnected nature of the mission and threat spaces means that we must partner at all levels to succeed. For the energy sector, we have seen examples of foreign adversaries conducting malicious cyber operations on the electric grids and oil and natural gas pipelines in the U.S. and in other countries and regions. Consequently, it is critical for DOE to work with foreign partners to more fully understand the nature of and the specifics concerning such attacks to better inform our ability to harden U.S. energy critical infrastructure.

International partnerships also facilitate opportunities to share best practices, capacity building efforts, and training to enhance the ability of a partner foreign government and their energy sector to prepare for, determine, and respond to a cyber threat impacting the interconnected energy sector.

Q3. In August 2019, the Government Accountability Office published a report called, "Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid."

One of the three recommendations included in the report was the need for DOE to develop a nationwide plan aimed at implementing a federal cybersecurity strategy for the grid.

Q3a. Since the publishing of the report last August, what efforts have been made by the Department to develop a federal cybersecurity strategy for the grid?

A3a. CESER continues to implement on the Multiyear plan and coordinate across the interagency specific to the National Cyber Strategy (NCS). The process for implementing the strategy continues to progress and DOE recently updated two items for the NCS. Both provide more actions to DOE as lead or supporting agency.

Q4. As we look to deploy more EVs on our nation's roads and build-out necessary charging infrastructure, researchers and industry groups are working to identify where new cyber vulnerabilities may arise.

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Alexander Gates

Knowing that cyber attacks pose a threat as we expand EV charging infrastructure is one of the reasons why I introduced the Electric Transportation Commission and National Strategy Act (S. 2040) to require the Department of Transportation and the Department of Energy to work together in establishing a commission to strategize and report on opportunities and barriers, including cyber threats.

Q4a. How are DOE, FERC, utilities, and industry working together to ensure EV infrastructure will be able to withstand cyber threats in the future?

A4a. In all matters involving devices that connect to the electric grid, including electric vehicle infrastructure, DOE actively partners with all applicable public and private sector stakeholders, including FERC, utilities, and the electric industry. This partnership exists with the intent and goal of better understanding the nature and degree of the current and emerging cyber threats and vulnerabilities facing the energy sector. As an example, this partnership takes the form of threat information sharing through a myriad of existing cross-sector forums (e.g., Multi State Information Sharing Analysis Center and Electric Subsector Coordinating Council). Through these established trust relationships, critical context of cyber threats and vulnerabilities are timely shared with parties who are empowered with the "tools" to undertake prioritized actions to remediate and ensure their resiliency. DOE's subject matter expertise across the energy sector, including the electricity infrastructure, provides parties with an extra level of assurance that their remediation and resiliency actions are timely, warranted, and appropriate.

With respect to the cyber-physical security of EV charging, DOE EERE's Vehicle Technologies Office (VTO) has two current national laboratory projects that are developing advanced threat models for EV charging and identifying the most critical threat vectors. The VTO also supports a number of projects with industry and academia, focused on addressing threats to the EV charging ecosystem by developing new intrusion detection systems, developing advanced hardened software and hardware, developing moving target defenses, addressing over-the-air updates to EVs and chargers, and developing a cyber secure reference architecture for EV charging. With respect to industry collaborations, VTO recently awarded three industry Funding Opportunity Announcement (FOA) projects to establish utility managed Smart Charge Management systems focusing on identifying, detecting, responding to, and mitigating EV charging ecosystem cyber incidents.

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Alexander Gates

Q4b. Could a commission help boost collaboration among federal agencies, as well as with local, state, and industry stakeholders?

A4b. DOE is fully supportive of all congressional actions that strengthen information sharing and other types of collaboration between and among federal agencies with local, state, and industry stakeholders that further the goals of strengthening the energy infrastructure for the Nation. Prior to the establishment of any additional commission, DOE recommends a thorough congressional review be conducted to ensure duplication and overlap is avoided with existing collaboration type forums and bodies.

Q5. Our National Labs play an important role in creating and testing technologies to mitigate and address cyber threats to the energy sector and the electric grid.

Q5a. What more could the federal government be doing to promote the early adoption of the state-of-the-art technologies to protect our electrical infrastructure that are being developed by DOE and the National Labs?

A5a. DOE has developed and continues to expand a portfolio of programs, tools, and facilities that allow for greater industry input, access, and use of the DOE research and development (R&D) portfolio. Specifically, through DOE's Office of Technology Transitions (OTT) Lab-industry technology summits have showcased relevant technologies and facilities from across the Lab system and seeded public-private partnership arrangements around emerging technologies. The InnovationXLab Series® events generate hundreds of new Lab-industry connections around each event's focus—including grid and cybersecurity. OTT has also developed and continues to expand on the Lab Partnering Service, which is a web portal that allows easy access to information about national laboratory expertise, facilities, and intellectual property. To complement these industry access tools that facilitate "market pull," OTT also supports entrepreneurship from within the national laboratories through its Energy I-Corps program. This program provides hands-on, immersive training for Lab researchers with promising technologies to conduct extensive customer outreach to better understand the potential for commercialization of those technologies.

DOE has also established the first ever Chief Commercialization Officer, the Director of the Office of Technology Transitions, who is charged with leading the Department's efforts to connect our world-

class research and technology with the private sector, in an effort to better bridge the early adoption gap and bring DOE's innovative technologies to market.

Q5b. How are public-private partnerships helping to deploy those technologies and ensure that industry is trained and prepared to deploy new cybersecurity technologies?

A5b. To further efforts in deploying technologies, DOE is executing cooperative agreements with select entities to engage distribution and municipal utility companies to improve the cyber and physical security posture of the electric sector. These projects will enhance the reliability and resilience of the nation's energy infrastructure, specifically distribution and municipal utility companies, through the development, demonstration, and deployment of innovative cybersecurity solutions that:

- detect and respond to Cyber adversarial activity on operational technology (OT) networks in the energy sector through a community-based policing approach;
- use artificial intelligence (AI) to identify anomalies, reduce false positives, and update OT assets;
- provide for advanced analytics to enable the user the capability to identify the systems when and where compromised;
- increase system resilience in energy delivery control systems or components; and
- employ autonomous defense solutions at remote endpoints to protect against in band and out of band attacks.

CESER also provides guidance and support to energy sector organizations seeking to implement cybersecurity capabilities by increasing access to leading practices for the management of cybersecurity programs, all of which builds flexible and capable organizations that are better able to identify and prioritize cybersecurity technology deployments and provides a foundation to use new technologies effectively.

Lastly, CESER actively leverages exercises, trainings, and competitions, to bring novel technologies to industry and familiarize operators with technology in highly-controlled and realistic environments—particularly those where the use of such technologies can be simulated in near-real-world scenarios.

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Joseph McClelland

Questions from Ranking Member Joe Manchin III

Question 1: The Eastern Interconnection Planning Collaborative filed comments in Docket No. IC20-13-000 regarding concerns that FERC's current process for designating and protecting Critical Electric Infrastructure Information (CEII), required by the FAST Act, is insufficient to guard against sensitive transmission infrastructure information falling into the wrong hands.

a. Has FERC considered amending the treatment of CEII in ways that would address some of the concerns outlined here?

Response:

FERC's CEII process is designed to protect CEII information and to limit the sharing of such information in order to avoid having it fall into the wrong hands. FERC established this process so that a legitimate individual with a valid need may request access to CEII.

Before the Commission discloses CEII to a requestor, the following steps must be taken. A requestor must submit a detailed statement demonstrating and attesting to his need for the information. With its request, the requestor also must submit an executed FERC non-disclosure agreement (NDA) to the Commission, which along with the Commission's regulations governs the requestor's use of the CEII. No CEII is disclosed, however, until after FERC staff verifies the requestor's statement of need and confirms that the CEII requestor is legitimate. Staff is also required to seek the input of the submitter of any CEII and provide an opportunity for the submitter to comment on the request. In deciding whether to disclose or not, FERC's CEII Coordinator is required to "balance the requester's need for the information against the sensitivity of the information." I note that in addition to the process I describe above, the Commission's regulations also allow it to impose additional conditions on a requester's access to CEII beyond what the standard NDA requires. For every request, the Commission not only applies the process described above but also considers if it is appropriate to place additional requirements and limitations on the requester's use of the CEII.

In the event an NDA is breached, the Commission has the authority to impose sanctions and prohibit a requester from receiving CEII in response to any future requests. Further, an individual who purposely falsifies a request for CEII could be subject to criminal prosecution under 18 U.S.C. § 1001.

To date, FERC staff has no basis for concluding that the NDAs have been ineffective in protecting the unauthorized disclosure of CEII. In particular, FERC staff is not aware of any instances of an intentional breach of an NDA. However, FERC staff is always open to considering ways in which the Commission may improve its regulations and processes. As an example, in addition to its own substantial analysis of a CEII request, FERC staff is open to extending submitters additional time if needed to more expansively present additional documentation which credibly examines the

legitimacy, validity, and the probability of misuse of a CEII request and the detrimental consequences.

Question 2: The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) recently came out with an advisory recommending the reduction of operational technology and control systems exposure.

a. Is FERC using these recommendations to inform your guidance and potential regulatory activities?

Response:

Yes, FERC is aware of these recommendations. FERC staff works closely with DHS CISA, NSA, DOE, ODNI, and our other federal partners to stay informed of the current threats against the energy infrastructure under our jurisdiction as well as the measures that can be used to mitigate them. FERC uses this information in a dual-fold approach: employing mandatory reliability standards to establish foundational practices as appropriate while also working collaboratively with industry, the states and other federal agencies to identify and promote best practices.

b. Do you have plans to address asset management and vulnerability management to understand in real time which assets and technologies are connected to energy networks, and how organizations should be prioritizing vulnerabilities that are discovered in their networks and systems?

Response:

Yes, FERC staff offers guidance through industry outreach recommending that they consider the installation of dynamic asset management programs to automatically and quickly detect unknown equipment connected to their networks so that unauthorized access can be immediately blocked. Staff recommends that mitigating actions should be prioritized consistent with the National Institute of Standards and Technology (NIST) Cyber Security Framework (NIST Framework), which states that they be "identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy."[1] I also note that on June 18, 2020, FERC staff issued a white paper that sought input on how the Commission may provide incentives to entities to make cybersecurity investments so that those entities may prioritize investments to address these

[1] In the NIST Framework, Dynamic Asset Management can be found within the Identify (ID) Function in the Asset Management Category (ID.AM) which states: "The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy."

types of issues, including investment in cybersecurity practices that exceed the regulatory requirements of the NERC Critical Infrastructure Protection (CIP) Reliability Standards.[2] The comment period for the staff white paper has closed and FERC staff is reviewing those comments.

c. Given that these issues exist around the world and not just the in United States, is there value in considering harmonizing global standards?

Response:

When identifying vulnerabilities, threats, and effective mitigations, the Commission's work is informed by cybersecurity events that occur around the world, using them as appropriate to help inform regulatory actions.

Question from Senator James E. Risch

Question: In June, the Department of Defense released a list of Chinese companies operating in the United States that have links to the Chinese military. To no one's surprise, Huawei was included on that list. Congress and the Administration have already taken steps to ban the use of Huawei equipment from our nation's telecommunications networks, but Huawei also manufacturer's energy equipment - like solar inverters. Senator King and I led a letter to FERC in December regarding the national security threat these inverters pose to U.S. national security. To fully protect the electric grid from foreign intrusion, do you think the federal government should also consider barring Huawei equipment from being used on our electrical grid?

Response:

I agree that any equipment that jeopardizes the security of our critical infrastructure, including the electric grid, should be barred from use. I note that the FCC, the Department of Commerce, and Congress have raised concerns regarding the use of Huawei in our critical infrastructure.

---

[2] Cybersecurity Incentives Policy White Paper, Docket No. AD20-19-000 (Issued June 18, 2020). That staff white paper, which is still under review, notes that "[an] installation of a dynamic asset management program to improve a utility's ability to quickly detect and address new or previously unknown equipment on its network is an example of a cybersecurity investment that may be eligible for an incentive under the automated and continuous monitoring security control type." White Paper at p. 20. The staff white paper also notes that "[u]nknown and unattended equipment can present significant vulnerabilities and threats to both the information technology and operational technology networks. Implementing a process that automatically and continuously scans the current inventory of hardware and software across both the information technology and operational technology networks can identify and block any unauthorized access." White Paper at p. 58.

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: *An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives*
Questions for the Record Submitted to Mr. Joseph McClelland

Regarding protection of our electric grid from foreign intrusion, I'd like to note here that on May 1, 2020, the President issued Executive Order 13920 (EO) titled "Securing the United States Bulk-Power System." The President determined that "the unrestricted foreign supply of bulk-power system electric equipment constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States, which has its source in whole or in substantial part outside the United States." He declared a national emergency with respect to the threat to the United States bulk-power system and DOE was named as the lead agency. Among other actions, the EO prohibited transactions of bulk-power system electric equipment "by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary." On July 8, 2020, DOE issued a request for information naming six foreign adversaries, including China, and asking for industry comment regarding potential actions it could take to protect the bulk-power.

Questions for the Record Submitted to Mr. Joseph McClelland
from Senator Cortez Masto

Question 1: In August 2019, the Government Accountability Office (GAO) published a report called, "Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid."

Two of the three recommendations included in the report were directed at the Federal Energy and Regulatory Commission (FERC), including: (1) altering FERC's approved cybersecurity standards to better incorporate the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and (2) evaluating and crafting proposals to better account for the potential risk of a coordinated cyberattack on geographically distributed targets.

a. Since the publishing of the report last August, what efforts have been made by FERC to incorporate GAO's recommendations?

Response:

Based on the August 2019 GAO report, FERC staff undertook a comprehensive review of the National Institute of Standards and Technology (NIST) Cyber Security Framework (NIST Framework), comparing its content with the NERC Critical Infrastructure Protection (CIP) Reliability Standards, and identified certain topics addressed in the NIST Framework that may not be adequately addressed in the CIP Reliability Standards. Based on this analysis, on June 28, 2020, the Commission issued a Notice of Inquiry seeking comment on whether the CIP Reliability Standards adequately address cybersecurity risks pertaining to data security, detection of anomalies and events and mitigation of cybersecurity events, noting the NIST provisions on these topics.[3] In addition, the Commission also asked for comments on the risk of a coordinated cyberattack on the bulk electric system as well as potential

[3] Potential Enhancements to the Critical Infrastructure Protection Reliability Standards, Notice of Inquiry, 171 FERC ¶ 61,215 (June 18, 2020).

approaches to address the matter, such as voluntary or mandatory participation in grid exercises, other types of training to prepare for a coordinated attack, and modifications to the current applicability thresholds in the CIP Reliability Standards

Initial comments were due on August 24, 2020, and reply comments are due on September 21, 2020.

Question from Senator John Hoeven

Question: We understand that FERC is exploring whether to provide incentives to utilities for cybersecurity advancements, given the importance of electric reliability to our society. FERC's recent proposal focuses primarily on incentivizing new capital investments. I understand many cyber activities are related to human capital, like hiring the right people and training them in new procedures. Has FERC considered approaches that would incentivize utilities for these types of activities, in addition to looking at capital investments?

Response:

On June 18, 2020, the FERC staff issued a white paper that sought input on how the Commission may provide incentives to entities to make cybersecurity investments. The main focus of the staff white paper is to explore a new framework for providing transmission incentives to utilities for cybersecurity investments that produce significant cybersecurity benefits for actions taken that exceed the requirements of the NERC Critical Infrastructure Protection Reliability Standards.[4] However, the paper solicits comments from the public on other ways in which the Commission may provide an incentive to address cybersecurity issues. The comment period on the white paper has closed and FERC staff is reviewing those comments.

[4] Cybersecurity Incentives Policy White Paper, Docket No. AD20-19-000 (Issued June 18, 2020).

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Steve Conner

Responses from Mr. Steve Conner
President
Siemens Energy, Inc.

Questions from Ranking Member Joe Manchin III

Question 1: The bulk power system Executive Order 13920 (EO) established a Task Force to engage with the energy industry, but manufacturers were not specifically included in that process.

a. Do you think a Task Force equivalent to the one in the EO for the manufacturers of electric equipment to inform the Department of Energy would be helpful?

Siemens Energy, Inc Answer 1a: Siemens Energy is constantly looking for additional ways to engage the public sector, including supporting vendor-driven forums that would improve industry involvement and promote wider discussion on vulnerabilities and supply chain risks. We would welcome every opportunity to have specific conversations with the Department of Energy to be able to share the perspective of one of the largest manufacturers in the world of equipment in the U.S. bulk power system.

b. How has Siemens engaged with the Department of Energy on this EO?

Siemens Energy, Inc. Answer 1b: Siemens Energy has been a reliable partner to the United States government for decades. We have a deep understanding of the safest and most resilient infrastructure technologies and processes necessary to secure one of our most essential national assets, America's power grid. We have shared this expertise directly with the Department of Energy and have expressed our commitment to support its efforts to implement Executive Order 13920 (EO). We have participated in the multiple public stakeholder briefings hosted by Department officials. The trade associations in which we are involved have also facilitated dialogue between the Department and industry.

Question 2: The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) recently came out with an advisory recommending the reduction of operational technology and control systems exposure.

a. Is Siemens familiar with the NSA/CISA guidance? If so, how are you implementing the practices recommended in the guidance?

Siemens Energy, Inc. Answer 2a: Siemens Energy is aware of NSA/CISA Alert AA20-205A which articulates a growing threat to our nation's critical infrastructure (CI) through the exploitation of internet-accessible operational technology (OT) assets. As a highly experienced partner and advisor, Siemens Energy has worked to meet this threat through a holistic risk-based approach that starts with our supply chain and extends all the way to our installed and

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Steve Conner

commissioned OT assets of our customers. Siemens Energy leverages its experience, expertise and industry partnerships to advance the OT cybersecurity industry by promoting and contributing to cyber information sharing organizations as well as developing and providing mitigation techniques and tools to our customers.

Siemens Energy currently implements the practices recommended by NSA/CISA Alert AA20-205A as part of our ongoing defense in depth approach to OT cybersecurity. Our products and solutions have industrial security functions that are built-in by design, enabled by default, and follow leading industrial standards such as ISO/IEC27001, ISA/IEC62443, and ISO/IEC27005. Additionally, we offer solutions and services to our customers that bring greater visibility to their system-wide risk profile by developing resilience plans, detecting security risks, mitigating security gaps, continuously monitoring their systems and helping to recover from a successful security incident.

Questions from Senator Mazie K. Hirono

Question 1: What are some of the cybersecurity benefits and risks that arise as power systems incorporate larger shares of distributed, variable, renewable power sources and energy storage. What steps should regulators, owners, and operators of assets in the power sector take to take advantage of the benefits and reduce the risks?

Siemens Energy, Inc. Answer 1: There are several ways in which a growing share of distributed renewable energy generation resources can increase the resilience of our energy systems and support the deployment of more renewable energy. Many smaller generation facilities are more difficult to target and disable at a scale that would have a similar impact to disabling a large centralized generation resource. Grid islanding using distributed renewable generation and energy storage can also protect critical facilities in the event of a cybersecurity attack on the grid operator as well as increase resilience during natural disasters such as hurricanes or earthquakes.

Siemens Corporation[1], through the AUtonomous and Resilient Operation of energy systems with high RenewAbles (AURORA) project, is developing these technologies for cyberattack detection and continuity of services during and after these attacks together with Holy Cross Energy, Columbia University, and the National Renewable Energy Laboratory.

The National Renewable Energy Laboratory (NREL) has also produced a set of recommended best practices for cybersecurity of distributed energy resources (DERs), which include: 1) an emphasis on strong cybersecurity governance to identify risks proactively, including within the supply chain; 2) cyber-physical technical management to control and restrict digital access to critical systems; and 3) physical security measures to protect systems from physical (non-networked) intrusion.

[1] Siemens Energy, Inc. is a separate legal entity from Siemens Corporation

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Steve Conner

Question 2: In your opinion, are industrial control systems in the energy sector more secure as the technology becomes better (e.g., use of advanced encryption algorithms), or are we losing ground because these systems are becoming more complex and inherently more vulnerable to advanced persistent cyber threats?

Siemens Energy, Inc. Answer 2: Industrial control systems in the energy sector have become more secure in part because of advances in technology, but perhaps more importantly because of a growing acceptance of cybersecurity as a foundational element of a holistic risk management process. Cybersecurity has moved from being a compliance driven afterthought to a competitive advantage with many energy providers elevating cybersecurity to a board level consideration. Our customers are investing in cybersecurity because they see the strategic benefits to their overall competitiveness and the enhanced ability to better serve their end customers. Public and private entities across the energy CI sector continue to bring IT and OT systems together to address the challenges associated with a changing workforce, the need for greater workflow efficiency, and a need for more flexible and real time control of geographically distributed and intermittent energy assets. A shift away from a digitally controlled energy sector will almost certainly increase energy costs to end users, reduce energy sector flexibility and resilience.

The tools to understand, detect, mitigate and continuously monitor for risks in these complex systems have never been easier to use. Siemens Energy has a wide portfolio of solutions and services that we offer to our customers, at reasonable cost, that bring visibility to assets, "as-operated" network architectures, device and system configurations, and can provide advanced features like vulnerability management and anomaly detection. Legacy OT systems may now utilize similar detection, protection and mitigation tools that were previously only available for Enterprise IT networks.

Questions from Senator Catherine Cortez Masto

Question 1: In July 2019, Jim Robb, President and CEO of the North American Electric Reliability Corporation, told the House Energy Subcommittee that it is important for the federal government to be able to rapidly declassify information in order to get the pertinent information to industry so they can act.

a. In your opinion, have the pipelines for information sharing improved over time?

b. How can information sharing be further improved, and are there ways Congress can help facilitate stronger collaboration and communication among the state, federal, and industry partners?

Siemens Energy, Inc. Answer 1a & 1b: The pipeline of information sharing has improved for specific threat information as well as general cybersecurity best practices and approaches. Authorities, operators and vendors are much more connected than in the past, and the energy industry has seen cybersecurity elevated to become a foundation of a competitive, connected, flexible and resilient energy system. In recent years, the release of NERC CIP alerts, CISA's recent "Guidance on the Essential Critical Infrastructure Workforce" and the "Cybersecurity

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Steve Conner

Practices for Industrial Control Systems" infographic have made cybersecurity for CI more accessible and taken the complexity out of the connection between operational excellence and cyber resilience.

Congress can help to facilitate stronger collaboration and communication between government and industry partners by supporting efforts to embed cybersecurity best practices within operational reliability guidelines. At Siemens Energy, we feel that cybersecurity is a foundational enabler for secure energy operations. Bringing cybersecurity to non-experts is done by taking the complexity out of interpreting existing standards. Government is well suited to support industry by providing case studies, examples, references, tips, and explicitly referencing existing standards such as IEC62443, ISO27001 and the NIST Cybersecurity Framework within guidelines such as the NERC CIP Reliability Standards used by the energy sector. Additionally, Congress can support collaboration of government and industry by supporting and growing training programs, like NIST's National Initiative for Cybersecurity Education, that connect emerging cyber talent with roles in industry.

Question 2: Are existing regulations and executive orders adequately motivating private action to improve cybersecurity?

Siemens Energy, Inc. Answer 2: Existing critical infrastructure protection (CIP) reliability standards are technically comprehensive and complete and understood best by experienced cybersecurity professionals. However, due to their technical complexity they are functionally challenging to navigate for most critical infrastructure owners and operators.

The specialized language used in the standards adversely impacts their full adoption by business operation focused asset owners. It drives operators to assume the implementation will be complex and burdensome to their businesses. New technologies such as cloud computing, artificial intelligence, edge devices and blockchains are also now entering the market and will have tremendous benefit in mitigating cybersecurity risk. Complex and technical regulatory language should not act as a disincentive to investing in and deploying these new tools before the full benefits can be realized.

To ensure the continued use of appropriate risk assessment, protection and compliance measures, while still driving the adoption of new secure technologies, explicitly mapping to existing standards such as IEC62443, ISO27001 and the NIST Cybersecurity Framework and providing sufficient case studies, examples, references and tips would improve overall usability of the critical infrastructure protection (CIP) reliability standards.

Question 3: As we look to deploy more EVs on our nation's roads and build-out necessary charging infrastructure, researchers and industry groups are working to identify where new cyber vulnerabilities may arise.

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Steve Conner

Knowing that cyber attacks pose a threat as we expand EV charging infrastructure is one of the reasons why I introduced the Electric Transportation Commission and National Strategy Act (S. 2040) to require the Department of Transportation and the Department of Energy to work together in establishing a commission to strategize and report on opportunities and barriers, including cyber threats.

a. How are DOE, FERC, utilities, and industry working together to ensure EV infrastructure will be able to withstand cyber threats in the future?

Siemens Energy, Inc. Answer 3a: The Department of Energy through the Vehicle Technology Office (VTO) has a Grid and Infrastructure Program which has multiple goals, including understanding and addressing potential cyber-physical security challenges. VTO has worked collaboratively with stakeholders, including manufacturers, utilities, and the National Labs. The work focuses on a range of topics, including modeling threats, analyzing different scenarios, and supporting the advancement of mitigation solutions.

b. Could a commission help boost collaboration among federal agencies, as well as with local, state, and industry stakeholders?

Siemens Energy, Inc. Answer 3b: Siemens eMobility[2] is a leader in transportation electrification with 7 market factories/operations in the U.S., 65,000 charge points across North America, and continuing R&D efforts that develop the next generation of innovative technology. It offers customers an end-to-end set of solutions for EV infrastructure (chargers, power supply equipment, planning & consulting, managed cloud services, as well as options like battery storage and other renewable integration). To protect these systems deployed at customer sites and within Siemens, it implements – and continuously maintains – a holistic, state-of-the-art cybersecurity strategy leveraging Siemens products and solutions as well as from leading suppliers in the industry. In addition to providing service to customers, it is also committed to transportation electrification and the role it will play in Siemens reaching its goal of becoming carbon neutral by 2030.

Siemens supports the goal of further collaboration between federal partners including the Department of Energy, Department of Transportation, and FERC; standards organizations, such as NIST; and EV stakeholders. Greater collaboration and support will help lead to further cybersecurity assurances, rapid expansion of critical EV technologies, infrastructure, and jobs in the transportation electrification space.

Question 4: Our National Labs play an important role in creating and testing technologies to mitigate and address cyber threats to the energy sector and the electric grid.

a. How are public-private partnerships helping to deploy those technologies and ensure that industry is trained and prepared to deploy new cybersecurity technologies?

[2] Siemens Energy, Inc. is a separate legal entity from Siemens Corporation

U.S. Senate Committee on Energy and Natural Resources
August 5, 2020 Hearing: ***An Examination of Federal and Industry Efforts to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration on Various Cybersecurity and Critical Infrastructure Protection Initiatives***
Questions for the Record Submitted to Mr. Steve Conner

Siemens Energy, Inc. Answer 4a: Siemens Energy supports a robust apprenticeship program with several local high school and community college campuses in Charlotte, NC. We also recently announced a new collaboration with New York Power Authority (NYPA) to develop an industrial cybersecurity Center of Excellence. The partnership is intended to bring the public and private sectors together in order to develop innovative cybersecurity best practices that will serve as a model for deployment at other utilities. The first-of-its-kind industrial cybersecurity monitoring, research and innovation center will focus on detecting and defending against cyberattacks on critical infrastructure owned and operated by NYPA, the largest state-owned electric utility in the nation.

The announcement is the first step in bringing together a coalition of public sector, private industry and academic partnerships that will build core capabilities needed to identify new and existing cyber threats, adopt new technologies to protect digital infrastructure and close the industry's talent-gap. Successful solutions have the potential to be deployed and commercialized at other public and private organizations that operate critical infrastructure systems in the state of New York and beyond.

U.S. Senate Committee on Energy and Natural Resources

August 5, 2020 Hearing: *An Examination of Federal and Industry Efforts*

to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration

on Various Cybersecurity and Critical Infrastructure Protection Initiatives

Questions for the Record Submitted to Mr. Thomas F. O'Brien

Questions from Ranking Member Joe Manchin III

Question 1: The Eastern Interconnection Planning Collaborative, of which PJM is a party, filed comments in Docket No. IC20-13-000 regarding concerns that FERC's current process for designating and protecting Critical Electric Infrastructure Information (CEII), required by the FAST Act, is insufficient to guard against sensitive transmission infrastructure information falling into the wrong hands.

a. Could you further elaborate on your concerns regarding FERC's process related to CEII?

Critical Energy Infrastructure Information (CEII) refers to specific engineering, vulnerability or detailed design information about proposed or existing critical infrastructure that: 1) relates details about the production, generation, transportation, transmission or distribution of energy; 2) could be useful to a person in planning an attack on critical infrastructure; 3) is exempt from mandatory disclosure under the Freedom of Information Act; and 4) does not simply give the general location of the critical infrastructure. With this in mind, CEII clearly represents data that would prove useful to an adversary in planning a disruption to the bulk electric system that serves this nation.

The Eastern Interconnection Planning Collaborative (EIPC) is a coalition of nineteen regional Planning Authorities that collectively represent more than 95% of the electricity capacity of the Eastern Interconnection. In essence, the EIPC members are those entities with direct responsibility to plan and operate the grid to ensure its safety, reliability and security. On May 8, 2020 the EIPC filed Comments with the FERC raising concerns that individual EIPC members had expressed for some time as to the Commission's procedures for release of CEII information to members of the public. The EIPC Comments were filed with reference to FERC's stated intent to make no changes to the information requested of those members of the public seeking to obtain CEII information. A copy of the EIPC Comments is attached to this submittal.

The EIPC Comments urge FERC to approach requests from members of the public for CEII based on a showing of the requestor's 'need to know' the requested information. The EIPC filing notes that the present showing requires only a cursory statement as to the requestor's proposed use of the information and provides, as its only means of enforcement, the signing of a non-disclosure agreement.

Given the recent tightening of the CEII rules through Congressional changes adopted in the FAST Act, the EIPC members believe that a corresponding set of controls are needed at FERC to better ensure that CEII information not end up in the hands of those seeking to disrupt grid operations or otherwise harm critical electric infrastructure. The EIPC looks forward to hearing from FERC on this request and working with this Committee as well.

U.S. Senate Committee on Energy and Natural Resources

August 5, 2020 Hearing: *An Examination of Federal and Industry Efforts*

to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration

on Various Cybersecurity and Critical Infrastructure Protection Initiatives

Questions for the Record Submitted to Mr. Thomas F. O'Brien

b. Have you engaged FERC further with these concerns?

We have discussed our concerns through helpful meetings with various FERC offices. To date, we have not received a response as to whether and how FERC will address those issues.

Question 2: The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) recently came out with an advisory recommending the reduction of operational technology and control systems exposure.

a. Is PJM Interconnection familiar with the NSA/CISA guidance? If so, how are you implementing the practices recommended in the guidance?

PJM monitors threat intelligence from government and non-government sources, reviews recommendations, and prioritizes work to apply applicable mitigations. PJM is familiar with the alert released by CISA (AA20-205A) in July 2020, which provided recommended actions to reduce exposure across operational technology (OT) networks. Specifically, PJM has technology and extensive training to help reduce the risk of spear phishing, protections against malware on OT systems, protected network access for all OT systems, and controls to protect vendor downloads.

The NSA/CISA guidance is complementary to the NERC Cybersecurity Infrastructure Protection (CIP) standards. The NSA/CISA guidance is also complementary to the National Institute of Standards and Technology (NIST) cybersecurity framework that PJM utilizes. We implement those practices using the principles of Identify, Protect, Detect, Respond, and Recover. These principles support the management of cybersecurity risks within the organization:

i. Identify - Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
ii. Protect – Develop and implement appropriate safeguards to ensure delivery of critical services.
iii. Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
iv. Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident
v. Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

U.S. Senate Committee on Energy and Natural Resources

August 5, 2020 Hearing: *An Examination of Federal and Industry Efforts*

to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration

on Various Cybersecurity and Critical Infrastructure Protection Initiatives

Questions for the Record Submitted to Mr. Thomas F. O'Brien

Questions from Senator Catherine Cortez Masto

Question 1: In July 2019, Jim Robb, President and CEO of the North American Electric Reliability Corporation, told the House Energy Subcommittee that it is important for the federal government to be able to rapidly declassify information in order to get the pertinent information to industry so they can act.

a. In your opinion, have the pipelines for information sharing improved over time?

PJM participates in the Cyber Risk Information Sharing Program (CRISP), managed by the Electricity Information Sharing and Analysis Center (E-ISAC). This program has made great progress in rapidly sharing government-informed threat intelligence with participating energy sector companies with actionable and applicable information that is not classified.

Other pipelines of information sharing have also improved. DOE, DHS, and the E-ISAC have provided more information related non-classified information and indicators of compromise without disclosing the classified information including details related to attribution.

b. How can information sharing be further improved, and are there ways Congress can help facilitate stronger collaboration and communication among the state, federal, and industry partners?

Threat information sharing is a matter of national security. Threat intelligence resides between many federal and state government agencies. Additional integration of threat intelligence across these agencies would be valuable to expose potential common threat vectors and identify potential gaps between intelligence agencies.

Additionally, further integration of threat intelligence data across critical infrastructure sectors including energy, telecommunications, finance, water and manufacturing would be valuable.

Federal government investment to support public and private partnerships similar to CRISP would allow for broader participation particularly from smaller companies. There is also significant technology investment needed for analysis of these large data sets including machine learning, advanced analytics and artificial intelligence. Technology investment for integrating cross sector real-time data with classified information and turning that into actionable de-classified information would prove valuable to industry and government. Programs like CRISP demonstrate what the electricity industry is doing to share information with the US Government, and in-turn, receive actionable threat intelligence.

The Cyberspace Solarium Commission (CSC) and the National Infrastructure Advisory Council both generated reports and recommendation that have the potential to lead to actionable solutions to improve information

U.S. Senate Committee on Energy and Natural Resources

August 5, 2020 Hearing: *An Examination of Federal and Industry Efforts*

to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration

on Various Cybersecurity and Critical Infrastructure Protection Initiatives

Questions for the Record Submitted to Mr. Thomas F. O'Brien

sharing as well as improve the overall protection of the nation from a significant cyber-attack. Congress can continue to advocate for these recommendations and work to ensure federal government, state government and industry stay aligned.

Question 2: As we look to deploy more EVs on our nation's roads and build-out necessary charging infrastructure, researchers and industry groups are working to identify where new cyber vulnerabilities may arise.

Knowing that cyber attacks pose a threat as we expand EV charging infrastructure is one of the reasons why I introduced the Electric Transportation Commission and National Strategy Act (S. 2040) to require the Department of Transportation and the Department of Energy to work together in establishing a commission to strategize and report on opportunities and barriers, including cyber threats.

a. How are DOE, FERC, utilities, and industry working together to ensure EV infrastructure will be able to withstand cyber threats in the future?

DOE, FERC, and utilities support the use of a cybersecurity framework to manage cybersecurity. The cybersecurity framework represents best practices that should be utilized for distributed technology and the internet of the things including EV charging stations.

While EV charging stations and other distributed technologies are included in the distribution system, a simultaneous mass disruption of these devices could affect the bulk power system. This will be particularly relevant as the penetration of these technologies increase. When considering distributed technology and the internet of the things a question must be answered, as to whether or not and if so when, they should be required to have mandatory cyber infrastructure protection standards. This discussion is underway within government agencies and industry and has been a topic with respect to the cybersecurity supply chain. No conclusion has been reached at this point and should be considered from a risk-based approach. When practical, a policy to utilize a NERC CIP approach to a broader set of assets could be warranted.

b. Could a commission help boost collaboration among federal agencies, as well as with local, state, and industry stakeholders?

I would suggest we utilize existing agencies with specific accountability to consider these threats. It is important that there is clear direction, and reducing the number of agencies or commissions would simplify the process. Given the mission of DHS and its cross-sector focus, DHS could be a good lead agency to boost collaboration

U.S. Senate Committee on Energy and Natural Resources

August 5, 2020 Hearing: *An Examination of Federal and Industry Efforts*

to Improve Cybersecurity for the Energy Sector, including How to Improve Collaboration

on Various Cybersecurity and Critical Infrastructure Protection Initiatives

Questions for the Record Submitted to Mr. Thomas F. O'Brien

among federal agencies as well as with local, state and industry stakeholders. In many respects, DHS is doing that today.

Question 3: Our National Labs play an important role in creating and testing technologies to mitigate and address cyber threats to the energy sector and the electric grid.

a. What more could the federal government be doing to promote the early adoption of the state-of-the-art technologies to protect our electrical infrastructure that are being developed by DOE and the National Labs?

The DOE creates many funding opportunities for academia, private industry, and the National Labs to collaborate on creating and testing technologies to secure the electric grid. Most notably, the Cybersecurity for Energy Delivery Systems (CEDS) has funded research that would be too risky for private industry to fund and conduct in isolation. This pipeline of research has resulted in commercial products, as research matures into marketable results. The federal government should continue to fund targeted basic research, like this, to promote further research to find innovative approaches to mitigating cyber threats. The National Labs have been impressive in developing relevant basic research, pilots, and proof-of-concept initiatives. The most important aspect would be to accelerate the pace of technology transformation through partnerships with industry and vendors.

b. How are public-private partnerships helping to deploy those technologies and ensure that industry is trained and prepared to deploy new cybersecurity technologies?

The most successful public-private partnerships resulting from the DOE and National Labs are those that can be commercialized and produced by suppliers at a reasonable cost to energy sector customers. These partnerships generally use the advanced research capabilities of the National Laboratories, the resources of commercial suppliers, the innovation of universities, and the expertise of electric industry advisors. This allows each type of organization to apply their strengths and resources to the benefit of the entire electricity industry. This makes new technologies accessible to the private sector without bearing all of the cost and risk associated with product research.

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Re: Commission Information Collection Activities Docket No. IC20-13-000
FERC Form 603 re: Requests for CEII

COMMENTS OF THE EASTERN INTERCONNECTION PLANNING COLLABORATIVE

The Eastern Interconnection Planning Collaborative (EIPC), a coalition of nineteen regional Planning Authorities that collectively represent more than 95% of the electricity capacity of the Eastern Interconnection, appreciates this opportunity to comment on the Federal Energy Regulatory Commission's (Commission's) proposal, as set forth in its March 23 Notice and Request for Comments ("March 23 Notice"), to extend FERC Form 603 with no changes to the current reporting requirements.[1]

As noted in the Commission's March 23 Notice, Form 603 is a request form submitted to the Commission by individuals seeking to obtain Critical Energy/Electric Infrastructure Information (CEII) from the Commission. With the exception of requiring a signature from the entity attesting to the accuracy of the information provided, the Commission proposes no changes to the form. March 23 Notice at p. 4. For the reasons stated below, the EIPC urges the Commission to revamp Form 603 (and the associated CEII process, which utilizes the information obtained in that form) rather than continue to utilize a form which, in the EIPC's view, does not provide adequate protections against the release of CEII (and specifically the detailed grid information included in Parts 2, 3 and 6 of FERC Form 715). EIPC seeks the opportunity to work with the Commission and its Staff on reforms that would ensure adequate protection of this CEII information while also respecting access to this information by stakeholders where warranted.

Description of the EIPC

The EIPC is a coalition of nineteen regional Planning Authorities that collectively represent more than 95% of the electricity capacity of the Eastern Interconnection.[2] The EIPC undertakes numerous interconnection-wide coordination activities including a

[1] While ISO New England, Inc. is a member of EIPC, it does not join in this submittal.
[2] The Planning Authorities which constitute the EIPC are Associated Electric Cooperative, Cube Hydro Carolinas, Dominion Energy South Carolina, Duke Energy-Carolinas, Duke Energy-Florida, Duke Energy-Progress, Florida Power & Light, Georgia Transmission Corporation, ISO-New England, LGE/KU (Louisville/Kentucky Utilities), MidContinent ISO, Municipal Electric Authority of Georgia, New York ISO, PJM Interconnection, PowerSouth Energy Cooperative, Santee Cooper, Southern Company, Southwest Power Pool and the Tennessee Valley Authority.

periodic 'roll-up' review of each EIPC Member's transmission expansion plans so as to ensure that the transmission planning activities of the individual EIPC members are coordinated on an interconnection-wide basis in order to maintain and enhance the reliability of the Eastern Interconnection as a whole. This information, together with additional detail on the EIPC and its initiatives, is made available to policy-makers and regulators at www.eipconline.org.

Concerns of the EIPC With the Present Content of Form 603

Members of the EIPC all share the same priority: delivering reliable electric energy to our respective customers. An important aspect of promoting reliability is the protection of data and information that could be used to identify and exploit vulnerabilities in the electric grid. This was an initial driver for the Commission to reconsider its treatment of data related to CEII following the September 11 attacks. Through the Fixing America's Surface Transportation Act signed by the President on December 4, 2015, Congress underscored its intention that this critical information be adequately protected. *See e.g.* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, 61,003, 129 Stat. 1312, 1773-1779 (2015) (to be codified at 16 U.S.C. 824 *et seq.*).

The EIPC is concerned that the requirements of Form 603 are insufficient to guard against transmission related CEII falling into the wrong hands. Specifically, Form 603 would allow for access to certain highly confidential information embodied in Parts 2, 3 and 6 of FERC Form 715. In fact, the Commission frequently receives and grants public requests for FERC Form 715 data under its existing CEII procedures. Parts 2, 3 and 6 of the Form 715 report includes data that arguably, in the past, may not have been sufficient for malicious actors to use in planning an attack on the bulk power system. However, given the advancement of technology and proliferation of cyber attack information, such data could allow vulnerabilities of the bulk power system to be exploited leading to widespread damage and prolonged loss of service.

Specifically, Form 603's "Statement of Need" invites the requester to provide mere conclusory statements as to "the extent to which a particular function (of the requestor) is dependent upon access to the information" and whether the entity's activities "cannot be achieved or performed without access to the information". No guidance is provided in the Form or its instruction as to the specific showing needed to satisfy this broad inquiry nor does the form require that any supporting documentation be provided to support the requester's response. Also, there is no guidance with respect to the destruction or disposal of the data. Moreover, the Commission has consistently overruled objections filed by many EIPC members, as well as other industry organizations, raising concerns as to the lack of specificity in the statements made by requesters in response to the Form's questions. In particular, objections have been filed and routinely overruled concerning the lack of specificity as to the requestor's need for and intended use of the requested information. *See as examples* Notice of Intent to Release, CEII No. CE19-074 (Sept. 23, 2019); Notice of

Intent to Release, CEII No. CE19-022 (Sept. 11, 2019); Notice of Intent to Release, CEII No. CE19-054 (May 15, 2019).

Rather than focusing solely on whether the requester needs the information to support *its* line of business (e.g. consulting, academic studies etc.), Form 603 should require a showing by the requester as to how dissemination of the information would advance the specific reliability responsibilities of the Commission, NERC and system planners and operators. *In short, rather than simply advancing the requester's line of business, the focus should also require a demonstration that dissemination of the information would enhance the work of those entities charged with ensuring bulk power reliability of the electric grid i.e. the Commission, DOE, NERC, state PUCs, NERC Reliability Coordinators and system planners and operators while maintaining the security of the grid.* The "Statement of Need" should be amended to include such a showing.

By the same token, Form 603 calls for a signed statement as to the accuracy of the information provided as well as an executed Non-Disclosure Agreement (NDA). The Commission evidently uses these documents as the principal means to ensure that the requested CEII is not misused. Terrorist organizations will hardly be deterred by the requirement to attest to a form or to sign an NDA. As a result, the Commission's perpetuating an enforcement system based on the signing of documents is inadequate, standing alone, to ensure the protection of this critical information from being used inappropriately.[3] The EIPC believes that more limited Commission dissemination of information on the front end (including more careful consideration rather than boilerplate summary dismissals of the objections that are filed to public release) is far superior to the proposed requirement for attestation of Form 603 and the signing of an NDA. Steps such as allowing:

a) limited and overseen 'view access' inspection;
b) requiring the requestor to show how they limited the breadth of their request; or
c) requiring the sharing of only a specific subset of cases and information rather than the entire case library requested

would be superior to today's mere hope that a requesting party is abiding by the limitations that it has signed as part of an NDA. As noted below, the EIPC stands ready to work with the Commission to detail those alternatives. Through an open dialogue, the EIPC and FERC may identify key vulnerabilities in the current process that may have simple, straightforward and non-burdensome solutions.

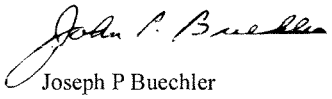
[3] In addition, the Commission has never explained how it actually enforces the provisions of the NDA so as to ensure that a third party, not regulated by the Commission, is complying with its terms.

EIPC Request for Meeting

Given that the EIPC consists of all of the major bulk electric system planners in the Eastern Interconnection of the United States, it is in a unique position to serve as a resource to the Commission on this important issue. Rather than perpetuating today's inadequate Form 603, EIPC suggests a more holistic revamp of both the form and the process based on the points raised in this pleading.

While the EIPC has suggested revisions to the Form itself, it would welcome the opportunity to meet with the Commission and its Staff and work to ensure that the CEII rules meet the dual requirements of protecting against the widespread dissemination of CEII information while allowing a channel for reasonable public requests for access to this information where appropriate.

Respectfully Submitted:



Joseph P Buechler
EIPC Executive Director
6 Candlewood Path North
Dix Hills, NY 11746
631-499-1555
jpbuechler@eipconline.com