AMERICAN PUBLIC POWER ASSOCIATION™
Powering Strong Communities

NRECA®
America's Electric Cooperatives

Statement for the Record by the

AMERICAN PUBLIC POWER ASSOCIATION (APPA) and the NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION (NRECA)

Submitted to the

HOUSE OVERSIGHT AND REFORM COMMITTEE'S SUBCOMMITTEE ON NATIONAL SECURITY

For the July 27, 2021, Hearing on

"Defending the U.S. Electric Grid Against Cyber Threats"

The American Public Power Association (APPA) and the National Rural Electric Cooperative Association (NRECA) appreciate the opportunity to submit a statement for the record for the House Oversight and Reform Committee's Subcommittee on National Security's hearing, "Defending the U.S. Electric Grid Against Cyber Threats."

The American Public Power Association is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. APPA represents public power before the federal government to protect the interests of the more than 49 million people that public power utilities serve, and the 93,000 people they employ. APPA advocates and advises on electricity policy, technology, trends, training, and operations.

NRECA is the national trade association representing nearly 900 local electric cooperatives and other rural electric utilities. America's electric cooperatives are owned by the people that they serve and comprise a unique sector of the electric industry. From growing regions to remote farming communities, electric cooperatives power 1 in 8 Americans and serve as engines of economic development for 42 million Americans across 56 percent of the nation's landscape. Electric cooperatives operate at cost and without a profit incentive. NRECA's member cooperatives include 62 generation and transmission (G&T) cooperatives and 831 distribution cooperatives. Both distribution and G&T cooperatives share an obligation to serve their members by providing safe, reliable, and affordable electric service.

A reliable energy grid is the lifeblood of the nation's economic and national security, as well as vital to the health and safety of all Americans. Electric utilities take very seriously their responsibility to maintain a secure and reliable electric grid. It is the only critical infrastructure sector that has mandatory and enforceable federal regulatory standards in place for cyber and physical security (collectively known as grid security). Cyber-attacks, relatively new compared to long-known physical threats, have rapidly evolved and could have operational consequences. The industry and its federal government partners have made great strides in addressing cybersecurity threats, vulnerabilities, and potential emergencies. Given the persistence and sophistication of threats, utilities cannot prevent all attacks at all times. For both cyber and physical threats, electric utilities employ risk management programs to prioritize facilities and equipment, develop contingency plans, and employ defense-in-depth techniques to keep the lights on and recover them as quickly as possible when they go off.

The electric utility sector has a mandatory and enforceable federal regulatory regime in place for cybersecurity. Congress approved the standards regime for the bulk power system in the Energy Policy Act of 2005 (EPAct05) (section 215 of the Federal Power Act (FPA)). Under section 215, the North American Electric Reliability Corporation (NERC), working with electric industry experts, regional entities, and government representatives, regularly drafts reliability, physical security, and cybersecurity standards that apply across North America's Bulk Electric System, including Canada. Participation by industry experts and compliance personnel in the NERC critical infrastructure protection (CIP) standards development process ensures that the standards are technically sound, fair, and balanced. The Federal Energy Regulatory Commission (FERC) has the power to then approve or remand those standards as they apply in the United States. To ensure compliance, under FERC's oversight, NERC and its regional entities conduct rigorous audits and can levy substantial fines for non-compliance. Additionally, FERC can instruct NERC to develop new or revised reliability standards with a very short turn-around time.

The Energy & Commerce Committee developed important grid security provisions in the comprehensive energy bill that was ultimately passed into law as part of H.R. 22, "Fixing America's Surface Transportation Act." These provisions included establishing the Department of Energy (DOE) as the sector-risk management agency for the electric utility industry, giving DOE authority to direct industry to take action in the event of a grid security emergency and protecting critical electric infrastructure information (CEII) from public disclosure.

Federal regulations establish an important baseline of security—but they are a floor, not a ceiling—and grid security is and should continue to be much more than a compliance exercise. Robust voluntary information sharing between the government and utilities, strong public-private partnerships, and regular sector-wide preparation exercises are also key pillars of grid security, examples of which are listed below.

- Electric Subsector Coordinating Council (ESCC) – The ESCC serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The ESCC includes utility CEOs and trade association leaders representing all segments of the industry. Their counterparts include senior Administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

- Electricity Information Sharing and Analysis Center (E-ISAC) – Electric utilities voluntarily share and receive grid security threats via the E-ISAC, as well as through other avenues when appropriate like the Multi-State Information and Sharing Analysis Center (for public power utilities). These information sharing organizations are critical to ensure that the electric power industry as a whole has shared awareness of the tactics, techniques, and procedures used by the adversaries targeting the electric grid.

- GridEx – GridEx is a biennial distributed play grid exercise that allows participants to engage remotely, simulates a cyber and physical attack on the North American electricity grid and other critical infrastructure. Led by NERC's E-ISAC, GridEx gives participants a forum to demonstrate and build upon how they would respond to and recover from coordinated cyber and physical security threats and incidents.

- Mutual Aid – The electric utility industry has long had in place mutual aid response networks to share employees and resources to restore power after natural disasters and other emergencies. The

ESCC used the concept of traditional mutual assistance networks to develop the Cyber Mutual Assistance program that can help electric and natural gas companies, public power utilities, and/or rural electric cooperatives restore critical computer systems following significant cyber incidents. The program now includes more than 170 entities across all segments of the industry, serving more than 80 percent of all U.S. electricity customers. The electric utility industry also regularly shares transformers and other equipment through bilateral and multilateral sharing arrangements and agreements. Industry has equipment sharing programs—like the Spare Transformer Equipment Program, SpareConnect, and Grid Assurance—to help improve grid resiliency.

- DOE Grants for Small and Medium Utilities - APPA and NRECA have worked directly with DOE's Office of Cybersecurity, Energy Security and Emergency Response (CESER) through cybersecurity grants since 2016 to bring tools and resources to small and medium utilities, including to develop and deploy cyber and cyber-physical solutions. One of these efforts is intended to provide utilities with emerging innovations at the hardware, firmware, and/or software levels to protect key operation technology (OT) components that enable the safe control of the physical systems that deliver electric power. This effort builds on the accomplishments of a 2016 three-year grant CESER awarded to APPA and NRECA geared to assess and help to strengthen the cybersecurity posture of small- and medium-sized public power and cooperative utilities. This grant enabled the development of a cybersecurity resources for small and medium public power and cooperative utilities, including self-assessment resources to assess their cyber readiness, the production of a cybersecurity roadmap, incident response playbooks, and other guidance documents to help utilities develop a culture of cybersecurity within their organization.

  Legislation based on the success of these grant programs, H.R. 2931, the Enhancing Grid Security through Public-Private Partnerships Act, recently passed the House of Representatives. Sponsored by Representatives Jerry McNerney (D-CA) and Bob Latta (R-OH), this legislation would permanently support public-private partnerships to promote and advance the physical and cybersecurity of electric utilities.

- NSC "100 Day Electric Sector Industrial Control Systems Cybersecurity Sprint" – On April 16, the Biden administration launched a new initiative to enhance the monitoring of the cybersecurity of electric utilities' industrial control systems (ICS). This 100 day "sprint" was a coordinated effort between the National Security Council (NSC), DOE, Department of Homeland Security, and industry to encourage and support utilities' visibility and situational awareness into their ICS and OT networks. APPA and NRECA are working with public power utilities and rural electric cooperatives to facilitate their participation in this voluntary pilot program. This effort has appropriately raised the issue of ICS security to a higher priority in the federal government. APPA and NRECA view this sprint as the start of a long journey of collaboration between public power, electric cooperatives and the federal government, which includes the work being done through the CESER grants to APPA and NRECA.

The regulations and standards ("NERC-FERC") process set up in EPAct05 provide a solid foundation allowing for these mandatory standards evolve with input from subject-matter experts from across industry and government. However, the industry recognizes that it cannot protect all assets from all threats all the time, and instead must manage risk. We believe that close coordination among industry and government partners at all levels is imperative to deterring attacks and preparing for emergency situations.