MISSOURI RIVER® ENERGY SERVICES

3724 West Avera Drive
PO Box 88920
Sioux Falls, SD 57109-8920
Telephone: 605.338.4042
Fax: 605.978.9360
www.mrenergy.com

February 2024

Protecting Grid Security

Increasingly, electric utilities face threats to physical infrastructure – the poles, wires, substations, transformers, and generating facilities. Most physical security threats to electric infrastructure, such as copper theft, have been known for years. However, ever more sophisticated and malicious physical threats have continued to emerge.

On February 6, 2023, the Justice Department announced the arrest of two individuals for planning to attack five electric power transmission substations around Baltimore, Maryland as part of a "racially or ethnically motivated violent extremist" conspiracy. On Christmas day in 2022, four electric distribution substations in the Tacoma, Washington area were physically attacked, allegedly by two malicious individuals in a burglary scheme, causing millions of dollars in damage and cutting power to some 30,000 utility customers. Three weeks later, unknown perpetrators attacked two substations in Moore County, North Carolina causing an extended blackout for 45,000 customers. Additionally, cybersecurity threats have continued to grow in both frequency and sophistication. The electric industry and federal agencies are constantly updating efforts to identify, thwart, and respond to these attacks.

All electric utilities, including municipal utilities, take physical and cybersecurity threats seriously and employ risk management programs to protect facilities and equipment, train employees on preventative measures, develop contingency plans, and continually upgrade their security protocols and mechanisms to protect their systems. In fact, the electricity industry was the first sector of the economy subject to mandatory, federally-enforced cybersecurity standards.

Federal Regulation and Grid Security

The Energy Policy Act of 2005 mandated the implementation of electric transmission reliability standards under new authority granted to the Federal Energy Regulatory Commission (FERC). FERC then designated the North American Electric Reliability Corporation (NERC), an industry-based non-profit company, to establish standards for the United States electric transmission grid, subject to FERC review. NERC subsequently issued several orders: risk, threat and vulnerability assessments for critical facilities; implementation of physical security plans for critical facilities; and compliance for monitoring assessment. Additionally, the Infrastructure Investment and Jobs Act included provisions to provide financial assistance to states for developing and implementing state energy security plans to secure energy infrastructure.

Utilities Continue to Take the Lead

In addition to compliance with NERC standards, utilities have continued to act on their own to analyze risks, take action to mitigate or prevent risk, and implement response and restoration should a physical or cyber-attack occur. For example, municipal utilities conduct exercises for a variety of situations that could impact operations. Missouri River Energy Services (MRES) has engaged in business continuity planning, network/cyber hardening, the creation of an additional operations site, various emergency response training for staff, and information sharing.

As Congress continues to examine the state of electric grid security, MRES and its members encourage its delegation **to ensure continued deference to the FERC-NERC model for the development and enforcement of security requirements to avoid duplicative or conflicting requirements**. Also, MRES calls for **no unfunded mandates which get passed along to ratepayers.**