GT GreenbergTraurig

Alert | Energy & Natural Resources

June 2020

FERC Announces Potential Changes to Critical Infrastructure Protection (CIP) Standards for Cybersecurity of the Bulk Electric System (BES)

On June 18, 2020, the Federal Energy Regulatory Commission (FERC, or the Commission) issued a Notice of Inquiry (NOI) to seek comment on whether the currently effective Critical Infrastructure Protection (CIP) Reliability Standards for the Bulk Electric System (BES) adequately address (i) cybersecurity risks pertaining to data security, (ii) detection of "anomalies" and "events," and (iii) mitigation of cybersecurity events. FERC also seeks comment on the potential risk of a coordinated cyberattack on geographically distributed targets and whether modifications to the CIP Reliability standards would be appropriate to address such a risk.

The NOI is part of a growing trend of recent federal action on the cybersecurity of the grid, including President Trump's Executive Order on BES equipment sourced from "foreign adversary" countries, as discussed in an earlier GT Alert. FERC's ultimate decision will be binding upon the entities that own cyber and physical assets affected by any new CIP Reliability Standards.

Specifically, FERC staff reviewed the National Institute of Standards and Technology (NIST) Cyber Security Framework (NIST Framework)[1] and compared it with the substance of the CIP Reliability

[1] The NIST Framework consists of five "Functions" that provide a strategic-level view of cybersecurity: Identify, Protect, Detect, Respond, and Recover).

© 2020 Greenberg Traurig, LLP

Standards to identify certain topics in the NIST Framework that may not be adequately addressed in the CIP Reliability Standards.

Commission Staff arrived at the categories selected for comment (data security, detection of anomalies and events, and mitigation of cybersecurity events) based on review of the NIST Framework and current standards, noting that while CIP Reliability Standards have been updated multiple times since the first mandatory standards were issued in 2008, new cyber threats continue to evolve and may warrant further updates to the standards.

The NOI further explains that the strategy of Commission-approved CIP Reliability Standards with regard to cybersecurity is risk-based and intended to provide "defense in depth" (or multiple, redundant "defensive" measures). In general, planning for a reliable grid is based on the ability to withstand the single largest contingency possible, known as the N-1 event, and FERC now questions whether greater defense in depth is warranted to protect from a coordinated attack on multiple cyber assets important to the grid.

The NOI also notes that the grid's transition from larger, centralized generation resources to smaller, more geographically distributed generation resources may exacerbate the risk of a coordinated attack (a related concern to the increased "threat surface" that proliferation of individual distributed assets may create[2]). This suggests that FERC may pay particular attention to distributed generation resources and other grid assets that were historically considered too small, individually, to be subject to CIP Reliability Standards (e.g., the NOI states that FERC is considering "potential modifications to the current MW thresholds [of CIP Reliability Standards]").

If FERC concludes that geographically distributed "targets" include any physical or cyber assets connected to the distribution-level, retail sale grid, then coordination with state public utility commissions may be required. However, the NOI currently makes no mention of such an eventuality.

The Commission's NOI provides specific questions under each of the three categories, with Initial Comments due Aug. 24, 2020, and Reply Comments due Sept. 22, 2020.

Authors

This GT Alert was prepared by:

- Rabeha Kamaluddin | +1 202.331.3197 | kamaluddinr@gtlaw.com
- Gregory K. Lawrence | +1 202.641.2293 | lawrenceg@gtlaw.com
- Jack T. LeBris Erffmeyer | +1 202.530.3100 | lebriserffmeyerj@gtlaw.com
- Thomas O. Lemon | +1 617.310.6215 | lemont@gtlaw.com

* Special thanks to Pablo Ortiz Mena for his valuable assistance in preparing this GT Alert.

Albany. Amsterdam. Atlanta. Austin. Boca Raton. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.¬ Houston. Las Vegas. London.* Los Angeles. Mexico City.+ Miami. Milan.» Minneapolis. Nashville. New Jersey. New York.

[2] *See* CyberX, 2020 Global IoT/ICS Risk Report (via download).

Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ¬Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Santa Maria, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ¤Greenberg Traurig Tokyo Law Offices are operated by GT Tokyo Horitsu Jimusho, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by Greenberg Traurig Grzesiak sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in Greenberg Traurig Grzesiak sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2020 Greenberg Traurig, LLP. All rights reserved.*