Resolution 24-07
Sponsors: Tacoma Public Utilities; Illinois Municipal Electric Association; Nebraska Public Power District

In Support of Risk-Based Grid Security Standards

The electric utility sector has long had in place a combination of risk-based mandatory regulations and voluntary cybersecurity and physical security ("grid security") standards. Congress approved a mandatory and enforceable standards regulatory regime for the bulk power system in the Energy Policy Act of 2005 (EPAct05) (section 215 of the Federal Power Act). 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 the North American grid, 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 regulations and standards process set up in EPAct05 provide a solid foundation allowing for these mandatory standards to evolve with input from subject-matter experts from across industry and government. The current mandatory regulatory structure in place is risk-based and appropriately applies to the most critical industry stakeholders and assets. The industry recognizes that it cannot protect all assets from all threats all the time, and instead must manage risk. The CIP standards establish an important baseline of security for the most critical of systems and assets, but grid security is and should be much more than a compliance exercise.

There have been numerous discussions in recent years suggesting the need to broadly expand mandatory grid security standards, in some cases down to the distribution level. APPA believes that expanding mandatory regulations beyond the scope of the most critical systems and assets would dilute the strength of the existing, proven regulatory model, as well as distract from voluntary efforts tailored to the size, resources, and risk profiles of individual utilities.

One area that could benefit from additional attention and resources from the federal government is digital component vendors and manufacturers. Under the existing NERC-FERC standards regime, utilities are responsible for assessing the cybersecurity of vendors and manufacturers of digital components. Utilities

have found that not all vendors and manufacturers of digital components feel compelled to respond to utilities as they seek to conduct these vendor assessments. The responsibility for demonstrating the cybersecurity of their supply chain for all equipment, components, and subcomponents used for critical electric infrastructure should rest with vendors and manufacturers.

NOW, THEREFORE, LET IT BE RESOLVED: That the American Public Power Association (APPA) supports the existing mandatory and enforceable regulatory regime for the bulk power system set up in the Energy Policy Act of 2005 (section 215 of the Federal Power Act); and

BE IT FURTHER RESOLVED: That APPA supports risk-based grid security standards and opposes "one-size fits all" approaches to security regulations; and

BE IT FURTHER RESOLVED: That APPA opposes mandatory and enforceable federal standards for distribution-level electric utilities; and

BE IT FURTHER RESOLVED: That APPA encourages the federal government to work directly with digital component vendors and manufacturers to strengthen supply chain security for all equipment, components, and subcomponents used for critical electric infrastructure using a risk-based framework that factors in cost and availability; and

BE IT FURTHER RESOLVED: That APPA encourages the federal government to: (a) expand domestic production of electric equipment, components, and subcomponents to ensure their security and (b) require vendors and manufacturers of such components to provide origin information for all components and subcomponents, including software code, included in any equipment, components, and subcomponents sold in the United States so purchasers can ensure that no such components or subcomponents were produced in hostile countries or by suspect suppliers; and

BE IT FURTHER RESOLVED: That APPA will continue to educate and encourage all APPA members to improve protection strategies that include tighter physical access measures and surveillance, voluntary industry-wide physical and cybersecurity standards and guidelines, participation in emergency preparedness drills that focus on protection, response, and recovery, and further development of emergency supply chain networks and spare equipment sharing programs to support restoration.

Adopted at the Legislative & Resolutions Committee Meeting
February 27, 2024

Sunsets in March 2032