THE
NATIONAL LAW REVIEW

NERC Proposes to Reduce Cybersecurity Risks in CIP Supply Chains

Thursday, October 5, 2017

The proposed Reliability Standards focus on vulnerabilities in vendor products and services and would regulate the utility procurement process.

Morgan Lewis

Article By
J. Daniel Skees
Arjun Prasad Ramadevanahalli
Morgan, Lewis & Bockius LLPLaw Flash

Environmental, Energy & Resources
All Federal

On September 26, the North American Electric Reliability Corporation (NERC) petitioned the Federal Energy Regulatory Commission (FERC or the Commission) for approval of a suite of Reliability Standards addressing supply chain cybersecurity risk management (the Petition). The proposed Reliability Standards—CIP-013-1 (Supply Chain Risk Management), CIP-005-6 (Electronic Security Perimeter(s)), and CIP-010-3 (Configuration Change Management and Vulnerability Assessments)—respond to the Commission's directive in Order No. 829 directing NERC to develop Reliability Standards addressing cybersecurity risks in the supply chains supporting utility control systems.

If approved, the proposed Reliability Standards would obligate Registered Entities to develop a plan to mitigate supply chain cybersecurity risks posed by vendor products and services, particularly during the vendor procurement process. Although the Standards only directly regulate those entities subject to FERC's jurisdiction under Section 215 of the Federal Power Act, i.e., the "users, owners, and operators of the bulk-power system," anyone providing IT equipment and related services to electric utilities will also need to be cognizant of these proposed changes, which are likely to alter future contracts and other arrangements with electric utilities.

The Commission has not yet set a deadline for comments on NERC's proposal.

Background

The industrial control systems, IT infrastructure, and telecommunications systems used by electric utilities for Bulk Electric System (BES) operations continue to grow increasingly complex. To meet the challenges of administering those complex systems, utilities often rely on third-party vendors to install and administer the technology used to support BES reliability. However, the supply chains required for that technology can be extensive, opaque, and subject to exploitation. As NERC observed in its Petition, "Multiple entities across the globe may participate in the development, design, manufacturing, and delivery of a single product purchased by a registered entity."

Responding to concerns over those risks, the Commission convened a staff-led technical conference on supply chain risk management in January 2016. Following the technical conference, the Commission issued Order No. 829 directing NERC to develop a Reliability Standard that addresses supply chain risk management. The Commission found that supply chains under existing vendor arrangements provide various opportunities for potential attackers to exploit vulnerabilities in the systems and components acquired from those vendors. The Commission highlighted specific supply chain risks, such as the insertion of counterfeit components or malicious software as well as poor vendor manufacturing and development practices. To address the myriad security concerns, the Commission determined that the new or modified Reliability Standard should require utilities to

- verify software integrity and authenticity;
- secure vendor remote access;
- enhance planning for information systems; and

- implement vendor risk management and procurement controls.

Because Section 215 of the Federal Power Act, the authority for FERC to approve Reliability Standards, does not confer the Commission with jurisdiction over the actual vendors, the Commission directed NERC to develop a standard that addresses the obligations of utilities as they engage with vendors for products or services supporting BES operations. The Commission also specified that any proposed requirements should only be prospective and apply to new vendor contracts.

NERC's Petition

In response to the Commission's directive in Order No. 829, and following a lengthy and contentious stakeholder development process, NERC proposed new Reliability Standard CIP-013-1, addressing supply chain risk management. NERC also proposed revisions to two existing Reliability Standards in proposed CIP-005-6 and CIP-010-3 to fully address the Commission's directives.

New Proposed Reliability Standard CIP-013-1 – Supply Chain Risk Management

Proposed Reliability Standard CIP-013-1 would ensure that Registered Entities establish and implement organizationally defined processes that integrate a cybersecurity risk management framework. Because the proposed Standard is focused on the processes Registered Entities must implement to mitigate supply chain risk, it does not require any specific controls or contract requirements. Instead, the Standard would allow utilities to design their own processes that incorporate certain minimum risk mitigation concepts:

- Identification and assessment of cybersecurity risks to the BES resulting from the procurement of vendor products and services or the transition between vendors
- Required vendor security event notification
- Coordinated incident response activities to vendor-identified events
- Vendor personnel termination notification for vendor employees with access to remote and onsite systems
- Product and service vulnerability disclosures by the vendor
- Verification of software integrity and authenticity for all software and patches provided by the vendor for use in the BES Cyber System
- Coordination of vendor remote access controls
- Periodic reassessment by the Registered Entity of the processes used to address the above concepts

Under the proposal, CIP-013-1 will only apply to IT systems at the most critical electric facilities (those systems identified as high- and medium-impact BES Cyber Systems under CIP-002-5.1a). However, NERC expressed hope that the vendor community servicing the electric industry would begin to include the CIP-013-1 security concepts in their BES Cyber System products and contracts, regardless of the associated impact level.

NERC stressed that the proposed Standard is intended to be flexible enough to account for the disparity in purchasing power among various Registered Entities. For example, a Registered Entity may not have the negotiating leverage to obtain each of its desired cybersecurity controls in its vendor contracts due to factors such as expense, limited supply sources, and relative maturity of the vendor's product line. Thus, NERC explained that failure to obtain a specific contract provision for one of the risk mitigation concepts would not result in a violation. NERC anticipates that compliance with CIP-013-1 will be assessed based on whether the Registered Entity integrated the risk mitigation concepts into its procurement activities and implemented those processes "in good faith." In particular, NERC said the compliance enforcement authority will evaluate the steps the Registered Entity took to assess risks posed by a vendor and, based on that assessment, the steps that entity took to mitigate those risks, including the negotiation of security provisions in vendor contracts.

Proposed Modification to CIP-005-5 – Vendor Remote Access

NERC proposed to add two new subparts to existing CIP Reliability Standard CIP-005-5 that address vendor remote access sessions. Proposed Standard CIP-005-6 introduces subparts 2.4 and 2.5 to Requirement R2, and would require Registered Entities to implement methods to identify active vendor remote access sessions and to disable active vendor remote access. The proposed revisions complement the Interactive Remote Access requirements in CIP-013-1 and are intended to control vendor remote access in order to mitigate risks associated with unauthorized access.

Proposed Modification to CIP-010-2 – Software Integrity and Authenticity

Proposed Reliability Standard CIP-010-6 includes a new subpart to Requirement R1 to address the first Order No. 829 objective regarding verification of the identity of software publishers and the integrity of all software and patches intended for use on BES Cyber Systems. As the Commission explained in Order No. 829, this would reduce the likelihood that an attacker could exploit the vendor patch management process to deliver compromised software or patch updates to a BES Cyber System. Proposed Requirement R1 Part 1.6 would address that objective by obligating Registered Entities to verify the identity of the software source and the integrity of any software obtained from that source prior to installation. NERC noted that the Registered Entity can only meet its affirmative obligation to verify software integrity and authenticity if the vendor provides a method to do so. For that reason, NERC stressed the importance of the proposed CIP-013-1 requirement to address software authenticity and integrity in the vendor procurement stage.

Source URL: https://www.natlawreview.com/article/nerc-proposes-to-reduce-cybersecurity-risks-cip-supply-chains