PUBLICATION

FERC Imposes Cybersecurity Standards on Third-Party Utility Vendors

Authors: Danielle M. Aymond, Alisa L. Chestler
February 26, 2019

Effective December 2018, the Federal Energy Regulatory Commission (FERC) approved supply chain risk management Reliability Standards (Order No. 850) that require all utilities to develop and implement a security controls plan for hardware, software, and services associated with bulk electric system operations. This rule also transfers cybersecurity standards onto third-party vendors of utilities. While compliance checks will start July 2020, all utilities and vendors need to be working toward meeting the outlined obligations as soon as possible to avoid disruptions and to ensure timely compliance.

Standard	Requirement(s)	Security Objective
CIP-013-1: Cybersecurity: Supply Chain Risk Management	Utilities must develop and implement one or more documented plans/policies that must address as applicable: (1) vendor security event notification; (2) coordinated incident response; (3) vendor personnel termination notification; (4) product/services vulnerability disclosures; (5) verification of software integrity and authenticity; and (6) coordination of vendor remote access controls.	Ensure Utilities establish organizationally defined processes that integrate a cybersecurity risk management framework into the system development lifecycle.
CIP-005-6: Cybersecurity: Electronic Security Perimeter(s)	Utilities must address Interactive Remote Access and system-to-system remote access **when procuring** industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. Utilities must be able to determine active vendor remote access sessions and have one or more methods to disable active vendor	Provide awareness of all active vendor remote access sessions, both Interactive Remote access and system-to-system remote access, that are taking place on a Utility's system.

	remote access sessions.	
CIP-010-3: Cybersecurity: Configuration Change Management and Vulnerability Assessments	Requires that the publisher is identified and the integrity of all software and patches are confirmed. Utilities must verify software integrity and authenticity prior to a change from the existing baseline configurations, if the software source provides a method to do so. Utilities must verify the identity of the software source and the integrity of the software obtained by the software sources prior to installing software that changes established baseline configurations, when methods are available to do so.	Ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Although utilities and their vendors may have already taken steps toward achieving many of the practices outlined in Order No. 850, this rule requires established organizational defined processes that are reduced into a written plan in policy(ies) that is auditable. Entities need to apply the rules to their needs and characteristics while balancing against over-promising on their capability and in effect causing themselves an unnecessary liability.

The utilities' developed plan will need to entail the training of procurement departments and legal counsels, not necessarily previously trained or consulted regarding cybersecurity. The entire procurement process for utilities will need to be reviewed and updated, if necessary, for compliance.

Policy drafting in the ever-changing technology and cybersecurity sector is particularly difficult. Practices and technology are quickly outdated, and it's crucial that policies outlining cybersecurity plans do not expose an entity to unnecessary liability by over-promising.

A few tips to drafting new Order No. 850 policy:

- Include in your process a record retention plan that is sustainable and also will provide evidence of compliance to Order No. 850 that includes training records and emails
- Establish an ongoing process for reviewing and updating policies to ensure the use of the latest industry standards and regulatory rules
- Seek redundancy when possible ensuring verification steps are taken
- Designate an accountability official to implement and enforce the policy
- Ensure the mechanisms adopted to meet the requirements of Order No. 850 are effective and maintainable
- Involve management, procurement, and legal departments into the process

The rule provides just the minimum expected of utilities and their contractors; however, Regulators are already strictly enforcing cybersecurity standards with increasing fines. The North American Electric Reliability Corporation (NERC) announced this month a Notice of Penalty with a $10 million settlement for 127 violations of the Critical Infrastructure Protection (CIP) NERC Reliability Standards. Many of the violations were cited because the entity failed to follow their own documented process.

Order No. 850 also notes changes for the Utilities and their contractors on the horizon. It directs NERC to develop modifications to the supply chain risk management Reliability Standards to expand to include Electronic Access Control and Monitoring Systems (EACMS). It also directed the study of expanding the supply chain risk management Reliability Standards to include Physical Access Control Systems (PACS) and Protected Cyber Assets (PCA).

The natural gas and oil pipeline industry should expect a similar future. The Transportation Security Administration (TSA) remains under scrutiny for falling behind in the cybersecurity fight. Even though it released new guidelines last year, the Government Accountability Office released a critical report, *Actions Needed to Address Significant Weakness in TSA's Pipeline Security Program Management*, in December making ten recommendations including the establishment of better processes for updating guidelines and assessing risks. FERC has encouraged TSA to adopt the same mandatory rules it placed on Utilities.

For more information on Order No. 850 and how it may affect your business operations, contact the author, Danielle Aymond, or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.