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.

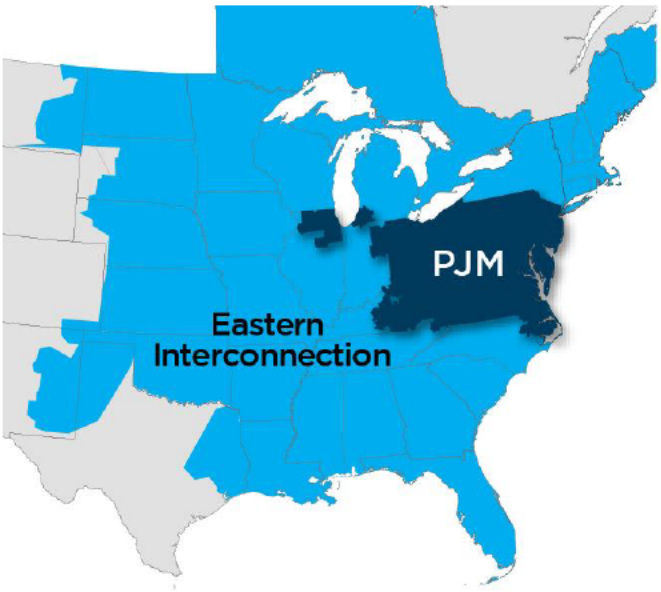
August 5, 2020

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.