Statement of the
LARGE PUBLIC POWER COUNCIL

Submitted to the
HOUSE ENERGY AND COMMERCE SUBCOMMITTEE ON ENERGY

Hearing on
"The Electricity Sector's Efforts to Respond to Cybersecurity Threats"

February 1, 2017

The Large Public Power Council ("LPPC") submits this statement to the House Energy & Commerce Committee's Subcommittee on Energy ("the Subcommittee"), in connection with the hearing on "The Electricity Sector's Efforts to Respond to Cybersecurity Threats." to be held February 1, 2017. LPPC is an association of the 25 largest state-owned and municipal utilities in the nation. LPPC members are located throughout the nation, both within and outside RTO boundaries. LPPC represents the larger, asset-owning members of the public power sector. Together, they own roughly 90% of the electric transmission investment owned by public power entities in the United States.

LPPC supports the Subcommittee's interest in being fully informed regarding the cyber threats facing the electric industry, and the industry's response. LPPC members are acutely aware of the risks facing the industry and are actively involved in efforts within their companies

and at the governmental level to manage risk and respond to known and emerging vulnerabilities. The attack on the Ukrainian electric grid, mentioned in the Majority Staff memorandum submitted to the Subcommittee in connection with this hearing, is certainly an indication that the industry must be vigilant.

Yet, LPPC urges the Committee to take stock of the measures that have been taken by the industry, the North American Electric Reliability Corporation ("NERC") and the government to respond to these risks. The focus of this statement is on those measures, including: (1) the mandatory standards regime administered by NERC; (2) the reliance by the industry on a range alternative frameworks and resources to evaluate vulnerability and anticipated response; (3) reliance on the Electric Sector Information Analysis Center ("ES-ISAC"); (4) existing government-industry partnerships; and (5) the range of mutual assistance programs relied on by the industry to enhance security.

1. NERC's Reliability Enforcement Regime

Cybersecurity measures undertaken by the electric industry areas are governed by a suite of mandatory Critical Infrastructure Protection ("CIP") standards promulgated by NERC and approved by the Federal Energy Regulatory Commission ("FERC"). The electric sector is the only sector of the economy that operates under mandatory, enforceable standards. NERC's CIP standards adopt a risk-based approach that begins with an inventory of critical assets, and attaches a comprehensive suite of protective measures encompassing security management controls, personnel and training, electronic security perimeters, physical security, system security management, incident reporting, response planning and recovery.

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 ultimately

submitted by NERC for approval by FERC, or FERC's oversight. Enforcement of the standards by both NERC and FERC is entirely independent of the industry. Under the Federal Power Act (FPA), FERC's certification of NERC as the Nation's Electric Reliability Organization (ERO) was contingent on its development of rules 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.

2. 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 promulgated 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 programs from various perspectives independent of the NERC CIP standards, and to strive for continuous improvement.

3. Information Sharing and Alerts Through the E-ISAC

The electric industry's primary resource for sharing information of cyber threats—with the government's encouragement—is the E-ISAC. Administered by NERC, and operated in coordination with the Electric Sector Coordinating Council (ESCC) and the Department of Energy, the E-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 members companies, sharing campaign analysis and incident data from private and public entities and it coordinates event and threat analysis with DOE, FERC and DHS. The E-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 E-ISAC is among the most robust and effective of these organizations and the electric industry's vehicle of choice for information sharing.

4. Partnership with the Government

At the most senior levels, the electric industry is in close contact with the government through the Electric Sector Coordinating Council ("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. As are other sectors of the electric utility industry, 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 and Energy Reliability) and the Federal Bureau of Investigation. Further, industry officials routinely coordinate with states, municipalities and local governments in order to maintain the most comprehensive view of threats, risks and vulnerabilities.

5. Voluntary Mutual Assistance

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,

Also of note, following NERC's Grid-Ex incident response exercise, the ESCC established the Cyber Mutual Assistance Task Force, an organization that has convened industry experts to develop a mutual assistance program for cyber threats, aimed at assisting electric utilities to rebuild and recover necessary computer systems in the event of a regional or national cyber incident. The Task Force also aims to provide shared educational assistance and training to facilitate the provision of mutual assistance in the event of an emergency.

The electric industry's response to cyber risks is robust, fast-evolving, and intimately tied to efforts by the government to enhance the nation's security posture. We welcome the opportunity to work with members of the Subcommittee to provide further information, and to receive their input in this joint endeavor.

John DiStasio
President
Large Public Power Council