AMERICA'S ELECTRIC COOPERATIVES

Fast Facts

March 2018

Maintaining Strong Cyber and Physical Security are Key Priorities for Electric Cooperatives

Protecting the nation's electric power grid and ensuring an affordable, reliable and secure supply of energy 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 threats and vulnerabilities in this complex system, are engaged across the industry and with government to plan and prepare for existing and potential threats to the reliability of electricity in our nation.

The electric sector's strategy to protect critical assets is known as defense-in-depth, and is designed to address a wide 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 and responds to events large and small. Consumers are rarely aware of these events primarily because the sector successfully executes its defense-in-depth strategy every day. In cases where an event impacts the consumer, this strategy combined with experience from decades of lessons learned maintaining and supplying power to the country have resulted in more efficient restoration of power.

As member-owned, not-for-profit utilities, electric cooperatives make protection and security of their systems and consumer-members' assets a high priority. NRECA works with its co-op members, industry partners and government agencies to develop and implement effective approaches to protecting systems.

Regulatory Environment

To maintain and improve upon the high level of reliability consumers expect, electric cooperatives work closely with the North American Electric Reliability Corporation (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 (BES). FERC delegated authority to NERC, a private not-for-profit entity, for standards development and enforcement of reliability and cybersecurity standards.

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

Government and Industry Partnerships

In 2013 the electric utility industry reorganized the Electricity 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, including NRECA's CEO Jim Matheson. 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 NERC's secure portal directly to industry asset owners and operators.

NRECA Positions

Protect the Standards Development Process: Electric cooperatives are concerned about any legislative proposals that would allow federal agencies to write, develop or directly edit reliability standards. We support the current process whereby industry experts participate in the NERC standards development process by writing and developing standards for a wide variety of threats and vulnerabilities. Those standards become mandatory and enforceable once the NERC Board of Trustees and FERC approve them. We oppose any expansion of FERC's authority in the process.

Improve Information Flow and Protection: In some circumstances there may be situations where government possesses intelligence information (classified and unclassified) on a particular threat or vulnerability that could be timely and actionable for industry. We support efforts aimed at increasing electric cooperatives access to such information, thereby helping us do an even better job of protecting the grid. In addition, we advocate allowing voluntary access to FBI Enhanced Background Investigation Screening processes for critical employees and seek 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 & 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 the DOE's "Improving the Cyber and Physical Security Posture of the Electric Sector" initiative. This initiative provided DOE funding which was utilized to launch in 2016 NRECA's Rural Cooperative Cybersecurity Capabilities Program (RC3), which is helping cooperatives build stronger cybersecurity programs.

NRECA also supports efforts to clarify the scope of SAFETY Act liability protections by including "qualifying cyber incidents" as triggers for that liability protection. Legislation sponsored by Senator Daines (R-MT), S. 2392, would explicitly provide the liability protections of the SAFETY Act when the DHS Secretary deems that an act of terrorism or a "qualifying cyber incident" has occurred. While the law applies to cyber events, in practice there have been questions impacting the programs full potential due to the requirement that an attack be deemed an "act of terrorism" by the DHS Secretary before liability protections become available.

for more information:

Bridgette Bourge
NRECA Legislative Affairs
703-907-6386
Bridgette.Bourge@nreca.coop
http://www.electric.coop

Barry Lawson
NRECA Regulatory Affairs
703-907-5781
Barry.Lawson@nreca.coop
http://www.electric.coop