Van Ness Feldman LLP

vnf.com

FERC Raises the Threshold for Cyber Incident Reporting

JULY 24, 2018

Darshana Singh and Gwen Keyes Fleming

Over the past year, the Federal Energy Regulatory Commission ("FERC" or the "Commission") has become increasingly vocal about their commitment to prioritize cybersecurity and protect the U.S. electric grid from cyber threats. In furtherance of this endeavor, last week the Commission issued a final rule (Order No. 848) which directs the North American Electric Reliability Corporation ("NERC") to expand its critical infrastructure protection standards ("CIP" standards) related to the reporting of cyber incidents. Under the current standard, entities are only required to report *successful* compromises which, the Commission found, is too low of a reporting threshold because it does not capture the full scope of cyber threats facing the electric grid. To address this gap, Order No. 848 is now requiring entities to report any *attempts* to compromise. Through issuing this final rule, FERC is seeking to bolster existing cyber standards without imposing unnecessary additional burdens on industry stakeholders. At the same time, FERC is seeking to better align the CIP standards to the reporting regimes used at the Department of Homeland Security and the Electricity Information Sharing and Analysis Center ("E-ISAC").

In addition to expanding the scope of reportable cyber incidents, Order No. 848 prescribes the content of the reports, the filing deadlines for reports and also the dissemination of reports. With these changes, FERC has added more standardization to the reporting process by laying out the minimum information requirements for a cyber-incident report. At NERC's request, FERC has provided some flexibility to ensure that NERC has the ability to shape the reporting requirements in a manner that maximizes efficiency while minimizing the burden on industry stakeholders, but is also effective for regulators.

This final rule, along with Order Nos. 840 and 843 issued earlier this year, dealing with event reporting and access control security respectively, demonstrate that FERC is delivering on its promise to bolster the grid's resiliency against cyber risks facing the energy sector. The urgent-manner in which the Commission is operating in this space further indicates that FERC views cyber as a high-priority issue that warrants an appropriate level of attention and investment of industry resources to meet the evolving threats.

For more information

Van Ness Feldman's cybersecurity team is prepared to help clients navigate the rapidly-evolving cybersecurity legal and policy landscape. If you have questions about FERC Order No. 848 or any other recent cyber developments, please contact Gwen Keyes Fleming, R. Scott Nuzum, Darshana Singh, or any member of the firm's Cybersecurity practice at (202) 298-1800 in Washington, D.C. or in Seattle at (206) 623-9372.

Follow us on Twitter @VanNessFeldman