FEDERAL ENERGY REGULATORY COMMISSION
News Release

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

September 14, 2020

News Media Contacts:
FERC: Mary O'Driscoll, mediadl@ferc.gov
NERC: Kimberly Mielcarek,
Kimberly.mielcarek@nerc.net

FERC, NERC Staff Outline Cyber Incident Response, Recovery Best Practices

Staff of the Federal Energy Regulatory Commission (FERC) and the North American Electricity Reliability Corporation (NERC) today published a report on cyber planning for response and recovery that outlines best practices for the electric utility industry.

The joint staffs of FERC and NERC, and the NERC Regional Entities, developed today's report after interviewing subject matter experts from eight electric utilities of varying size and function. The report includes the joint staffs' observations on their defensive capabilities and on the effectiveness of their Incident Response and Recovery (IRR) plans.

The report identifies common elements among the IRR plans: They define their scope, computer security events and incidents, staff roles and responsibilities, levels of authority for response, reporting requirements, requirements and guidelines for external communications and information sharing, and procedures to evaluate performance.

The report also identifies best practices, finding that effective IRR plans:

- Contain well-defined personnel roles, promote accountability and empower personnel to act without unnecessary delays, and use supporting technology and automated tools while recognizing the importance of human performance;
- Require well-trained personnel who are constantly updating their skills and incorporate lessons learned from past incidents or tests;
- Use baselining so personnel can detect significant deviations from normal operations, and flowcharts or decision trees to determine quickly when the utility reaches a predefined risk threshold and a suspicious set of circumstances qualifies as an event;
- Remove all external connections when activated, and consider the possibility that a containment strategy may trigger predefined destructive actions by the malware, and employ evidence collection and continued analysis to determine whether an event indicates a larger compromise;
- Consider the resource implications of incident responses of indeterminate length; and
- Implement lessons learned from previous incidents and simulated activities.

The report concludes that effective IRR plans are important resources for addressing cyber threats, and that effective IRR plans should be in place and response teams should be prepared to detect, contain, and, when appropriate, eradicate cyber threats before they can harm utility operations.

-30-