Michael Best

February 19, 2020

Controlling Control Centers: FERC Approves Increased Data Security Controls for Bulk Electric System

The Federal Energy Regulatory Commission (FERC, or the Commission) continues to prioritize measures to safeguard the power grid against cybersecurity concerns. On January 23, 2020, FERC issued four orders aimed at improving the bulk power grid, with one of those orders directly influencing cybersecurity grid reliability. This order approves a new Critical Infrastructure Reliability (CIP) Standard improving data communication between bulk electric system Control Centers.

FERC's final rule in Order No. 866, accepts Reliability Standard CIP-012-1 which addresses communications between Control Centers. Reliability Standard CIP-012-1 was submitted by the North American Electric Reliability Corporation (NERC) – the Commission-certified Electric Reliability Organization (ERO). NERC's proposal comes in response to the Commission's 2016 Order No. 822 directing NERC to modify the Commission-approved CIP Reliability Standards to address the cybersecurity of the bulk electric system. Order No. 866 further directs NERC to modify CIP Reliability Standards to enforce protection of both the *availability of communication channels* and the *data communicated between bulk electric system Control Centers*.

In accepting NERC's proposal, FERC emphasized the importance of protecting the "confidentiality and integrity of real-time assessment and real-time monitoring data transmitted between bulk electric system control centers" by utilities and other energy industry participants. Importantly, the Commission also approved: 1) the violation risk factors, 2) violation severity levels, 3) implementation plan, and 4) an effective date of April 13, 2020, associated with the new CIP standard. FERC found it unnecessary to identify the types of data that must be protected under Reliability Standard CIP-012-1, and thus declined to adopt a proposal to do so.

Related Industries

Energy

Related Practices

Energy Law
Privacy & Cybersecurity
Regulatory

Industry participants objecting to the rule argued that existing cybersecurity standards already require redundancy in data-exchange capabilities in their control centers and that this rule is not necessary. However, FERC disagreed, finding that the current standards do not go far enough, since they do not create an obligation to protect the availability of those communication capabilities and the associated data, by applying appropriate security controls.

According to FERC, the new standard will affect reliability coordinators, generator owners and operators, transmission owners and operators, and balancing authorities – up to 719 entities. Reliability Standard CIP-012-1 requires responsible entities to:

- Identify security protections that will mitigate the risks of unauthorized disclosure and modification of Real-time Assessment and Real-time monitoring data being transmitted between Control Centers;
- Identify where to apply security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and
- Identify, in cases where the Control Centers are owned or operated by different entities, the responsibilities of each entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

The agency stated that about 82% of the affected parties would be “small entities,” projected to incur compliance costs of $49,067 in the first year of implementation, half of which will be for paperwork alone; however, annual paperwork costs will drop to $7,594 in subsequent years. For larger utilities, compliance costs would reach up to $23 million in one-time costs, and $5.4 million in annual costs thereafter.

To learn more about how the new CIP standard affects your business, or for assistance with developing or updating your vendor cybersecurity risk management program, please contact your Michael Best attorney in either of our energy or privacy and cybersecurity practice groups. Michael Best is committed to tracking regulatory developments affecting this, as well as other standards pertaining to cybersecurity and data privacy for the energy industry.

Related People

Elizabeth Rogers
Partner
earogers@michaelbest.com
T 512.640.3164