Michael Best

June 25, 2020

FERC Makes Major Moves Towards Increasing Grid Cybersecurity through Standards

Related Industries

Energy

Related Practices

COVID-19 Resource Center
Privacy & Cybersecurity

Since the onset of the COVID-19 pandemic, utilities have experienced an increase in ransomware and other cybersecurity attacks, and the Department of Energy advised the energy sector to remain vigilant to these cybersecurity threats. Only months after this warning, the Federal Energy Regulatory Commission (FERC, or the Commission), on June 18, 2020, issued a Notice of Inquiry (NOI) seeking comments on potential cyber-related enhancements to the Critical Infrastructure Protection (CIP) Reliability standards.

These enhancements are the result of FERC's recent comparison of the current CIP Reliability standards with National Institute of Standards and Technology (NIST) Cyber Security Framework (NIST Framework). The NIST Framework sets forth a comprehensive, repeatable structure to guide cybersecurity activities and to consider cybersecurity risks as part of an organization's risk management processes of its critical infrastructure. Seeking consistency with the NIST Framework, the Commission compared the content of the NIST Framework with the substance of the CIP Reliability Standards, and identified certain topics addressed in the NIST Framework that were not adequately addressed in the CIP Reliability Standards.

The Commission identified potential cybersecurity gaps in the areas of data security, detection of anomalies and events, and mitigation of cybersecurity events; the Commission also highlighted the risk of a coordinated cyberattack on geographically distributed targets. FERC seeks comment on whether Commission action, including modifications to the CIP Reliability Standards, would be appropriate to address such risk.

The major shortcoming that FERC identified in the current standards is that they do not adequately extend to parts of the bulk electric system's (BES) Cyber Systems that have a "low impact" rating. The Commission is concerned that, if a

low impact BES Cyber System is compromised, it can potentially be used to gain access to other BES Cyber Systems, including medium and high impact BES Cyber Systems.

In the area of data security, FERC found that current CIP Reliability Standards do not ensure enough capacity to consistently maintain information availability, which is necessary to effectively operate or restore the BES. Existing standards relating to information protection and communication between control centers do not address availability or apply to low impact BES Cyber Systems. FERC also found that the current CIP Reliability Standards do not broadly require mechanisms that verify the integrity of software, firmware, and information.

With regard to cyber anomalies and events, FERC determined that internal controls should require that: (1) a baseline of network operations and expected data flows for users and systems is established and managed; (2) detected events are analyzed to understand attack targets and methods; (3) event data are aggregated and correlated from multiple sources and sensors; (4) the impact of events is determined; and (5) incident alert thresholds are established. Currently, CIP Reliability Standards that require incident response do not extend to low impact BES Cyber Systems.

According to the Commission, to ensure mitigation, standards should require that incidents are contained and mitigated, and newly identified vulnerabilities are mitigated or documented as accepted risks. The existing CIP Reliability Standards mandate documentation of cybersecurity incident response plans, but do not specifically require incident containment or mitigation, or apply to low impact BES Cyber Systems.

Finally, based on recent studies assessing the possible reliability impacts of a coordinated cyberattack on geographically distributed targets, the Commission expressed concern about the potential risk of such attacks. Geographically distributed generation resources are smaller than centralized generation and often do not meet the megawatt threshold to be categorized as high or medium impact BES Cyber Systems. As such, many of them are not required to comply with the full suite of CIP Reliability Standards. FERC seeks comments on whether modifications to the CIP Reliability Standards, including changes to the current megawatt thresholds, would be appropriate to address the risk of coordinated cyberattack on geographically distributed targets.

FERC's last NOI on cybersecurity CIP standards came after a 2015 cyberattack on the Ukraine grid that affected 225,000 customers, concerning utility regulators around the world. However, the Commission ultimately terminated the inquiry, which involved the cybersecurity of control centers used to monitor and control the BES, after receiving comments from the industry. Through comments, stakeholders indicated that FERC's proposed revisions would remove needed flexibility afforded by the then-current standards, while unnecessarily imposing increased costs to implement the changes. This June 2020 NOI could have similar effects on distributed generation assets, exposing them to a level of compliance and costs that they have not yet experienced. On the other hand, increased cybersecurity standards for distributed and low impact resources may provide increased protection for the overall bulk power grid, helping utilities protect their larger assets.

Importantly, the Commission also issued a notice that it published a White Paper discussing a potential new framework for providing transmission return on equity (ROE) incentives to utilities for cybersecurity investments – a move that could increase costs for transmission ratepayers. The White Paper proposes two possible ways to identify investments eligible for incentives. In the first proposal, a utility could seek incentive treatment for applying CIP Reliability Standards requirements to transmission facilities that are not subject to those requirements. The second way involves an applicant's demonstration that a

cybersecurity investment meets NIST security controls and would *exceed* the requirements of the CIP Reliability Standards. According to the White Paper, under each proposal, utilities could be eligible for an ROE adder as high as 200 basis points.

FERC has given stakeholders until **August 17, 2020** to comment on the cybersecurity transmission incentives White Paper. Meanwhile, initial comments on the NOI are due **August 24, 2020**, and reply comments are due September 22, 2020. The Michael Best Energy Cyber Security team has broad experience assisting energy industry stakeholders to advocate for their business interests before FERC, which can strongly influence the outcome of these two cybersecurity related proceedings. To discuss the impact on of the NOI or the White Paper on your business, or for assistance preparing responsive comments, please contact Elizabeth Rogers, Uju Okasi, or Eric Callisto.

Related People

William Booth
Partner
wdbooth@michaelbest.com
T 202.747.9568

Eric Callisto
Partner
ejcallisto@michaelbest.com
T 608.283.4437

Elizabeth Rogers
Partner
earogers@michaelbest.com
T 512.640.3164