THE
NATIONAL LAW REVIEW

FERC Issues Orders Concerning NERC Critical Infrastructure Protection Reliability Standards

Article By
Debra Ann Palmer
Melan Patel
Schiff Hardin LLP
Energy and Environmental Law Adviser

- Environmental, Energy & Resources
- Utilities & Transport

- All Federal

Friday, August 5, 2016

On June 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued three orders related to the North American Electric Reliability Corporation's (NERC) critical infrastructure protection reliability standards (CIP reliability standards). The Commission issued a final rule directing NERC to develop a new or modified reliability standard, an Order Denying Rehearing and a Notice of Inquiry.

Final Rule

Pillars, FERC

FERC issued a final rule directing that NERC develop a new or modified reliability standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations. The Commission directed NERC to develop a standard that addresses the following security objectives:

1. Software publisher identity and integrity of software and patches before they are installed in the BES Cyber System environment;

2. Logging and control of third-party vendor remote access;

3. How a responsible entity will include security considerations as part of its information system planning and system development lifecycle process; and

4. Vendor risk management and procurement controls in future contracts for industrial control system hardware, software, and computing and networking services associated with BES operations.

The Commission stated that the new or modified reliability standard should require responsible entities to develop a plan to meet the four objectives, or some equally efficient and effective means to meet these objectives, while providing flexibility to responsible entities as to how to meet the objectives.

FERC, in determining the need for this directive, found that “attacks targeting the supply chain are on the rise, particularly attacks involving third party service providers.” The Commission noted that supply chain risks include the “insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software, and inadequate safety measures in manufacturing and development practices.” FERC stated that existing Reliability Standards do not adequately protect against the increasing supply chain risks.

To ensure that the Commission and NERC stay within the ambit of Section 215 authority, the final rule states that NERC should only address obligations of responsible entities and not directly impose obligations on suppliers, vendors, or other entities that provide products or services to regulated entities. Further, NERC should not dictate the abrogation or renegotiation of currently effective contracts with vendors, suppliers, or other entities.

In the final rule, FERC directs that the reliability standard address verification of:

1. The identity of the software publisher for all software and patches intended for use on BES Cyber Systems; and

2. The integrity of the software and any patches, before installation in the BES Cyber System environment.

In addition, the standard must address both user-initiated and remote third party access to BES Cyber Systems. The standard must also address how entities include security considerations in system planning and development, particularly when installing new hardware. The reliability standard must also require specific cyber-security provisions in contracts for new software and hardware including vendor personnel termination notification for employees with access to remote and onsite systems and product and services vulnerability disclosures.

For the four objectives to be addressed by the new or modified reliability standard, FERC cited example policies developed by National Institute of Standards and Technology (NIST), the Department of Homeland Security and the Department of Energy.

Commissioner LaFleur dissented from the order, arguing that the Commission rushed development of the final rule, which will ultimately hamper the development and implementation of an enforceable standard. Commissioner LaFleur noted that the four objectives in the final rule were not included in the supply chain NOPR, thus interested parties have not provided insight into whether these objectives adequately protect against supply chain risks. The Commissioner also argued that the final rule hampers NERC's ability to develop an effective and enforceable proposed standard for the Commission to consider because it truncates NERC's suggested timetable for development. The Commissioner recommended that instead of issuing a final rule, the Commission should issue a supplemental NOPR in order to allow for greater stakeholder participation.

Interested parties may participate in the development of the NERC standard, which NERC is required to file with the Commission for approval within one year following publication in the Federal Register. The final rule was published in the Federal Register on July 28, 2016 and becomes effective on September 27, 2016.

Order 822-A, Order Denying Rehearing

FERC Denied a Request for Rehearing of Order No. 822. In Order No. 791, in which FERC approved the CIP Version 5 reliability standards, FERC had directed NERC to develop a new or modified reliability standard that addressed the protection of nonprogrammable components of communications networks, and to develop a definition of "communication networks" for the NERC Glossary of Terms Used in Reliability Standards. In Order 822, FERC approved NERC's proposed alternative to the directive in Order No. 791, while also directing NERC to modify standard CIP-006-6 to require responsible entities to implement controls to protect, at a minimum, communications links and sensitive BES data communicated between BES Control Centers in a manner that is appropriately tailored to address the risks posed to the BES by the assets being protected. FERC found that NERC's alternative addressed, in part, the concerns in Order No. 791 regarding the security of nonprogrammable components of communications networks. Certain parties filed

requests for rehearing, arguing that the Commission erred in accepting NERC's alternative, because it did not include an "inclusive" definition of communications networks, including "substations," and therefore violated the intent of Section 215 of the Federal Power Act.

The Commission denied rehearing, stating that there is no support for the assertion that Section 215 requires a definition of communications networks for inclusion in the NERC Glossary. FERC concluded that directives in Order No. 822 addressed Petitioner's assertions regarding the need to define the term "communications network." FERC found that Petitioner's request would require NERC to develop standards that would apply to distribution level substations; however, this would exceed the scope of FERC's and NERC's authority under Section 215, which excludes facilities used in the local distribution of electricity from the definition of the Bulk-Power System.

FERC rejected Petitioner's argument that the December 2015 cyber attack in Ukraine should play a role in the decision, instead holding that future rulemaking proceedings will address the lessons learned from the attack. The FERC's Notice of Inquiry, explained below, begins the process of implementing those lessons.

FERC also rejected a request for rehearing that the Commission erred in Order No. 822 by not requiring the removal of malware currently embedded in the Bulk-Power system. FERC found that the CIP reliability standards, specifically CIP-007-6, already address the threat to the Bulk-Power system posed by malicious code.

Notice of Inquiry

FERC also issued a Notice of Inquiry regarding potential modifications to the CIP reliability standards. The Notice of Inquiry stems from the Ukraine cyber attack and addresses lessons learned from analyses performed by the Electricity Information Sharing and Analysis Center, SANS Industrial Control Systems, and the U.S. Department of Homeland Security.

In the Notice of Inquiry, FERC seeks comments regarding whether the CIP reliability standards should be modified to require:

1. Separation (physical or logical) between the Internet and the BES Cyber Systems in Control Centers that perform transmission operator functions; and

2. Computer administration practices that prevent unauthorized programs from running (application whitelisting).

FERC also seeks comment on the operational impact to the Bulk-Power System if BES Cyber Systems were isolated from the Internet in all Control Centers performing transmission operator functions.

The Commission noted various provisions of the existing CIP reliability standards that may require unused ports to be locked down and require electronic security perimeters, but observed that the current CIP reliability standards do not require isolation between the Internet and BES Cyber Systems in Control Centers performing transmission operator functions, through use of either physical (hardware) or logical

(software) means. FERC also observed that while NERC Guidelines and the Technical Basis document associated with standard CIP-007-6 Requirement 3 identify application whitelisting as an option for mitigating malicious cyber activity, its use is not mandatory. On this issue, the Commission seeks comment on whether application whitelisting is appropriate for all BES Cyber Systems in Control Centers or only for certain devices or components, as well as on the operational impact, including potential reliability concerns.

Comments are due September 26, 2016, 60 days from publication in the Federal Register.

The Final Rule is available at http://ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf

The Order on Rehearing is available at http://ferc.gov/whats-new/comm-meet/2016/072116/E-9.pdf

The NOI is available at http://ferc.gov/whats-new/comm-meet/2016/072116/E-10.pdf

The Press Release is available at http://www.ferc.gov/CalendarFiles/20160721130702-E-8-NEWS.pdf