Van Ness Feldman LLP
vnf.com

Significant Cyber Supply Chain Management Changes on the Horizon for Electric Utilities

OCTOBER 31, 2018

Gwen Keyes Fleming and *Darshana Singh*

On October 18, 2018 the Federal Energy Regulatory Commission ("FERC") approved three (3) Critical Infrastructure Protection (CIP) Reliability Standards including a long awaited supply chain risk management standard for the electric sector which, among other things, will require electric utilities to develop, document, and implement a supply chain cybersecurity risk management plan for any cyber systems that are classified as "medium" or "high" impact as defined by the North American Electric Reliability Corporation ("NERC"). The new regulations are aimed at ensuring software integrity and authenticity, strengthening vendor remote access protections and addressing vendor risk management procedures and controls. Responsible entities will have until June 2020 to comply with the new standards, in large part because it is projected that compliance will require significant technical upgrades which could impact long-term capital budgets and planning cycles.

Currently there are 1,250 U.S. entities ("responsible entities") subject to mandatory compliance with NERC's Reliability Standards. While responsible entities are within NERC's jurisdiction and must comply with NERC Reliability Standards, NERC cannot impose obligations on non-jurisdictional entities such as suppliers, vendors or other companies that tangentially provide products or services to responsible entities in the energy space. However, these regulations will *indirectly* impose obligations on those doing business with electric utilities because the regulations influence the procurement process by requiring responsible entities to mitigate any risk resulting from the interface with outside vendors.

In addition to approving the three (3) new Reliability Standards, FERC directed NERC to expand the scope of the standards to incorporate Electronic Access Control and Monitoring Systems ("EACMS"). EACMS include firewalls, authentication servers, security event monitoring systems and other intrusion detection or alert systems. In its order, FERC explained that EACMS provide the first line of defense against cyber threats to several integral operational systems and therefore must be included in the new Reliability Standards. In addition to adding EACMS, NERC has committed to further evaluating whether the reliability standards should be expanded even further to include other cyber assets and systems such as motion sensors and badge readers that control access to a facility's physical perimeter. Given that the industry has asked NERC to take an active role in helping utilities tackle cybersecurity supply chain risk management challenges, moving forward, NERC may consider establishing a third party accreditation process to augment utility procurement processes and further bolster resiliency and national security.

For more information

For more detailed information on the new reliability standards, including whether and how the standards impact your utilities, or assistance with developing a compliance plan please contact Gwen Keyes Fleming, Darshana Singh, or any other member of the cybersecurity team.

Follow us on Twitter @VanNessFeldman