FERC APPROVES NEW SUPPLY CHAIN RELIABILITY STANDARDS TO ADDRESS CYBER SECURITY RISKS

On October 18, 2018, FERC issued a final rule approving a package of NERC CIP Standards supporting supply chain cyber security risk management, including new CIP-013-1. This final rule is the culmination of over three years of regulatory developments to satisfy FERC's initial concern that supply chain management controls were necessary to address security gaps in the NERC CIP Standards.

As the BES supply chain continues to grow in complexity, the cyber vulnerabilities presented by vendors and suppliers have in turn increased. Organizations that are prepared to meet these new regulatory obligations with a robust risk management plan and associated controls will be better positioned to mitigate potential supply chain threats identified by FERC.

In short, the Standards will require responsible entities to do the following:

- Develop and implement a supply chain cyber security risk management plan, including a process to identify and assess risks from vendor equipment and software, and obtain CIP Senior Manager approval of the plan at least once every 15 calendar months (CIP-013-1)
- Have a method(s) to determine active vendor remote access sessions and to disable such access (CIP-005-6)
- Verify the identify and integrity of software and its source prior to making a change from the existing BES baseline configuration (CIP-010-3).

The risk management plans must include supply chain security controls for industrial control system hardware, software and services associated with BES operations.

Notably, these Standards will only apply to High and Medium Impact BES Cyber Systems (BCS), although many of these activities are equally as important for Low Impact-only responsible entities to consider as part of their procurement and vendor management processes. FERC will await the findings from a NERC Board-directed final report evaluating the supply chain risks presented by Low Impact BCS prior to considering their inclusion in another version of these Standards. The Standards will not impose any direct obligations on vendors providing products or services to responsible entities.

FERC approved NERC's request for an **18-month** implementation period, recognizing the timeline required to not only develop and implement a risk management plan but also make necessary technical upgrades to meet the CIP Standards (likely effective on or around July 1, 2020).

These requirements are meant to be forward-looking, applying to new procurement processes as of the effective date of CIP-013-1. Responsible entities will not be required to renegotiate or abrogate (i.e., terminate) existing vendor contracts, including amendments to master agreements and purchase orders.

Given the implementation timeline set by FERC and the potential challenges presented by CIP-013-1, responsible entities should begin to consider new or updated procurement/vendor management processes and controls they can use to support risk management.

GridSME recommends the following as some guiding practices:

- Be sure to engage multiple business units and subject matter experts at your organization when you develop your risk assessment program;
- Consider developing a matrix of risks presented by vendors and systems, and identify those supply chain controls that can mitigate risk in various instances;
- Develop new language for your RFPs and procurement contracts involving BCS to include the CIP-013-1 security expectations for vendors and suppliers, and be prepared to negotiate; and
- Promote continuous improvement in your staff by monitoring supply chain threats and risks facing our industry.

GridSME has been tracking these developments at FERC and NERC since they were proposed, including the various resources available to the industry to assess risks, develop a compliant risk management plan, and update vendor contract language that will fit within the context of your existing supply chain program. Please contact us if you are interested in learning how we can help you understand the new Standards and develop a roadmap to meet the upcoming compliance requirements.