75 Years of Service NRECA America's Electric Cooperatives

July 2017

Building Cyber Resiliency Across America's Electric Cooperatives

Protecting the nation's complex, interconnected network of power plants, transmission lines and distribution facilities is a top priority for electric cooperatives and other segments of the electric power industry.

The electric power industry continuously monitors the electric grid and responds to events large and small. Consumers are rarely aware of these events because of system resilience supported by planning, coordination and response/recovery efforts. In rare cases where an event does impact electric service, industry resilience and preparedness ensures service is promptly restored in most cases.

A high level of resilience is built into the power supply system to protect against extreme weather events, vandalism and major equipment failure. This concept is often referred to as defense in depth, and is also used for cybersecurity. In general, this means that multiple layers of protection safeguard assets from cyber threats.

Co-ops' Flexible, Comprehensive Protection Strategy

The possibility of a cybersecurity attack impacting grid operations is something for which the power sector has been preparing for years. These preparations include:

- Implementing rigorous security standards and technology to protect systems,
- Forging close partnerships to protect our systems and respond to incidents, and
- Engaging in active information sharing about threats and vulnerabilities.

As threats and threat actors continue to evolve, so must the industry's capability to defend against them. Maintaining the resilience and security of the electric grid requires a flexible approach that draws on a variety of tools, resources and options.

The protection and security of consumer-members' assets is paramount for electric cooperatives. NRECA, its member cooperatives, industry partners and government agencies work closely to develop flexible, effective approaches to protecting the electric system. Electric cooperatives are taking the following steps to protect their critical assets:

- **Electricity Sector Cybersecurity Capability Maturity Model** – Developed by the U.S. Department of Energy (DOE), this tool provides utilities the framework for performing a comprehensive self-assessment of their current cybersecurity plans and procedures. Electric cooperatives were among the first utilities to pilot and use the tool, which assists organizations in evaluating, prioritizing and improving their cybersecurity capabilities.

- **NRECA's Guide to Developing a Cybersecurity and Risk Mitigation Plan and Template** helps cooperatives improve their security posture while ensuring that security is not undermined as new smart grid components and technologies are integrated into the electric grid.

- **Rural Cooperative Cybersecurity Capabilities Program** is an NRECA-led program aimed at helping small- and mid-sized cooperatives develop cyber resiliency and security programs. The program provides training and guidance to assist cooperatives in assessing their cybersecurity risks, and enhancing their cybersecurity capabilities to prevent and mitigate cyber incidents. While focused mainly on co-ops with smaller information technology staffs, these products and materials are available to help all cooperatives.

- **Cyber Mutual Assistance programs**: Electric cooperatives and other utilities have a collaborative approach to emergency management and disaster recovery. Following a physical disaster, cooperatives rapidly deploy support staff and equipment to emergency and recovery zones to assist other cooperatives and utilities when needed. The Electricity Subsector Coordinating Council's (ESCC's) Cyber Mutual Assistance (CMA) program is a natural continuation of the electric power industry's longstanding approach of sharing critical personnel and equipment when responding to emergencies.

- **Cybersecurity Research and Development:** NRECA works with DOE, National Laboratories, the Department of Defense, research universities and industry partners to develop cybersecurity technologies that benefit electric utilities. Two technologies are currently in development.
    - **Essence** is a technology to monitor traffic on a utility network and flag anomalous activity that could indicate a security breach.
    - **Simba** is a technology to develop a rapid cybersecurity testing capability using software that can process a year's worth of data in less than an hour. One of the primary research goals is to dramatically reduce the time it takes for utilities to detect cyber-threats.

Industry, Government Collaboration Enhances Grid Security

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

NERC Standards: Approximately 60 generation and transmission cooperatives and 60 distribution cooperatives must comply with North American Electric Reliability Corporation's (NERC's) electric reliability and cybersecurity standards, based on the criticality of the assets they own and operate. These standards require the operators of power plants and transmission networks to establish plans, protocols and controls to safeguard physical and electronic access to these systems. NERC also has an alert system that provides the electric sector with timely and actionable information when a standard may not be the best method to address a particular event or topic.

The Electric Sector Coordinating Council allows the utility sector to work with federal government leadership to coordinate policy-level efforts to prevent, prepare for, and respond to national-level incidents affecting critical infrastructure. NRECA, other trade associations and industry work with government agencies to improve cybersecurity through the council. These efforts include planning and exercising coordinated responses, and ensuring that information about threats is communicated quickly among government and industry stakeholders.

The **Electricity Information Sharing and Analysis Center**, operated by NERC, 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 center also manages the **Cybersecurity Risk Information Sharing Program**, a public-private partnership that shares actionable threat information. The program uses advanced data collection technologies, analysis and dissemination tools to identify threat patterns and trends across the electric power industry with near real-time exchange of information.