Cyber Planning for Response and Recovery Study: 2020 FERC, NERC and REs Report

Walter Wright, Jr.
wwright@mwlaw.com
(501) 688.8839

10/15/2020

The Federal Energy Regulatory Commission ("FERC"), North American Electricity Reliability Corporation ("NERC") and Regional Entities ("REs") released a September 2020 report titled:

Cyber Planning for Response and Recovery Study ("Report")

The *Report* addresses cyber planning for response and recovery outlining what it describes as best practices for the electric utility industry.

Development of the *Report* is stated to have included interviewing subject matter experts from eight electric utilities. The utilities are stated to have varied in size and function. Included in the *Report* are the FERC, NERC, and REs staffs' observations on their respective defense capabilities. Further described are their views on the effectiveness of Incident Response and Recovery plans.

Cyber threats are described as posing a risk to electric utilities because they can:

- Impact operations
- Impose substantial costs

A utility's Incident Response and Recovery plan describes how it will respond to a cyber incident. It includes phases and procedures.

The *Report* notes that:

. . . Establishing clear procedures for handling incidents is a complex undertaking and, though individualized to an organization's mission, size, structure, and functions, generally contain common elements . . .

The common elements are described as:

1. they define their scope (to whom they apply, what do they cover, and under what circumstances); and
2. they define computer security events and incidents, staff roles and responsibilities, levels of authority for response (e.g., authority to disconnect equipment), reporting requirements, requirements and guidelines for external communications and information sharing, and procedures to evaluate performance.

Best practices identified by the *Report* include:

- 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

A copy of the *Report* can be downloaded here.