Fact Sheet

May 2021

Electric Co-ops Prioritize Cybersecurity, Grid Protection

Key Facts

- Electric cooperatives prioritize the protection and security of their electric system assets and consumer-member data.
- The electric utility industry is the only U.S. critical infrastructure with mandatory and enforceable cybersecurity standards.
- Electric cooperatives proactively engage in industry/government cybersecurity efforts to stay ahead of potential threats. As threats and threat actors continue to evolve, so must the industry's capability to defend against them. Electric co-ops are leading efforts to maintain the security and resilience of the grid with a flexible approach that draws on a variety of resources and options.

Electric Cooperatives Employ a Defense-in-Depth Cybersecurity Strategy

Electric cooperatives prioritize grid security to ensure American families and businesses have continued access to affordable and reliable electricity. Because the electric grid is incredibly complex, co-ops and the electric sector continuously monitor the bulk electric system and quickly respond to events large and small.

America's electric cooperatives are modernizing their systems and using technology to improve efficiency, safety, and reliability. Electric cooperatives work together to manage growing cyberthreats, promote continuous improvement, and develop solutions that keep the grid and their systems secure.

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 cyber threats, severe weather, vandalism and other natural or man-made events. In cases when an event may impact consumers, this defense-in-depth strategy—combined with experience from decades of lessons learned maintaining and supplying power—results in more efficient restoration of electric service.

Government, Industry Partnerships are Keys to Success

Protecting the electric grid from threats that could impact national security and public safety is a responsibility shared of the government and the electric power sector.

The electric utility industry is the only American critical infrastructures with mandatory and enforceable cybersecurity standards. NRECA and electric cooperative leaders, along with other industry stakeholders, participate in the Electricity Subsector Coordinating Council (ESCC), the principal liaison between the federal government and the electric power sector. The ESCC focuses on preparing for and responding to natural disasters or threats to critical infrastructure. The ESCC also serves as a conduit for timely information sharing between the public and private sectors.

Electric cooperatives also work closely with federal agencies on matters of critical infrastructure protection, including sharing needed information about potential threats and vulnerabilities.

Co-op Cybersecurity Leadership

As threats and threat actors continue to evolve, so must the industry's capability to defend against them. Electric co-ops are leading efforts to maintain the security and resilience of the grid with a flexible approach that draws on technology, shared strategies and resources, and preparedness. These efforts include:

- Elevating the cybersecurity posture of electric co-ops through the Rural Cooperative Cybersecurity Capabilities (RC3) program.
    - With funding from DOE, the RC3 program helped more than 500 co-ops build stronger cybersecurity programs with a focus on developing tools and resources for improving cybersecurity capabilities of electric cooperatives. The program also provides collaboration, education, and training opportunities.
- Developing and deploying Essence technology at co-ops.
    - Essence is a proven, industry-ready solution to enhance the cybersecurity posture at electric utilities and beyond. It is an information and operational technology sensor platform created by NRECA with advanced capabilities to precisely detect system anomalies and threats in seconds rather than months.
    - The technology is used by cybersecurity teams and operating engineers to protect key systems against unknown, emerging threats. It measures the continuous behavior of operations technology and grid physics data and allows utilities to interact with data and receive immediate notice of anomalous issues that could indicate a breach.
- Partnering with the federal government on its 100-day Industrial Control System initiative, designed to enhance the cybersecurity of the electric industry.
- Pioneering a groundbreaking approach to information sharing with the federal government.
    - Through a partnership with the Pacific Northwest National Laboratory's (PNNL), co-ops running the Essence cybersecurity software will be able to share anonymized network information with the government's Cybersecurity Risk Information Sharing Program (CRISP), which leverages DOE intelligence to collect, analyze, and distribute actionable threat information to the energy sector.
- Partnering with Pacific Northwest National Laboratory (PNNL) on a software bill of materials (SBOM) pilot to evaluate battery energy storage systems installed by two different rural electric cooperatives for critical infrastructure. This initiative will allow NRECA Research and PNNL to create an incubator program to help rural electric cooperatives address any supply chain concerns with installing new technology.