Testimony of
JOHN DI STASIO, PRESIDENT,
LARGE PUBLIC POWER COUNCIL

Before the
UNITED STATES SENATE
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SUBCOMMITTEE ON ENERGY

Hearing to Examine the Cybersecurity Threats to the U.S. Electric Grid and Technology Advancements to Minimize Such Threats and to Receive Testimony on S. 79, the Securing Energy Infrastructure Act

March 28, 2017

CELEBRATING
30 YEARS
LPPC
LARGE PUBLIC POWER COUNCIL

Testimony of John Di Stasio
President, Large Public Power Council

Introduction

Chairman Gardner, Ranking Member Manchin and Members of the Subcommittee, thank you for the opportunity to testify today on the electric industry's active and collaborative efforts to anticipate and address cybersecurity threats, and to provide comments on S. 79, the Securing Energy Infrastructure Act. I am John Di Stasio, President of the Large Public Power Council ("LPPC"). LPPC represents 26 of the nation's largest public power systems, which provide power to over 30 million people in thirteen states. Collectively, the LPPC utilities own more than 71,000 megawatts of generation capacity powered by natural gas, nuclear, coal, hydroelectric, wind, solar and other renewable energy sources, and operate about 90 percent of non-federal, public agency owned transmission in the United States.

The points I will emphasize today are:

- Industry is engaged. While cybersecurity threats to the electric grid are fast evolving and require quick, adaptive responses, much is known about the threat environment. The industry, working within the standards promulgated and enforced by the North American Electric Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC), and working with our governmental partners, has effectively responded to known threats, while actively working to anticipate those that are emerging.

- Because the nature of the threats faced by the industry evolves so rapidly, the electric industry has repeatedly emphasized the need for the flexible application of cybersecurity regulations that permits industry agility in responding to threats and implementing evolving technology solutions.

I. The Threat Environment and Existing Responses

The electric industry has been grappling with cybersecurity threats for at least a decade. The public's attention was first dramatically captured in 2007 by the Idaho National Laboratory's "Aurora" experiment suggesting that control systems for generating stations might be hacked and manipulated. Since then, much has been learned about the nature of the threats we face through a variety of attack vectors, including hacking via internet access, phishing (email), watering hole attacks (mined websites), malware (including Stuxnet and reversed engineered versions), and mobile device attacks. In response to these threats, FERC and NERC have promulgated the nation's only mandatory suite of cybersecurity standards, the Critical Infrastructure Protection (CIP) standards, and the electric industry has implemented these standards.

NERC's CIP standards adopt a risk-based approach that begins with an inventory of critical assets and cyber systems, and attaches a comprehensive set of protective measures encompassing security management controls, personnel and training, electronic security

perimeters, physical security for cyber systems, system security management, incident reporting, response planning, recovery, configuration change management and vulnerability assessments, and information protection.

Though the electric industry is involved in the development of the NERC standards through an ANSI-approved process, it does not control the nature of the standards that are ultimately submitted by NERC to FERC for approval, or FERC's oversight. Under the Federal Power Act, FERC's certification of NERC as the nation's Electric Reliability Organization was contingent on NERC's development of procedures assuring its independence from "users and owners and operators of the bulk-power system." Further, FERC has the authority to order NERC to submit to the Commission proposed reliability standards or modifications to reliability standards that address vulnerabilities identified by the Commission. Enforcement of the standards by both NERC and FERC is entirely independent of the industry.

II. Responses to New and Emerging Threats

The cyberattack on the Ukrainian electric grid on December 23, 2015, underscored concern over the electric grid's vulnerability. As reported by the Department of Homeland Security (DHS) on February 25, 2016, and later in additional detail by the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) and SANS Industrial Control System (SANS ICS), the successful cyberattack on a Ukrainian regional electricity distribution company plunged approximately 225,000 customers into darkness. The attack was widely attributed to Russian security services. While service was restored within some hours, the attack underscored the destructive potential of a cyberattack on the electric grid, and highlighted points of vulnerability.

As disclosed in the ES-ISAC/SANS ICS report, hackers gained access to the Ukrainian utility's industrial control system (ICS) network and its supervisory control and data acquisition (SCADA) system via the Internet, enabling them to shut the system down remotely. Access to the Ukrainian utility's control systems was gained through spear phishing - the use of malware and the manipulation of Microsoft Office documents to harvest credentials enabling remote access to the ICS network. I do not want to discount the concern that the attack raises. But I do want to emphasize that these attack vectors are not unknown to U.S. utilities and are meaningfully addressed by NERC's existing reliability standards, as well as other security measures increasingly being adopted by the electric industry (discussed below). Specifically relevant are those CIP standards that provide for electronic security perimeters, access control, and malware detection and remediation.

In its alert and report on the Ukrainian incident, DHS, acting through its Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), also highlighted areas in which further study and potential action are recommended. These include the potential for control center isolation (sometimes referred to as "air gapping"), application "whitelisting" (automated systems permitting only expressly cleared programs to run on utility systems), greater levels of network segmentation, and the prudence in software and hardware procurement (supply chain). These areas are under study by NERC and FERC and, in the case of supply chain security, active standards development is underway.

In Docket No. RM16-18, FERC has asked for comments on whether additional reliability standards are needed to address the potential for control room isolation and application whitelisting. In responsive comments, NERC indicates that both areas are under active study, but also that existing reliability standards guard against related vulnerabilities. NERC also notes that there are operational and reliability drawbacks to each of these approaches that must be weighed carefully. Relevant existing CIP protections include:

- NERC's CIP-005 standard, requirements 1 and 2 of which impose mandatory Electronic Security Perimeters controlling electronic access to Bulk Electric Cyber Systems and securing Remote Access connectivity); and

- CIP-007, requirements 1-5 of which limit network accessible ports; call for active patch management, requires the implementation of methods to detect, deter, prevent and mitigate the threat of malicious code (malware), enables security event monitoring, and enforces system access control.

These standards permit control center isolation, but, as NERC notes, there are operational drawbacks to this approach. For one thing, a utility's ability to access control centers remotely enhances security to the extent it permits otherwise infeasible onsite support from critical vendors whose help is needed to address system failures. Remote access is also important when physical access to facilities by utility personnel is not possible. Further, remote access facilitates vendor patches, which themselves guard against evolving cyber threats. In addition, the ability to receive and transmit real-time data telemetry and security event data is crucial for situational awareness as well as monitoring and analysis.

Similarly, while application whitelisting is one feasible way to guard against the operation of malware on utility systems, the unintended consequences may include interference with future vendor support, conflicts with ongoing patch management and interference with essential programs that may be inadvertently overlooked in the pre-screening process. Here again, further study will be useful.

As to supply chain security (software and hardware procurement), NERC is currently in the process of developing a standard, at FERC's direction. This is an important initiative; one we are following closely. Certainly, the procurement of "trusted" hardware and software, as DHS put it, is an important matter. But having said that, it would not be reasonable to ask utilities to police their suppliers' compliance with security practice commitments the vendors have made. LPPC members are experts at running utility systems, but are not well-positioned to dictate or police the security practices of sophisticated vendors often much larger than the utilities themselves. For that reason, we are pressing for an approach to a supply chain standard which places the onus on vendors to assure compliance with their commitments to implement reliable security practices.

Finally, I want to emphasize the important work that is ongoing with respect to grid recovery and resiliency. This work is critical in order to anticipate the potential that one day our cyber security walls may be breached, despite our best efforts. The focus of this

ongoing work is on the development of systems that can be restarted following incapacitation, on operation of these systems with less than complete electronic control over the grid, and on ongoing service by segments of the grid that may remain operational despite loss of control of other segments. Some of the specific techniques and operational features on which we are focusing attention include the potential for manual operation of certain elements of our systems and facilities (in many cases - e.g., combined cycle gas turbine generators - the degree of digitization will not allow for manual operation), and the use of micro-grids and distributed energy resources.

III. The Importance of Flexible Regulation

Because the nature of the threats faced by the industry evolves so rapidly, the electric industry has repeatedly emphasized the need for the flexible application of regulations that permits agility and a wide variety of evolving responses that are not tied to specific solutions which seem attractive in one context and not the next. Such "performance-based" regulation emphasizes regulatory objectives, and not specific methods. In other words, the key is for the regulator to address "the what and not the how."

NERC's cybersecurity standard CIP-007-6, Requirement 1, for example, addresses protection from malware in just this way, calling for utilities to (1) deploy method(s) to deter, detect, or prevent malicious code; (2) mitigate the threat of detected malicious code; and (3) for those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. This standard does not specify which methods a utility must employ. As NERC explained in its technical guidelines describing the standard: "Due to the wide range of equipment comprising the [Bulk Electric System] Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset."

IV. LPPC's Comments on S. 79

LPPC applauds Senators Risch and King on bipartisan efforts to improve cybersecurity collaboration and research. S. 79 includes several study provisions that should be helpful. Specifically, Section 3 of S. 79 would establish a two-year pilot program within the National Laboratories that would facilitate partnership with relevant entities (including equipment suppliers) to identify new classes of security vulnerabilities. The section further provides that these pilots would support research, development, testing and implementation of technology platforms and standards that would "isolate and defend industrial control systems of covered entities." Section 4 of the bill would establish a working group "to develop a national cyber-informed engineering strategy to isolate and defend covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities."

However, LPPC cautions against provisions of the bill that call for the development of specific technology applications and prescribed standards designed to "isolate" control systems. We believe the existing framework is demonstrating its ability to address the

underlying concerns this provision seeks to remedy through the study NERC is conducting in connection with FERC's ongoing Notice of Inquiry in FERC Docket No. RM16-18. We look forward to working with the Committee on this issue as the NERC analysis and FERC consideration continues.

V. Other Important Resources and Partnerships

Independent of their engagement in NERC and FERC cybersecurity oversight, LPPC members are actively engaged in a variety of related forums that support cybersecurity threat responses. Some of these are as follows:

A. Reliance on Other Government-Sponsored Reliability Frameworks

LPPC participated directly, along with others in the electric industry, in the process leading to the development of the Cybersecurity Framework in 2014 by the National Institute of Standards and Technology, following a Presidential Directive. As well, LPPC members closely followed the development of the Department of Energy's Cybersecurity Maturity Model. Both of these frameworks provide models for the evaluation of cybersecurity vulnerabilities, and processes for risk management aimed at continuous evolution and improvement. LPPC members routinely use these tools to evaluate their cyber security programs from various perspectives independent of the NERC CIP standards, and to strive for continuous improvement.

B. Information Sharing and Alerts Through the ES-ISAC

The electric industry's primary resource for sharing information of cyber threats—with Federal government support—is the ES-ISAC. Administered by NERC, and operated in coordination with the Electric Sector Coordinating Council (ESCC) and the Department of Energy, the ES-ISAC was chartered to facilitate sharing of information regarding physical and cyber threats, vulnerabilities, incidents and potential protective measures. It serves as the primary security communications channel for the electricity sector, coordinating communications by and between member companies, sharing campaign analysis and incident data from private and public entities, and coordinating event and threat analysis with DOE, FERC and DHS. The ES-ISAC was launched following the issuance of Presidential Decision Directive 63 (PPD-63), along with nearly a dozen other ISACs operating critical infrastructure in other sectors of the economy. The ES-ISAC is among the most robust and effective of these organizations and the electric industry's vehicle of choice for information sharing. An indication of LPPC-member commitment to the ES-ISAC's work is the members' participation in a "Watch Floor Augmentation Program" placing staff from LPPC-member companies in the E-ISAC for one-week periods of time in order to expand coordination of information sharing.

C. Partnership with the Government

At the most senior levels, the electric industry is in close contact with the government through the ESCC. The ESCC serves as the principal link between the Administration and high-level electric industry executives. It is populated by Cabinet-level members from DOE and DHS, senior electric industry executives and trade association leaders. LPPC is

represented on the ESCC and values the direct contact it offers, enabling the Administration and industry to share information regarding ongoing and anticipated risks, and recommended responses. The forum provides an invaluable communication tool.

These contacts extend to other levels of government. The electric industry is in close contact with officials at the Department of Energy working on grid security (the Office of Energy Policy and Systems Analysis and the Office of Electricity Delivery and Energy Reliability) and the Federal Bureau of Investigation. Further, industry officials routinely coordinate with state and local governments in order to maintain the most comprehensive view of threats, risks and vulnerabilities.

D. Cyber Mutual Assistance

The ESCC recently established a voluntary Cyber Mutual Assistance (CMA) Program that is managed by EEI and has nearly 100 member utilities, including investor-owned utilities, public power utilities, electric cooperatives, Canadian utilities, and RTOs/ISOs. LPPC has a representative on the Executive Committee for the CMA Program and several of its members are in the Program. The CMA has a framework in which utilities can assist each other in responding to and recovering from cyber incidents that might exceed the capacity of one or a few entities. The program is structured to provide assistance to electric utilities in rebuilding and recovering necessary computer systems in the event of a regional or national cyber incident.

E. Cyber Security Best Practice Sharing

Along with other members of the electric industry, LPPC members routinely rely on voluntary industry associations for the purpose of strengthening their approach to cybersecurity. Best practices are shared through the North American Transmission Forum and the American Public Power Association's "Improving the Cyber Resiliency and Security Posture of Public Power" (sponsored by the Department of Energy). LPPC has created its own Cyber Security Task Force, charged with the responsibility of sharing best practices, serving to disseminate news of emerging risks, and helping to advocate public policy solutions.

VI. Conclusion

The electric industry's response to cybersecurity risk is robust, fast evolving, and intimately tied to efforts by the government to enhance the nation's security posture. No responsible official involved in the energy industry would claim that all risks are covered, but a great deal of good work is being undertaken in this area, and I am confident that we are intelligently addressing known risks, while making important efforts to anticipate new ones. As in any security environment, there is a great deal of focus on not only prevention, but also response and recovery. We welcome the opportunity to work with members of the Committee to provide further information, and to receive their input in this joint endeavor.

LPPC MEMBER COMPANIES

CELEBRATING 30 YEARS
LPPC
LARGE PUBLIC POWER COUNCIL

Arizona
Salt River Project

California
Imperial Irrigation District
Los Angeles Department of Water & Power
Sacramento Municipal Utilities District (SMUD)

Colorado
Colorado Springs Utilities
Platte River Power Authority

Florida
JEA
Orlando Utilities Commission (OUC)

Georgia
MEAG Power

Nebraska
Nebraska Public Power District
Omaha Public Power District

New York
Long Island Power Authority
New York Power Authority

North Carolina
ElectriCities of NC, Inc.

Oklahoma
Grand River Dam Authority

South Carolina
Santee Cooper

Texas
Austin Energy
CPS Energy
Lower Colorado River Authority

Washington
Chelan County PUD No.1
Clark Public Utilities
Grant County PUD
Seattle City Light
Snohomish County PUD No.1
Tacoma Public Utilities

Puerto Rico
Puerto Rico Electric Power Authority