

Maintaining Cyber, Physical Security are High Co-op Priorities

Key Facts

- Electric cooperatives make protection and security of their electric system assets and consumer-member data a high priority.
- Electric cooperatives support the current standard development process in which industry experts participate in developing mandatory and enforceable standards for a wide variety of potential threats.
- Improved flow of timely and actionable information and liability protections for electric systems is needed, along with research and development of new technologies for small and medium systems.

Electric Cooperative Priorities

Protecting the nation's electric power grid and ensuring an affordable, reliable, and secure supply of electricity are top priorities for electric cooperatives. The North American power system is an incredibly complicated machine. System owners and operators, who have the greatest expertise in responding to and mitigating potential threats and vulnerabilities, are working together across the industry and with government agencies to prepare for existing and potential threats to the reliability and security of the electric grid.

The electric sector uses a defense-in-depth strategy to protect critical assets. This approach is designed to address a variety of hazards to electric grid operations, including severe earth and space weather, cyber incidents, vandalism and other natural and manmade events. The electric power sector continuously monitors the bulk electric system (BES) and responds to events large and small. In cases where an event impacts consumers, this strategy combined with experience from decades of lessons learned maintaining and supplying power to the country has resulted in more efficient restoration of power.

Government and Industry Partnerships

The Electricity Subsector Coordinating Council (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. Its government counterparts include senior administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

The ESCC also serves an advisory role with the Electricity Information Sharing and Analysis Center (E-ISAC). The E-ISAC collects and promptly disseminates threat indicators, analyses and warnings from a variety of private sector and government resources to assist electric sector participants in taking protective action. The information is handled confidentially and distributed through the North American Electric Reliability Corporation's (NERC) secure portal directly to industry asset owners and operators.

Current Regulatory Environment

Electric cooperatives work closely with NERC, the Department of Homeland Security (DHS), the Department of Energy (DOE), and the Federal Energy Regulatory Commission (FERC) on matters of critical infrastructure protection, including sharing needed information about potential threats and vulnerabilities to the bulk electric system. NERC, a private not-for-profit entity, develops and enforces reliability and cybersecurity standards.

Since 2007, when these NERC standards became mandatory, electric cooperative representatives have participated in numerous NERC standard development activities. The electric utility industry, along with the nuclear energy industry, are the only critical infrastructures with mandatory and enforceable cybersecurity standards. The electric utility industry also developed standards on physical security and geomagnetic disturbances (GMDs) and continues to revise the cybersecurity and GMD standards.

NRECA Positions

Protect the Standards Development Process: Electric cooperatives do not support proposals to allow federal agencies to create reliability standards. The current process is working. Industry experts participate in the NERC standards development process by writing and developing standards for a wide variety of threats and vulnerabilities. These standards are mandatory and enforceable once the NERC Board of Trustees and FERC approve them. Electric co-ops oppose any expansion of FERC's authority in the process.

Improve Information Flow and Protection: NRECA supports efforts to increase electric cooperatives' access to government intelligence information relating to a particular threat or vulnerability that could be timely and actionable for industry. This includes more quickly granting security clearances for electric co-op representatives, and higher level clearances for electric cooperative leadership. In addition, the government should have a program that allows voluntary access to FBI Enhanced Background Investigation Screening processes for critical employees. Also, industry should have assurance that sensitive information shared from industry to government is properly protected and free of liability concerns when shared in good faith.

Support Research, Development and Adoption of New Technologies for Small and Medium Entities: NRECA supports efforts to develop and expand cybersecurity resources and technologies to meet the unique needs of small- and medium-sized utilities, such as DOE's Cybersecurity for Energy Delivery Systems (CEDS) program. This program provided funding for NRECA to develop the Rural Cooperative Cybersecurity Capabilities Program (RC3) in 2016, which is helping cooperatives build stronger cybersecurity programs. As this program is in its final year of funding NRECA encourages DOE to extend funding for future years on existing public-private partnerships through the CEDS program.

NRECA also supports efforts to clarify the scope of SAFETY Act liability protections by including "qualifying cyber incidents" as triggers for liability protection. Clarifying these protections for coverage of cyber incidents could help incentivize innovation and provide industry certainty.

Contact:

Bridgette Bourge
NRECA Legislative Affairs
703-907-6386
Bridgette.Bourge@nreca.coop

Barry Lawson
NRECA Regulatory Affairs
703-907-5781
Barry.Lawson@nreca.coop