156 FERC ¶ 61,050
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM15-14-002; Order No. 829]

Revised Critical Infrastructure Protection Reliability Standards

(Issued July 21, 2016)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule.

SUMMARY: The Federal Energy Regulatory Commission (Commission) directs the North American Electric Reliability Corporation to 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 operations. The new or modified Reliability Standard is intended to mitigate the risk of a cybersecurity incident affecting the reliable operation of the Bulk-Power System.

DATES: This rule will become effective **[INSERT DATE 60 days after publication in the FEDERAL REGISTER].**

FOR FURTHER INFORMATION CONTACT:

Daniel Phillips (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426
(202) 502-6387
daniel.phillips@ferc.gov

Simon Slobodnik (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426
(202) 502-6707
simon.slobodnik@ferc.gov

Kevin Ryan (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426
(202) 502-6840
kevin.ryan@ferc.gov

SUPPLEMENTARY INFORMATION:

156 FERC ¶ 61,050
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Norman C. Bay, Chairman;
Cheryl A. LaFleur, Tony Clark,
and Colette D. Honorable.

Revised Critical Infrastructure Protection Reliability Standards — Docket No. RM15-14-002

ORDER NO. 829

FINAL RULE

(Issued July 21, 2016)

1. Pursuant to section 215(d)(5) of the Federal Power Act (FPA),[1] the Commission directs the North American Electric Reliability Corporation (NERC) to 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 operations. The new or modified Reliability Standard is intended to mitigate the risk of a cybersecurity incident affecting the reliable operation of the Bulk-Power System.

2. The record developed in this proceeding supports our determination under FPA section 215(d)(5) that it is appropriate to direct the creation of mandatory requirements that protect aspects of the supply chain that are within the control of responsible entities

[1] 16 U.S.C. 824o(d)(5).

and that fall within the scope of our authority under FPA section 215. Specifically, we direct NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations.[2] The new or modified Reliability Standard should address the following security objectives, discussed in detail below: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. In making this directive, the Commission does not require NERC to impose any specific controls, nor does the Commission require NERC to propose "one-size-fits-all" requirements. The new or modified Reliability Standard should instead 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 those objectives.

[2] *Revised Critical Infrastructure Protection Reliability Standards*, Notice of Proposed Rulemaking, 80 Fed. Reg. 43,354 (Jul. 22, 2015), 152 FERC ¶ 61,054, at P 66 (2015) (NOPR).

I. Background

A. Section 215 and Mandatory Reliability Standards

3. Section 215 of the FPA requires a Commission-certified Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval. Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[1] Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[2] and subsequently certified NERC.[3]

B. Notice of Proposed Rulemaking

4. The NOPR, *inter alia*, identified as a reliability concern the potential risks to bulk electric system reliability posed by the "supply chain" (i.e., the sequence of processes involved in the production and distribution of, *inter alia*, industrial control system hardware, software, and services). The NOPR explained that changes in the bulk electric system cyber threat landscape, exemplified by recent malware campaigns targeting supply chain vendors, have highlighted a gap in the Critical Infrastructure Protection

[1] 16 U.S.C. 824o(e).

[2] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

[3] *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

(CIP) Reliability Standards.[4] To address this gap, the NOPR proposed to direct that NERC develop a forward-looking, objective-driven Reliability Standard that provides security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations.[5]

5. Recognizing that developing supply chain management requirements would likely be a significant undertaking and require extensive engagement with stakeholders to define the scope, content, and timing of the Reliability Standard, the Commission sought comment on: (1) the general proposal to direct that NERC develop a Reliability Standard to address supply chain management; (2) the anticipated features of, and requirements that should be included in, such a standard; and (3) a reasonable timeframe for development of a Reliability Standard.[6]

6. In response to the NOPR, thirty-four entities submitted comments on the NOPR proposal regarding supply chain risk management. A list of these commenters appears in Appendix A.

C. January 28, 2016 Technical Conference

7. On January 28, 2016, Commission staff led a Technical Conference to facilitate a dialogue on supply chain risk management issues that were identified by the Commission in the NOPR. The January 28 Technical Conference addressed: (1) the need for a new or modified Reliability Standard; (2) the scope and implementation of a new or modified

[4] NOPR, 152 FERC ¶ 61,054 at P 63.

[5] *Id.* P 66.

[6] *Id*.

Reliability Standard; and (3) current supply chain risk management practices and collaborative efforts.

8. Twenty-four entities representing industry, government, vendors, and academia participated in the January 28 Technical Conference through written comments and/or presentations.[7]

9. We address below the comments submitted in response to the NOPR and comments made as part of the January 28 Technical Conference.

II. Discussion

10. Pursuant to section 215(d)(5) of the FPA, the Commission determines that it is appropriate to direct NERC to develop a new or modified Reliability Standard(s) that address supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations.[1] Based on the comments received in response to the NOPR and at the technical conference, we determine that the record in this proceeding supports the development of mandatory requirements for the protection of aspects of the supply chain that are within the control of responsible entities and that fall within the scope of our authority under FPA section 215.

---

[7] Written presentations at the January 28, 2016 Technical Conference and the Technical Conference transcript referenced in this Final Rule are accessible through the Commission's eLibrary document retrieval system in Docket No. RM15-14-000.

[1] 16 U.S.C. 824o(d)(5) ("The Commission . . . may order the [ERO] to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses as specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section.").

11. In its NOPR comments, NERC acknowledges that "supply chains for information and communications technology and industrial control systems present significant risks to [Bulk-Power System] security, providing various opportunities for adversaries to initiate cyberattacks."[2] Several other commenters also recognized the risks posed to the bulk electric system by supply chain security issues and generally support, or at least do not oppose, Commission action to address the reliability gap.[3] For example, in prepared remarks submitted for the January 28 Technical Conference, one panelist noted that attacks targeting the supply chain are on the rise, particularly attacks involving third party service providers.[4] In addition, it was noted that, while many responsible entities are already independently assessing supply chain risks and asking vendors to address the risks, these individual efforts are likely to be less effective than a mandatory Reliability Standard.[5]

12. We recognize, however, that most commenters oppose development of Reliability Standards addressing supply chain management for various reasons. These

[2] NERC NOPR Comments at 8.

[3] *See* Peak NOPR Comments at 3-6; ITC NOPR Comments at 13-15; CyberArk NOPR Comments at 4; Ericsson NOPR Comments at 2; Isologic and Resilient Societies Joint NOPR Comments at 9-12; ACS NOPR Comments at 4; ISO NE NOPR Comments at 2-3; NEMA NOPR Comments at 1-2.

[4] Olcott Technical Conference Comments at 1-2.

[5] Galloway Technical Conference Comments at 1 ("…ISO-NE supports the Commission's proposal to direct NERC to develop requirements relating to supply chain risk management. We believe that the risks to the reliability of the Bulk Electric System that result from compromised third-party software are real, significant and largely unaddressed by existing reliability standards. While many public utilities are already assessing these risks and asking vendors to address them, these one-off efforts are far less likely to be effective than an industry-wide reliability standard.").

commenters contend that Commission action on supply chain risk management would, among other things, address or influence activities beyond the scope of the Commission's FPA section 215 jurisdiction.[6] Commenters also assert that the existing CIP Reliability Standards adequately address potential risks to the bulk electric system from supply chain issues.[7] In addition, commenters claim that responsible entities have minimal control over their suppliers and are not able to identify all potential vulnerabilities associated with each of their products or parts; therefore, even if a responsible entity identifies a vulnerability created by a supplier, the responsible entity does not necessarily have any authority, influence or means to require the supplier to apply mitigation.[8] Other commenters argue that the Commission's proposal may unintentionally inhibit innovation.[9] A number of commenters assert that voluntary guidelines would be more effective at addressing the Commission's concerns.[10] Finally, commenters are concerned

[6] *See* Trade Associations NOPR Comments at 24; Southern NOPR Comments at 14-16; CEA NOPR Comments at 4-5; NIPSCO NOPR Comments at 7.

[7] *See* Trade Associations NOPR Comments at 20-25; Gridwise NOPR Comments at 3; Arkansas NOPR Comments at 6; G&T Cooperatives NOPR Comments at 8-9; NEI NOPR Comments at 3-5; NIPSCO NOPR Comments at 5-6; Luminant NOPR Comments at 4-5; SCE NOPR Comments at 4.

[8] *See* Arkansas NOPR Comments at 5-6; G&T Cooperatives NOPR Comments at 9; Trade Associations NOPR Comments at 25.

[9] *See* Arkansas NOPR Comments at 6; G&T Cooperatives NOPR Comments at 9; NERC NOPR Comments at 13.

[10] *See* Trade Associations NOPR Comments at 23; Southern NOPR Comments at 13; AEP NOPR Comments at 5; NextEra NOPR Comments at 4-5; Luminant NOPR Comments at 5.

that the contractual flexibility necessary to effectively address supply chain concerns does not fit well with a mandatory Reliability Standard.[11]

13. As discussed below, we conclude that our directive falls within the Commission's authority under FPA section 215. We also determine that, notwithstanding the concerns raised by commenters opposed to the NOPR proposal, it is appropriate to direct the development of mandatory requirements to protect industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. Many of the commenters' concerns are addressed by the flexibility inherent in our directive to develop a forward-looking, objective-based Reliability Standard that includes specific security objectives that a responsible entity must achieve, but affords flexibility in how to meet these objectives. The Commission does not require NERC to impose any specific controls nor does the Commission require NERC to propose "one-size-fits-all" requirements. The new or modified Reliability Standard should instead 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 those objectives. Moreover, our directive comports well with the NOPR comments submitted by NERC, in which NERC explained what it believes would be the features of a workable supply chain management Reliability Standard.[12]

[11] *See* Arkansas NOPR Comments at 6; Southern NOPR Comments at 13.

[12] NERC NOPR Comments at 8-9. The record evidence on which the directive in this Final Rule is based is either comparable or superior to past instances in which the Commission has directed, pursuant to FPA section 215(d)(5), that NERC propose a Reliability Standard to address a gap in existing Reliability Standards. *See*, *e.g.*,

14. We address below the following issues raised in the NOPR, NOPR comments, and January 28 Technical Conference comments: (1) the Commission's authority to direct the ERO to develop supply chain management Reliability Standards under FPA section 215(d)(5); and (2) the need for supply chain management Reliability Standards, including the risks posed by the supply chain, objectives of a supply chain management Reliability Standard, existing CIP Reliability Standards, and responsible entities' ability to affect the supply chain.

A. Commission Authority to Direct the ERO to Develop Supply Chain Management Reliability Standards Under FPA Section 215(d)(5)

NOPR

15. In the NOPR, the Commission stated that it anticipates that a Reliability Standard addressing supply chain management security would, *inter alia*, respect FPA Section 215 jurisdiction by only addressing the obligations of responsible entities and not directly imposing obligations on suppliers, vendors, or other entities that provide products or services to responsible entities.[13]

Reliability Standards for Physical Security Measures, 146 FERC ¶ 61,166 (2014) (directing, without seeking comment, that NERC develop proposed Reliability Standards to protect against physical security risks related to the Bulk-Power System).

[13] NOPR, 152 FERC ¶ 61,054 at P 66.

Comments

16. Commenters contend that the Commission's proposal to direct NERC to develop mandatory Reliability Standards to address supply chain risks could exceed the Commission's jurisdiction under FPA section 215. The Trade Associations state that the NOPR discussion "appears to suggest a new mandate, over and above Section 215 for energy security, integrity, quality, and supply chain resilience, and the future acquisition of products and services."[14] The Trade Associations assert that the Commission's NOPR proposal does not provide any reasoning that connects energy security and integrity with reliable operations for Bulk-Power System reliability. The Trade Associations seek clarification that the Commission does not intend to define energy security as a new policy mandate.[15]

17. Southern states that it agrees with the Trade Associations that expanding the focus of the NERC Reliability Standards "to include concepts such as security, integrity, and supply chain resilience is beyond the statutory authority granted in Section 215."[16] Southern contends that while these areas "have an impact on the reliable operation of the bulk power system, […] they are areas that are beyond the scope of [the Commission's] jurisdiction under Section 215."[17] NIPSCO raises a similar argument, stating that the existing CIP Reliability Standards should address the Commission's concerns "without

[14] Trade Associations NOPR Comments at 24.

[15] *Id.*

[16] Southern NOPR Comments at 16.

[17] Southern NOPR Comments at 16; *see also* Trade Association NOPR Comments at 24.

involving processes and industries outside of the Commission's jurisdiction under section 215 of the Federal Power Act."[18]

18. Southern questions how a mandatory Reliability Standard that achieves all of the objectives specified in the NOPR "could effectively address [the Commission's] concerns and still stay within the bounds of [the Commission's] scope and mission under Section 215."[19] Southern asserts that "a reading of Section 215 indicates that [the Commission's] mission and authority under Section 215 is focused on the *operation* of the bulk power system elements, not on the acquisition of those elements and associated procurement practices."[20] In support of its assertion, Southern points to the definition in FPA section 215 of "reliability standard," noting the use and meaning of the terms "reliable operation" and "operation." Southern contends that "Section 215 standards should ensure that a given BES Cyber System asset is protected from vulnerabilities once connected to the BES, and should not be concerned about how the Responsible Entity works with its vendors and suppliers to ensure such reliability (such as higher financial incentives or greater contractual penalties)."[21]

19. The Trade Associations and Southern also observe that, while the NOPR indicates that the Commission has no direct oversight authority over third-party suppliers or vendors and cannot indirectly assert authority over them through jurisdictional entities,

[18] NIPSCO NOPR Comments at 7.

[19] Southern NOPR Comments at 14-15.

[20] *Id.* at 15 (emphasis in original).

[21] *Id.* at 16.

the NOPR proposal appears to assert that authority.[22] The Trade Associations maintain that such an extension of the Commission's authority would be unlawful and, therefore, seek clarification that "the Commission will avoid seeking to extend its authority since such an extension would set a troubling precedent."[23] CEA raises a concern that the NOPR proposal "appears to lend itself to the interpretation that authority is indirectly being asserted over non-jurisdictional entities."[24]

20. The Trade Associations also maintain that the Commission's use of the term "industrial control system" in the scope of its proposal suggests that the Commission is seeking to address issues beyond CIP and cybersecurity-related issues. The Trade Associations seek clarification that the Commission does not intend for NERC broadly to address industrial control systems, such as fuel procurement and delivery systems or system protection devices, but intends for its proposal to be limited to CIP and cybersecurity-related issues.[25]

Discussion

21. We are satisfied that FPA section 215 provides the Commission with the authority to direct NERC to address the reliability gap concerning supply chain management risks identified in the NOPR. We reject the contention that our directive could be read to address issues outside of the Commission's FPA section 215 jurisdiction.

[22] Trade Associations NOPR Comments at 24-25; Southern NOPR Comments at 17; *see also* Trade Associations Post-Technical Conference Comments at 20-21.

[23] Trade Associations NOPR Comments at 24-25.

[24] CEA NOPR Comments at 5.

[25] Trade Associations NOPR Comments at 25.

However, to be clear, we reiterate the statement in the NOPR that any action taken by NERC in response to the Commission's directive to address the supply chain-related reliability gap should respect "section 215 jurisdiction by only addressing the obligations of responsible entities" and "not directly impose obligations on suppliers, vendors or other entities that provide products or services to responsible entities."[26] The Commission expects that NERC will adhere to this instruction as it works with stakeholders to develop a new or modified Reliability Standard to address the Commission's directive. As discussed below, we reject the remaining comments regarding the Commission's authority to direct the development of supply chain management Reliability Standards under FPA section 215(d)(5).

22. Our directive does not suggest, as the Trade Associations contend, a new mandate above and beyond FPA section 215. The Commission's directive to NERC to address supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations is not intended to "define 'energy security' as a new policy mandate" under the CIP Reliability Standards.[27] Instead, our directive is meant to enhance bulk electric system cybersecurity by addressing the gap in the CIP Reliability Standards identified in the NOPR relating to supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system

[26] NOPR, 152 FERC ¶ 61,054 at P 66.

[27] *See* Trade Associations NOPR Comments at 24.

operations. This directive is squarely within the statutory definition of a "reliability standard," which includes requirements for "cybersecurity protection." [28]

23. We reject Southern's argument that FPA section 215 limits the scope of the NERC Reliability Standards to "ensur[ing] that a given BES Cyber System asset is protected from vulnerabilities once connected" to the bulk electric system.[29] While Southern's comment implies that the Commission should only be concerned with real-time operations based on the definition of the term "reliable operation," the definition of "reliability standard" in FPA section 215 also includes requirements for "the design of planned additions or modifications" to bulk electric system facilities "necessary to provide for reliable operation of the bulk-power system."[30] Moreover, as noted, FPA section 215 is clear that maintaining reliable operation also includes protecting the bulk electric system from cybersecurity incidents.[31] Indeed, our findings and directives in the Final Rule are intended to better protect the Bulk-Power System from potential cybersecurity incidents that could adversely affect reliable operation of the Bulk-Power System. Accordingly, we would not be carrying out our obligations under FPA section

[28] *See* 16 U.S.C. 824o(a)(3) (defining "reliability standard" to mean "a requirement, approved by the Commission under [section 215 of the FPA] to provide for the reliable operation of the bulk-power system. The term includes requirements for the operation of existing bulk-power system facilities, *including cybersecurity protection*, and *the design of planned additions or modifications to such facilities* to the extent necessary to provide for reliable operation…") (emphasis added).

[29] *See* Southern NOPR Comments at 16.

[30] *See* 16 U.S.C. 824o(a)(4) (defining "reliable operation"); *see also* 16 U.S.C. 824o(a)(3).

[31] *See* 16 U.S.C. 824o(a)(4).

215 if the Commission determined that cybersecurity incidents resulting from gaps in supply chain risk management were outside the scope of FPA section 215.

24. With regard to concerns that the NOPR's use of the term "industrial control system" signals the Commission's intent to address issues beyond the CIP Reliability Standards or cybersecurity controls, we clarify that our directive is only intended to address the protection of hardware, software, and computing and networking services associated with bulk electric system operations from supply chain-related cybersecurity threats and vulnerabilities.

B. Need for a New or Modified Reliability Standard

1. Cyber Risks Posed by the Supply Chain

NOPR

25. In the NOPR, the Commission observed that the global supply chain, while providing an opportunity for significant benefits to customers, enables opportunities for adversaries to directly or indirectly affect the operations of companies that may result in risks to the end user. The NOPR identified supply chain risks including the insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software, as well as poor manufacturing and development practices. The NOPR pointed to changes in the bulk electric system cyber threat landscape, evidenced by recent malware campaigns targeting supply chain vendors, which highlighted a gap in the protections under the current CIP Reliability Standards.[32]

26. Specifically, the NOPR identified two focused malware campaigns identified by the Department of Homeland Security's Industry Control System - Computer Emergency Readiness Team (ICS-CERT) in 2014.[33] The NOPR stated that this new type of malware campaign is based on the injection of malware while a product or service remains in the control of the hardware or software vendor, prior to delivery to the customer.[34]

[32] NOPR, 152 FERC ¶ 61,054 at PP 61-62.

[33] *Id.* P 63 (citing ICS-CERT, *Alert: ICS Focused Malware (Update A)*, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A; ICS-CERT, *Alert Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)*, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B). ICS-CERT is a division of the Department of Homeland Security that works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community.

[34] NOPR, 152 FERC ¶ 61,054 at P 63.

Comments

27. NERC acknowledges the NOPR's concerns regarding the threats posed by supply chain management risks to the Bulk-Power System. NERC states that "the supply chains for information and communications technology and industrial control systems present significant risks to [Bulk-Power System] security, providing various opportunities for adversaries to initiate cyberattacks."[35] NERC further explains that "supply chains risks are … complex, multidimensional, and constantly evolving, and may include, as the Commission states, insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices."[36] NERC states, however, that as to these supply chains, there are "significant challenges to developing a mandatory Reliability Standard consistent with [FPA] Section 215…."[37]

28. IRC, Peak, Idaho Power, CyberArk, NEMA, Resilient Societies and other commenters share the NOPR's concern that supply chain risks pose a threat to bulk electric system reliability. IRC states that it supports the Commission's efforts to address the risks associated with supply chain management.[38] Peak explains that "the security risk of supply chain management is a real threat, and … a CIP standard for supply chain management may be necessary."[39] Peak notes, for example, that it is possible for a

[35] NERC NOPR Comments at 8.

[36] *Id.* at 10.

[37] *Id.* at 2.

[38] IRC NOPR Comments at 1-2.

[39] Peak NOPR Comments at 3.

malware campaign to infect industrial control software with malicious code while the product or service is in the control of the hardware and software vendor, and states that, "[w]ithout proper controls, the vendor may deliver this infected product or service, unknowingly passing the risk onto the utility industry customer."[40] Isologic and Resilient Societies comments that supply chain vulnerabilities are one of the most difficult areas of cybersecurity because, among other concerns, entities "are seldom aware of the risks [supply chain vulnerabilities] pose."[41]

29. Idaho Power agrees "that the supply chain could pose an attack vector for certain risks to the bulk electric system."[42] CyberArk states that "infection of vendor web sites is just one of the potential ways a supply chain management attack could be executed" and notes that network communications links between a vendor and its customer could be used as well.[43] NEMA agrees with the NOPR that "keeping the electric sector supply chain free from malware and other cybersecurity risks is essential."[44] NEMA highlights a number of principles it represents as vendor best practices, and encourages the Commission and NERC to reference those principles as the effort to address supply chain risks progresses.[45]

---

[40] *Id.* at 3.

[41] Isologic and Resilient Societies Joint NOPR Comments at 9.

[42] Idaho Power NOPR Comments at 3.

[43] CyberArk NOPR Comments at 4.

[44] NEMA NOPR Comments at 1.

[45] *Id.* at 2.

30. Other commenters do not agree that the risks identified in the NOPR support the Commission's NOPR proposal. The Trade Associations, Southern, and NIPSCO contend that the two malware campaigns identified by ICS-CERT and cited in the NOPR do not actually represent a changed threat landscape that defines a reliability gap. Specifically, the Trade Associations state that the two identified malware campaigns "seek to inject malware, while a product is in the control of and in use by the customer and not, as the NOPR suggests, the vendor."[46] In support of this position, the Trade Associations note that the ICS-CERT mitigation measures for the two alerts "focused on the customer and do not address security controls, while the products are under control of the vendors."[47]

31. The Trade Associations and Southern also contend that there is no information from various NERC programs and activities that leads to a reasonable conclusion that supply chain management issues have caused events or disturbances on the bulk electric system.[48] Luminant states that it "does not perceive the same reliability gap that is expressed in the NOPR concerning risks associated with supply chain management" and contends that it is important to understand the potential risks and cost impacts related to any potential mitigation efforts before developing any additional security controls.[49] KCP&L states that it does not share the Commission's view of the supply chain-related

[46] Trade Associations NOPR Comments at 20-21.

[47] Trade Associations NOPR Comments at 21; *see also* NIPSCO NOPR Comments at 6.

[48] Trade Associations NOPR Comments at 21; Southern Comments at 11.

[49] Luminant NOPR Comments at 4.

reliability gap described in the NOPR and, therefore, does not support the Commission's proposal.[50]

Discussion

32. We find ample support in the record to conclude that supply chain management risks pose a threat to bulk electric system reliability. As NERC commented, "the supply chains for information and communications technology and industrial control systems present significant risks to [Bulk-Power System] security, providing various opportunities for adversaries to initiate cyberattacks."[51] The malware campaigns analyzed by ICS-CERT and identified in the NOPR are only examples of such risks (i.e., supply chain

[50] KCP&L NOPR Comments at 7.

[51] NERC NOPR Comments at 8.

attacks targeting supply chain vendors). Commenters identified additional supply chain-related threats,[52] including events targeting electric utility vendors.[53]

33. Even among the comments opposed to the NOPR, there is acknowledgment that supply chain reliability risks exist. The Trade Associations state that their "respective members have identified security issues associated with potential supply chain disruption or compromise as being a significant threat."[54] Recognizing that such risks exist, we reject the assertion by the Trade Associations and Southern that there is an inadequate basis for the Commission to take action because "[t]he Trade Associations can find

[52] Commenters reference tools and information security frameworks, such as ES-C2M2, NIST-SP-800-161 and NIST-SP-800-53, which describe the scope of supply chain risk that could impact bulk electric system operations. *See* Department of Energy, Electricity Subsector Cybersecurity Capability Maturity Model (February 2014), http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf; NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* at 51, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf; NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. These risks include the insertion of counterfeits, unauthorized production and modification of products, tampering, theft, intentional insertion of tracking software, as well as poor manufacturing and development practices. One technical conference participant noted that supply chain attacks can target either (1) the hardware/software components of a system (thereby creating vulnerabilities that can be exploited by a remote attacker) or (2) a third party service provider who has access to sensitive IT infrastructure or holds/maintains sensitive data. *See* Olcott Technical Conference Comments at 1.

[53] Olcott discusses two events targeting electric utility vendors and service providers. Olcott Technical Conference Comments at 2. Specific recent examples of attacks on third party vendors include: (1) unauthorized code found in Juniper Firewalls in 2015; (2) the 2013 Target incident involving stolen vendor credentials; (3) the 2015 Office of Personnel Management incident also involving stolen vendor credentials; and (4) two events targeting electric utility vendors. *See id.* at 1-4.

[54] Trade Associations NOPR Comments at 17.

nothing within various NERC programs and activities that lead to a reasonable conclusion that supply chain management issues have caused events or disturbances on the bulk power system."[55]

34. We disagree with the Trade Associations' arguments suggesting that the two malware campaigns identified in the NOPR do not represent a change in the threat landscape to the bulk electric system. First, while the Trade Associations are correct that the ICS-CERT alerts referenced in the NOPR describe remediation steps for customers to take in the event of a breach, the vulnerabilities exploited by those campaigns were the direct result of vendor decisions about: (1) how to deliver software patches to their customers and (2) the necessary degree of remote access functionality for their information and communications technology products.[56] Second, the malware campaigns also demonstrate that attackers have expanded their efforts to include the execution of broad access campaigns targeting vendors and software applications, rather than just individual entities. The targeting of vendors and software applications with potentially broad access to BES Cyber Systems[57] marks a turning point in that it is no longer

[55] *See* Trade Associations NOPR Comments at 21.

[56] The ICS-CERT alert regarding ICS Focused Malware indicated that "the software installers for … vendors were infected with malware known as the Havex Trojan."

[57] Cyber systems are referred to as "BES Cyber Systems" in the CIP Reliability Standards. The NERC Glossary defines BES Cyber Systems as "One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." NERC Glossary of Terms Used in Reliability Standards (May 17, 2016) at 15 (NERC Glossary). The NERC Glossary defines "BES Cyber Asset" as "A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or

sufficient to focus protection strategies exclusively on post-acquisition activities at individual entities. Instead, we believe that attention should also be focused on minimizing the attack surfaces of information and communications technology products procured to support bulk electric system operations.

2. Objectives of a Supply Chain Management Reliability Standard

NOPR

35. The NOPR stated that the reliability goal of a supply chain risk management Reliability Standard should be a forward-looking, objective-driven Reliability Standard that encompasses activities in the system development life cycle: from research and development, design and manufacturing stages (where applicable), to acquisition, delivery, integration, operations, retirement, and eventual disposal of the responsible entity's information and communications technology and industrial control system supply chain equipment and services. The NOPR explained that the Reliability Standard should support and ensure security, integrity, quality, and resilience of the supply chain and the future acquisition of products and services.[58]

36. The NOPR recognized that, due to the breadth of the topic and the individualized nature of many aspects of supply chain management, a Reliability Standard pertaining to supply chain management security should:

---

otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems." *Id.*

[58] NOPR, 152 FERC ¶ 61,054 at P 64.

- Respect FPA section 215 jurisdiction by only addressing the obligations of responsible entities. A Reliability Standard should not directly impose obligations on suppliers, vendors or other entities that provide products or services to responsible entities.
- Be forward-looking in the sense that the Reliability Standard should not dictate the abrogation or re-negotiation of currently-effective contracts with vendors, suppliers or other entities.
- Recognize the individualized nature of many aspects of supply chain management by setting goals (the "what"), while allowing flexibility in how a responsible entity subject to the Reliability Standard achieves that goal (the "how").
- Given the types of specialty products involved and the diversity of acquisition processes, the Reliability Standard may need to allow exceptions (e.g., to meet safety requirements and fill operational gaps if no secure products are available).
- Provide enough specificity so that compliance obligations are clear and enforceable. In particular, the Commission anticipated that a Reliability Standard that simply requires a responsible entity to "have a plan" addressing supply chain management would not suffice. Rather, to adequately address the concerns identified in the NOPR, the Commission stated a Reliability Standard should identify specific controls.[59]

37. The NOPR recognized that, because security controls for supply chain management likely vary greatly with each responsible entity due to variations in

[59] *Id.* P 66.

individual business practices, the right set of supply chain management security controls should accommodate, *inter alia*, an entity's: (1) procurement process; (2) vendor relations; (3) system requirements; (4) information technology implementation; and (5) privileged commercial or financial information. As examples of controls that may be instructional in the development of any new Reliability Standard, the NOPR identified the following Supply Chain Risk Management controls from NIST SP 800-161: (1) Access Control Policy and Procedures; (2) Security Assessment Authorization; (3) Configuration Management; (4) Identification and Authentication; (5) System Maintenance Policy and Procedures; (6) Personnel Security Policy and Procedures; (7) System and Services Acquisition; (8) Supply Chain Protection; and (9) Component Authenticity.[60]

[60] NOPR, 152 FERC ¶ 61,054 at P 65 (citing NIST Special Publication 800-161 at 51).

Comments

38. NERC states that a Commission directive requiring the development of a supply chain risk management Reliability Standard: (1) should provide a minimum of two years for Reliability Standard development activities; (2) should clarify that any such Reliability Standard build on existing protections in the CIP Reliability Standards and the practices of responsible entities, and focus primarily on those procedural controls that responsible entities can reasonably be expected to implement during the procurement of products and services associated with bulk electric system operations to manage supply chain risks; and (3) must be flexible to account for differences in the needs and characteristics of responsible entities, the diversity of bulk electric system environments, technologies, risks, and issues related to the limited applicability of mandatory NERC Reliability Standards.[61]

[61] NERC NOPR Comments at 8-9.

39. While sharing the Commission's concern that supply chain risks pose a threat to bulk electric system reliability, some commenters suggest that the Commission address certain threshold issues before moving forward with the NOPR proposal. IRC notes its concern that the NOPR proposal is overly broad, which IRC states could hamper industry's ability to address the Commission's concerns.[62] Idaho Power expresses a concern "that tightening purchasing controls too tightly could also pose a risk because there are limited vendors" available to industry.[63] Idaho Power states that any supply chain Reliability Standard "should be laid out in terms of requirements built around controls that are developed by the regulated entity rather than prescriptive requirements like many other CIP standards."[64] ISO-NE supports the development of procedural controls "such as requirements that Registered Entities must transact with organizations that meet certain criteria, use specified procurement language in contracts, and review and validate vendors' security practices."[65] Peak notes that "the number of vendors for certain hardware, software and services may be limited" and, therefore, a supply chain-related Reliability Standard should grant responsible entities the flexibility "to show preference for, but not the obligation to use, vendors who demonstrate sound supply chain security practices."[66]

---

[62] IRC NOPR Comments at 2.

[63] Idaho Power NOPR Comments at 3.

[64] *Id.* at 3-4.

[65] ISO-NE NOPR Comments at 2 (citing NERC NOPR Comments at 17-18).

[66] Peak NOPR Comments at 4.

40. NERC, the Trade Associations, Southern, Gridwise, and other commenters request that, should the Commission find it reasonable to direct NERC to develop a new or modified Reliability Standard for supply chain management, the Commission adopt certain principles for NERC to follow in the standards development process. As an initial matter, NERC and other commenters state that the Commission should identify the risks that it intends NERC to address.[67] In addition, NERC, SPP RE, and AEP state that the Commission should ensure that any new or modified supply chain-related Reliability Standard carefully considers the risk being addressed against the cost of mitigating that risk.[68]

41. NERC states that the focus of any supply chain risk management Reliability Standard "should be a set of requirements outlining those procedural controls that entities should take, as purchasers of products and services, to design more secure products and modify the security practices of suppliers, vendors, and other parties throughout the supply chain."[69] Similarly, SPP RE notes that, while one responsible entity alone may not have adequate leverage to make a vendor or supplier adopt adequate security practices, "the collective application of the procurement language across a broad collection of Responsible Entities may achieve the intended improvement in security

---

[67] NERC NOPR Comments at 9-11; Trade Associations NOPR Comments at 26; Gridwise NOPR Comments at 5; AEP NOPR Comments at 8; SPP RE NOPR Comments at 11; EnergySec NOPR Comments at 4.

[68] NERC NOPR Comments at 11-12; SPP RE NOPR Comments at 11; AEP NOPR Comments at 9.

[69] NERC NOPR Comments at 17.

safeguards."[70] Isologic and Resilient Societies recommends limiting the Reliability Standard requirements to a few that are immediately necessary, such as: (1) preventing the installation of cyber related system or grid components which have been reported by ICS-CERT to be provably vulnerable to a supply chain attack, unless the vulnerability has been corrected; (2) removing from operation any system or component reported by ICS-CERT as containing an exploitable vulnerability; and (3) subjecting hardware and software to penetration testing prior to installation on the grid.[71]

42. In post-technical conference comments, while still opposing the NOPR proposal, APPA suggests certain parameters that should govern the development of any supply chain-related Reliability Standard.[72] Specifically, APPA states that a supply chain-related Reliability Standard should be risk-based and "must embody an approach that enables utilities to perform a risk assessment of the hardware and systems that create potential vulnerabilities," similar to the approach taken in Reliability Standard CIP-014-2, Requirement R1 (Physical Security).[73] In addition, APPA states that a supply chain-related Reliability Standard should not require responsible entities to actively manage third-party vendors or their processes since that would risk involving utilities in areas that are outside of their core expertise. APPA also argues that "it would be unreasonable for any standard that FERC directs to hold utilities liable for the actions of third-party

[70] SPP RE NOPR Comments at 12.

[71] Isologic and Resilient Societies Joint NOPR Comments at 11.

[72] APPA's post-technical conference comments were submitted jointly with LPPC and TAPS.

[73] APPA Post-Technical Conference Comments at 3-4.

vendors or suppliers."[74] Finally, APPA states that responsible entities should be able to rely on a credible attestation by a vendor or supplier that it complied with identified supply chain security process. APPA contends that this would be the most efficient way to "establish a standard of care on the suppliers' part."[75]

Discussion

43. We direct that NERC, pursuant to section 215(d)(5) of the FPA, develop a forward-looking, objective-driven new or modified Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. Our directive is consistent with the NOPR comments advocating flexibility as to what form the Commission's directive should take.

44. We agree with NERC and other commenters that a supply chain risk management Reliability Standard should be flexible and fall within the scope of what is possible using Reliability Standards under FPA section 215. The directive discussed below, we believe, is consistent with both points. In particular, the flexibility inherent in our directive should account for, among other things, differences in the needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies and risks. For example, the new or modified Reliability Standard may allow a responsible entity to meet the security objectives discussed below

[74] *Id.* at 4-5.

[75] *Id.* at 5.

by having a plan to apply different controls based on the criticality of different assets. And by directing NERC to develop a new or modified Reliability Standard, the Commission affords NERC the option of modifying existing Reliability Standards to satisfy our directive. Finally, we direct NERC to submit the new or modified Reliability Standard within one year of the effective date of this Final Rule.[76]

45. The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. Responsible entities should be required to achieve these four objectives but have the flexibility as to how to reach the objective (i.e., the Reliability Standard should set goals (the "what"), while allowing flexibility in how a responsible entity subject to the Reliability Standard achieves that goal (the "how")).[77] Alternatively, NERC can propose an equally effective and efficient approach to address the issues raised in the objectives identified below. In addition, while in the discussion below we identify four objectives, NERC may address additional supply chain management objectives in the standards development process, as it deems appropriate.

[76] We note that the Trade Associations request that the Commission allow "at least one year for discussion, development, and approval by the NERC Board of Trustees." *See* Trade Associations Post-Technical Conference Comments at 22. NERC should submit an informational filing within ninety days of the effective date of this Final Rule with a plan to address the Commission's directive.

[77] *See* Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 260.

46. The new or modified Reliability Standard should also require a periodic reassessment of the utility's selected controls. Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1, the Reliability Standard should require the responsible entity's CIP Senior Manager to review and approve the controls adopted to meet the specific security objectives identified in the Reliability Standard at least every 15 months. This periodic assessment should better ensure that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities.

47. Also, consistent with this reliance on an objectives-based approach, and as part of this periodic review and approval, the responsible entity's CIP Senior Manager should consider any guidance issued by NERC, the U.S. Department of Homeland Security (DHS) or other relevant authorities for the planning, procurement, and operation of industrial control systems and supporting information systems equipment since the prior approval, and identify any changes made to address the recent guidance. This periodic reconsideration will help ensure an ongoing, affirmative process for reviewing and, when appropriate, incorporating such guidance.

First Objective: Software Integrity and Authenticity

48. The new or modified Reliability Standard must address verification of: (1) the identity of the software publisher for all software and patches that are intended for use on BES Cyber Systems; and (2) the integrity of the software and patches before they are installed in the BES Cyber System environment.

49. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. One of the two focused malware campaigns identified by ICS-CERT in 2014 utilized similar tactics, executing what is commonly referred to as a "Watering Hole" attack[78] to exploit affected information systems. Similar tactics appear to have been used in a recently disclosed attack targeting electric sector infrastructure in Japan.[79] These types of attacks might have been prevented had the affected entities applied adequate integrity and authenticity controls to their patch management processes.

50. As NERC recognizes in its NOPR comments, NIST SP-800-161 "establish[es] instructional reference points for NERC and its stakeholders to leverage in evaluating the appropriate framework for and security controls to include in any mandatory supply chain management Reliability Standard."[80] NIST SP-800-161 includes a number of security controls which, when taken together, reduce the probability of a successful Watering Hole or similar cyberattack in the industrial control system environment and thus could

[78] "Watering Hole" attacks exploit poor vendor/client patching and updating processes. Attackers generally compromise a vendor of the intended victim and then use the vendor's information system as a jumping off point for their attack. Attackers will often inject malware or replace legitimate files with corrupted files (usually a patch or update) on the vendor's website as part of the attack. The victim then downloads the files without verifying each file's legitimacy believing that it is included in a legitimate patch or update.

[79] *See* Cylance, Operation DustStorm, https://www.cylance.com/hubfs/2015_cylance_website/assets/operation-dust-storm/Op_Dust_Storm_Report.pdf.

[80] NERC NOPR Comments at 16-17; *see also* Resilient Societies NOPR Comments at 11.

assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and components should be tested and verified using controls such as digital signatures and obtaining software directly from the developer. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without verification that the component has been digitally signed to ensure that hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing the Commission's directive regarding this first objective. Other security controls also could meet this objective.

Second Objective: Vendor Remote Access to BES Cyber Systems

51. The new or modified Reliability Standard must address responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions. This objective covers both user-initiated and machine-to-machine vendor remote access.

52. This objective addresses the threat that vendor credentials could be stolen and used to access a BES Cyber System without the responsible entity's knowledge, as well as the threat that a compromise at a trusted vendor could traverse over an unmonitored connection into a responsible entity's BES Cyber System. The theft of legitimate user credentials appears to have been a critical aspect to the successful execution of the 2015 cyberattack on Ukraine's power grid.[81] In addition, controls adopted under this objective

[81] *See* E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid* at 3 (Mar. 18, 2016), http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

should give responsible entities the ability to rapidly disable remote access sessions in the event of a system breach.

53. DHS noted the importance of controlling vendor remote access in its alert on the Ukrainian cyberattack: "Remote persistent vendor connections should not be allowed into the control network. Remote access should be operator controlled, time limited, and procedurally similar to "lock out, tag out." The same remote access paths for vendor and employee connections can be used; however, double standards should not be allowed."[82]

54. NIST SP-800-53 and NIST SP-800-161 provide several security controls which, when taken together, reduce the probability that an attacker could use legitimate third-party access to compromise responsible entity information systems. In the Systems and Communications (SC) control family, for example, control SC-7 addressing boundary protection requires that an entity implement appropriate monitoring and control mechanisms and processes at the boundary between the entity and its suppliers, and that provisions for boundary protections should be incorporated into agreements with suppliers. These protections are applied regardless of whether the remote access session is user-initiated or interactive in nature.

55. In the Access Control (AC) control family, control AC-17 requires usage restrictions, configuration/connection requirements, and monitoring and control for remote access sessions, including the entity's ability to expeditiously disconnect or disable remote access. In the Identification and Authentication (IA) control family,

[82] *See* ICS-CERT Alert, *Cyber-Attack Against Ukrainian Critical Infrastructure*, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

control IA-5 requires changing default "authenticators" (e.g., passwords) prior to information system installation. In the System and Information Integrity (SI) control family, control SI-4 addresses monitoring of vulnerabilities resulting from past information and communication technology supply chain compromises, such as malicious code implanted during software development and set to activate after deployment. These sources, while not meant to be definitive, provide examples of controls for addressing the Commission's directive regarding objective two. Other security controls also could meet this objective.

Third Objective: Information System Planning and Procurement

56. The new or modified Reliability Standard must address how a responsible entity will include security considerations as part of its information system planning and system development lifecycle processes. As part of this objective, the new or modified Reliability Standard must address a responsible entity's CIP Senior Manager's (or delegate's) identification and documentation of the risks of proposed information system planning and system development actions. This objective is intended to ensure adequate consideration of these risks, as well as the available options for hardening the responsible entity's information system and minimizing the attack surface.

57. This third objective addresses the risk that responsible entities could unintentionally plan to procure and install unsecure equipment or software within their information systems, or could unintentionally fail to anticipate security issues that may arise due to their network architecture or during technology and vendor transitions. For example, the BlackEnergy malware campaign identified by ICS-CERT and referenced in

the NOPR resulted from the remote exploitation of previously unidentified vulnerabilities, which allowed attackers to remotely execute malicious code on remotely accessible devices.[83] According to ICS-CERT, this attack might have been mitigated if affected entities had taken steps during system development and planning to: (1) minimize network exposure for all control system devices/subsystems; (2) ensure that devices were not accessible from the internet; (3) place devices behind firewalls; and (4) utilize secure remote access techniques.[84] The third objective also supports, where appropriate, the need for strategic technology refreshes as recommended by ICS-CERT in response to the 2015 Ukraine cybersecurity incident.[85]

58. NIST SP 800-53 and SP 800-161 provide several controls which, when taken together, reduce the likelihood that an information system will be deployed and/or remain in service with potential vulnerabilities that have not been identified or adequately considered. For example, in the NIST SP 800-53 Systems Acquisition (SA) control family, control SA-3 provides that organizations should: (1) manage information systems using an organizationally-defined system development life cycle that incorporates information security considerations; and (2) integrate the organizational information security risk management process into system development life cycle activities.[86]

---

[83] *See* ICS-CERT Alert, *Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)*.

[84] *See* ICS-CERT Advisory, *GE Proficy Vulnerabilities*, https://ics-cert.us-cert.gov/advisories/ICSA-14-023-01.

[85] *See* ICS-CERT Alert, *Cyber-Attack Against Ukrainian Critical Infrastructure*.

[86] NIST Special Publication 800-53, Appendix F (Security Control Catalog) at 157.

Similarly, control SA-8 recommends using secure engineering principles during the planning and acquisition phases of future projects such as: (1) developing layered protections; (2) establishing sound security policy, architecture, and controls as the foundation for design; (3) incorporating security requirements into the system development life cycle; and (4) reducing risk to acceptable levels, thus enabling informed risk management decisions.[87] Finally, control SA-22 provides controls to address unsupported system components, recommending the replacement of information and communication technology components when support is no longer available, or the justification and approval of an unsupported system component to meet specific business needs. These sources, while not meant to be definitive, provide examples of controls for addressing the Commission's directive regarding objective three. Other security controls also could meet this objective.

Fourth Objective: Vendor Risk Management and Procurement Controls

59. The new or modified Reliability Standard must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. Specifically, NERC must address controls for the following topics: (1) vendor security event notification processes; (2) vendor personnel termination notification for employees with access to remote and onsite systems; (3) product/services vulnerability disclosures, such as accounts that are able to bypass authentication or the presence of hardcoded passwords; (4) coordinated incident response activities; and (5)

[87] *Id.* at 162.

other related aspects of procurement. NERC should also consider provisions to help responsible entities obtain necessary information from their vendors to minimize potential disruptions from vendor-related security events.

60. This fourth objective addresses the risk that responsible entities could enter into contracts with vendors who pose significant risks to their information systems, as well as the risk that products procured by a responsible entity fail to meet minimum security criteria. In addition, this objective addresses the risk that a compromised vendor would not provide adequate notice and related incident response to responsible entities with whom that vendor is connected.

61. The Department of Energy (DOE) Cybersecurity Procurement Language for Energy Delivery Systems document outlines security principles and controls for entities to consider when designing and procuring control system products and services (e.g., software, systems, maintenance, and networks), and provides example language that could be incorporated into procurement specifications. The procurement language encourages buyers to incorporate baseline procurement language that ensures the supplier establishes, documents and implements risk management practices for supply chain delivery of hardware, software, and firmware.[88] In addition, NIST SP 800-161 encourages buyers to use the Information and Communications Technology supply chain risk management (ICT SCRM) plans for their respective systems and missions

[88] *See* Energy Sector Control Systems Working Group, *Cybersecurity Procurement Language –Energy Delivery Systems* at 27, http://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf.

throughout their acquisition activities.[89] The controls in the ICT SCRM plans can be applied in different life cycle processes.

62. NIST SP 800-161 also provides specific recommendations in control SA-4 pertaining to systems acquisition processes, which are relevant for consideration during the standards development process, including but not limited to: (1) defining requirements that cover regulatory requirements (i.e., telecommunications or IT), technical requirements, chain of custody, transparency and visibility, sharing information on supply chain security incidents throughout the supply chain, rules for disposal or retention of elements such as components, data, or intellectual property, and other relevant requirements; (2) defining requirements for critical elements in the supply chain to demonstrate a capability to remediate emerging vulnerabilities based on open source information and other sources; and (3) defining requirements for the expected life span of the system and ensuring that suppliers can provide insights into their plans for the end-of-life of components. Other relevant provisions can be found in the System and Communications Protection (SC) control family under control SC-18 addressing SCRM guidance for mobile code, which recommends that organizations employ rigorous supply chain protection techniques in the acquisition, development, and use of mobile code to be

[89] *See* NIST Special Publication 800-161 at 51.

deployed in information systems.[90] These sources, while not meant to be definitive, provide examples of controls for addressing the Commission's directive regarding objective four. Other security controls also could meet this objective.

3. Existing CIP Reliability Standards

Comments

63. NERC comments that although the CIP Reliability Standards do not explicitly address supply chain procurement practices, existing requirements mitigate the supply chain risks identified in the NOPR. In particular, NERC states that requirements in Reliability Standards CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, and CIP-011-2 "include controls that correspond to controls in NIST SP 800-161."[91]

64. For example, NERC explains that responsible entity compliance with Reliability Standard CIP-004-6, addressing the implementation of cybersecurity awareness programs, may include reinforcement of cybersecurity practices to mitigate supply chain risks. NERC also states that requirements in Reliability Standard CIP-004-6 (addressing personnel risk assessment) and requirements in Reliability Standards CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, and CIP-010-2 (addressing electronic and physical access) apply to any outside vendors or contractors.

[90] Mobile code is a software program or parts of a program obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. NIST Special Publication 800-53, Appendix B (Glossary) at 14. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. *Id*.

[91] NERC NOPR Comments at 15-16.

65. The Trade Associations, Arkansas, G&T Cooperatives, NIPSCO, Luminant, Southern, NextEra, and SCE contend that the existing CIP Reliability Standards, at least partly, address supply chain risks that are within a responsible entity's control.

66. The Trade Associations state that, while the existing CIP Reliability Standards do not contain explicit provisions addressing supply chain management, "transmission owners and operators already have significant responsibilities to perform under various Commission-approved CIP standards that already address supply chain issues."[92] Specifically, the Trade Associations, NIPSCO, and others state that Reliability Standard CIP-010-2 establishes requirements for cyber asset change management that mandate extensive baseline configuration testing and change monitoring, as well as vulnerability assessments, prior to connecting a new cyber asset to a High Impact BES Cyber Asset.[93]

67. The Trade Associations also contend that the CIP Reliability Standards provide adequate vendor remote access protections by mandating: (1) controls that restrict personnel access (physical and electronic) to protected information systems; (2) controls that prevent direct access to applicable systems for interactive remote access sessions using routable protocols; (3) the use of encryption for connections extending outside of an electronic security perimeter; (4) the use of two factor authentication when accessing

[92] Trade Associations NOPR Comments at 19-20.

[93] Trade Associations NOPR Comments at 20; NIPSCO NOPR Comments at 5; Southern NOPR Comments at 12; Luminant NOPR Comments at 4-5; SCE NOPR Comments at 6.

medium and high impact systems; and (5) integration controls which require changing known default accounts and passwords.[94]

68. NIPSCO, Luminant, and G&T Cooperatives point to Reliability Standard CIP-007-6 as an existing Reliability Standard that addresses supply chain risks. Reliability Standard CIP-007-6 requires responsible entities to have processes under which only necessary ports and services should be enabled; security patches should be tracked, evaluated, and installed on applicable BES Cyber Systems; and anti-virus software or other prevention tools should be used to prevent the introduction and propagation of malicious software on all Cyber Assets within an Electronic Security Perimeter.[95]

69. Commenters also identify existing voluntary guidelines that, they contend, augment the existing CIP Reliability Standards to further address any potential risks posed by the supply chain. Southern points to voluntary cybersecurity procurement guidance materials developed by the DHS and the DOE as examples of procurement language that could be used in the course of vendor negotiations. Southern states that the DHS and DOE guidelines recognize the need for flexibility and allow for multiple contractual approaches.[96]

70. Commenters suggest that the Commission direct NERC to develop cybersecurity procurement guidance documents as opposed to a mandatory Reliability Standard. AEP, NextEra, and Southern state that the Commission could direct NERC to

[94] Trade Associations Post-Technical Conference Comments at 6.

[95] NIPSCO NOPR Comments at 5; Luminant NOPR Comments at 4; G&T Cooperatives NOPR Comments at 8-9.

[96] Southern NOPR Comments at 13.

develop guidance documents addressing supply chain risk management based, in part, on the DHS and DOE voluntary cybersecurity procurement guidance materials.[97] Luminant asserts that NERC-developed guidance "would effectively communicate key issues while permitting industry the flexibility to effectively protect their BES Cyber Systems in a way most effective for that entity and at the lowest cost."[98]

Discussion

71. While we recognize that existing CIP Reliability Standards include requirements that address aspects of supply chain management, we determine that existing Reliability Standards do not adequately protect against supply chain risks that are within a responsible entity's control. Specifically, we find that existing CIP Reliability Standards do not provide adequate protection for the four aspects of supply chain risk management that underlie the four objectives for a new or modified Reliability Standard discussed above.[99] Moreover, a fundamental premise of cyber security is "defense in depth," and addressing issues in the supply chain (to the extent a utility reasonably can) is an important component of a strong, multi-layered defense.

Software Integrity and Authenticity

72. With regard to software integrity and authenticity, we agree with commenters who state that the existing CIP Reliability Standards contain requirements for responsible

[97] AEP NOPR Comments at 7-8; NextEra NOPR Comments at 4-5; Southern NOPR Comments at 12-13.

[98] Luminant NOPR Comments at 5.

[99] Since the directive to NERC to develop a new or modified Reliability Standard is limited to the four objectives discussed above, we limit our analysis of the existing CIP Reliability Standards to requirements that relate to those objectives.

entities to implement a patch management process for tracking, evaluating, and installing cybersecurity patches and to implement processes to detect, prevent, and mitigate the threat of malicious code. These provisions, however, do not require responsible entities to verify the identity of the software publisher for all software and patches that are intended for use on their BES Cyber Systems or to verify the integrity of the software and patches before they are installed in the BES Cyber System environment.[100] As discussed above, the CIP Reliability Standards should address compromised software or patches that a responsible entity receives from a vendor, in order to protect the bulk electric system from Watering-Hole or similar cyberattacks. These concerns are not addressed by existing CIP Reliability Standards.

73. Mandatory controls in the existing CIP Reliability Standards referenced by commenters do not provide sufficient protection against attacks that compromise software and software patch integrity and authenticity. For example, while Reliability Standard CIP-007-6, Requirement R2 requires responsible entities to enforce a patch management process for tracking, evaluating, and installing cyber security patches for applicable systems, including evaluating security patches for applicability, the requirement does not address mechanisms to acquire the patch file from a vendor in a secure manner and methods to validate the integrity of a patch file before installation.

[100] *See* Trade Associations NOPR Comments at 38 (indicating that integrity checking mechanisms used to verify software, firmware, and information integrity found in the NIST SP-800-161 System and Information Integrity (SI) control family are not addressed in the CIP version 5 Reliability Standards).

74. With respect to mandatory configuration controls, Reliability Standard CIP-010-2, Requirement R1 requires responsible entities to authorize and document all changes to baseline configurations and, where technically feasible, test patches in a test environment before installing. However, NERC's technical guidance document for CIP-010-2, Requirement R1, Part 1.2 does not require the authorizer to first verify the authenticity of a patch. Similarly, the testing of patches in a test environment under Requirement R1.5 would likely provide insufficient protection as many malware variants are programmed to execute only after the system is rebooted several times. Regarding patch source monitoring, the guidelines and technical basis section for Reliability Standard CIP-007-6 suggests that responsible entities should obtain security patches from original sources, where possible, and indicates that patches should be approved or certified by another source before being assessed and applied.[101] The Reliability Standard, however, does not require the use of these techniques. Implementing controls that verify integrity and authenticity of software and its publishers may help mitigate security gaps listed above.

75. In sum, the current CIP Reliability Standards do contain certain controls addressing the risks posed by malware, as stated by commenters. Verifying software integrity and authenticity, however, is a reasonable and appropriate complement to these controls, is not required by the current Standards, and is supported by the principle of

[101] Reliability Standard CIP-007-6 (Cyber Security – Systems Security Management), Guidelines and Technical Basis at 42-43.

defense-in-depth. In fact, this verification can be viewed as the first line of defense against malware-infected software.

Vendor Remote Access to BES Cyber Systems

76. On the subject of vendor remote access, which includes vendor user-initiated Interactive Remote Access and vendor machine-to-machine remote access, existing CIP Reliability Standards contain system access requirements, including a requirement for security event monitoring. However, the CIP Reliability Standards do not require remote access session logging for machine-to-machine remote access, nor do they address the ability to monitor or close unsafe remote connections for both vendor Interactive Remote Access and vendor machine-to-machine remote access.[102] The CIP Reliability Standards should address enhanced session logging requirements for vendor remote access in order to improve visibility of activity on BES Cyber Systems and give responsible entities the ability to rapidly disable remote access sessions in the event of a system breach.

77. The existing requirements referenced by NERC, the Trade Associations, and other commenters do not adequately address access restrictions for vendors. For example, while Reliability Standard CIP-004-6, Requirements R4 and R5 provide controls that must be applied to vendors such as restricting access to individuals "based

[102] *See* Trade Association NOPR Comments at 43 (indicating that mechanisms for monitoring for unauthorized personnel, connections, devices, and software found in the NIST SP-800-161 System and Information Integrity (SI) control family are not addressed in the CIP version 5 Reliability Standards).

on need," these Requirements do not include post-authorization logging or control of remote access. The existing CIP Reliability Standards do not require a responsible entity to monitor data traffic that traverses remote communication to their BES Cyber Systems. The absence of post-authorization monitoring and logging presents an opportunity for unmonitored malicious or otherwise inappropriate remote communication to or from a BES Cyber System. The inability of a responsible entity to rapidly terminate a connection may allow malicious or otherwise inappropriate communication to propagate, contributing to a degradation of a BES Cyber Asset's function. Enhanced visibility into remote communications and the ability to rapidly terminate a remote communication could mitigate such a vulnerability.

78. Reliability Standard CIP-005-5, Requirement R1 provides controls for vendor machine-to-machine and vendor user-initiated Interactive Remote Access sessions by restricting all inbound and outbound communications through an identified Electronic Access Point for bi-directional routable protocol connections. Reliability Standard CIP-005-5, Requirement R2 provides controls for vendor interactive remote access sessions by requiring the use of encryption and requiring multi-factor authentication. However, the provisions of Reliability Standard CIP-005-5, Requirement R2 addressing interactive remote access management do not apply to vendor machine-to-machine remote access. The Reliability Standard CIP-005-5, Requirement R2 controls addressing interactive remote access management only apply to remote connections that are user-initiated (i.e., initiated by a person). Machine-to-machine connections are not user-initiated and, therefore, are not subject to the requirements of Reliability Standard CIP-005-5,

Requirement R2. When the interactive remote access management controls of Reliability Standard CIP-005-5, Requirement R2 do not apply, a machine-to-machine remote communication may access a BES Cyber System without any access credentials, over an unencrypted channel, and without going through an Intermediate System.

79. For both Interactive Remote Access and machine-to-machine remote access, Reliability Standard CIP-007-6, Requirement R3 requires monitoring for malicious code and Requirement R4 requires logging of successful and unsuccessful login attempts, as well as logging detected malicious code. However, Reliability Standard CIP-007-6 does not address the risks posed by inappropriate activity that could occur during a remote communication. The lack of a requirement addressing the detection of inappropriate activity represents a risk because the responsible entity may not be aware if an authorized user is performing inappropriate activity on a BES Cyber Asset via a remote connection. This risk is higher for machine-to-machine communication due to the lack of authentication and encryption requirements in the existing CIP Reliability Standards, lowering the threshold for a malicious actor to execute a man-in-the-middle attack to gain access to a BES Cyber System and conduct inappropriate activity such as reconnaissance or code modification.

80. Therefore, we recognize that the current CIP Reliability Standards do contain certain controls addressing the risks posed by vendor remote access, as noted by commenters. However, the current CIP Reliability Standards do not require monitoring remote access sessions or closing unsafe remote connections for either vendor Interactive Remote Access and vendor machine-to-machine remote access. Accordingly, we

determine that vendor remote access is not adequately addressed in the approved CIP Reliability Standards and, therefore, is an objective that must be addressed in the supply chain management plans directed in this final rule.

Information System Planning and Procurement

81. The existing CIP Reliability Standards do not address information system planning. Recent cybersecurity incidents[103] have made it apparent that overall system planning is as important to overall BES Cyber System security and reliability as any other component of security architecture. In general, the CIP Reliability Standards do not provide a framework for maintaining ongoing awareness of information security, vulnerabilities, and threats to support organization risk management decisions;[104] nor do they address the concept of integrating continuous improvement of organizational security posture with supply chain risk management as recommended by NIST SP 800-161.[105] Based on the threats evidenced by recent cybersecurity incidents, the absence of security considerations in system lifecycle processes constitutes a gap in the CIP Reliability Standards that could contribute to pervasive and systemic vulnerabilities that threaten bulk electric system reliability.

[103] *See* E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid* at 3 (March 18, 2016); *see also* Dell, *Dell Security Annual Threat Report* (2015) at 7, https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf; Olcott Technical Conference Comments at 2.

[104] *See* NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* at vi, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf.

[105] NIST Special Publication 800-161 at 46.

82. The existing CIP Reliability Standards also do not provide for procurement controls for industrial control system hardware, software, and computing and networking services. As discussed above, procurement controls are intended to address the threat that responsible entities could enter into contracts with vendors who pose significant risks to their information systems or procure products that fail to meet minimum security criteria, as well as the risk that a compromised vendor would not provide adequate notice and related incident response to responsible entities with whom that vendor is connected.

83. With regard to commenters' suggestion that the Commission direct NERC to develop cybersecurity procurement guidance documents as opposed to a mandatory Reliability Standard, we agree that the voluntary efforts identified by commenters could provide guidance or otherwise inform NERC's standard development process. We conclude, however, that relying on voluntary guidelines to address the supply chain risks described above is not sufficient to fulfill the Commission's responsibilities under FPA section 215.

4. Vendor Risk Management and Procurement Controls

Comments

84. NERC, G&T Cooperatives, Arkansas and others state that responsible entities have limited influence over vendors and contractors, and, therefore, a limited ability to affect the supply chain for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations.[106] NERC contends that any supply chain management Reliability Standard "must balance the reliability need to implement supply chain management security controls with entities' business need to obtain products and services at a reasonable cost."[107] NERC maintains that responsible entities lack bargaining power to persuade vendors or suppliers to implement cybersecurity controls without significantly increasing the cost of their products or services. NERC points to NIST SP 800-161 to highlight that implementing supply chain security management controls "will require financial and human resources, not just from the [acquirer] directly but also potentially from their system integrators, suppliers, and external service providers that would also result in increased cost to the acquirer."[108]

85. G&T Cooperatives contend that they "have minimal control over their suppliers and are not able to identify all potential vulnerabilities associated with each and every

[106] NERC NOPR Comments at 11-12; G&T Cooperatives NOPR Comments at 9; Arkansas NOPR Comments at 5.

[107] NERC NOPR Comments at 11-12.

[108] *Id.* (citing NIST Special Publication 800-161 at 3).

supplier and their products/parts."[109] G&T Cooperatives and Arkansas maintain that responsible entities do not have the ability to force a vendor to address all potential vulnerabilities. G&T Cooperatives assert that even if a contract between a responsible entity and a supplier "could include" language requiring the supplier to implement security controls, "it is not feasible for contractual terms … to address all potential vulnerabilities related to supply chain management."[110]

86. NERC, Trade Associations, G&T Cooperatives and Arkansas also raise a concern that the Commission's proposal could place compliance risk on responsible entities for actions beyond their control and, ultimately, incent responsible entities to avoid upgrades that could trigger such compliance risk.[111] NERC states that any supply chain management Reliability Standard should be drafted so that it "creates affirmative obligations to implement supply chain management security controls without holding entities strictly liable for any failure of those controls to eliminate all supply chain threats and vulnerabilities."[112] NERC explains that if a supply chain management Reliability Standard is not reasonably scoped to avoid unreasonable compliance risk, it could create a disincentive for responsible entities to purchase and install new technologies and equipment.

---

[109] G&T Cooperatives NOPR Comments at 9.

[110] *Id.* at 9.

[111] NERC NOPR Comments at 13; Trade Associations NOPR Comments at 24-25; G&T Cooperatives NOPR Comments at 9-10; Arkansas NOPR Comments at 6.

[112] NERC NOPR Comments at 13.

87. G&T Cooperatives state that "placing the compliance risk of vendor and supplier security vulnerability on Responsible Entities could incent Responsible Entities to avoid upgrades to their industrial control system hardware, software, and other services." G&T Cooperatives explain that there are three primary incentives for a responsible entity to avoid upgrades if faced with compliance risks: (1) new regulations would result in additional costs for vendors and suppliers that would be passed on to the end-user; (2) since security patches are not issued by vendors for unsupported hardware and software, there is less security patch management responsibility for the responsible entity; and (3) avoiding new hardware and software reduces the risk of introducing undetected security threats.[113]

Discussion

88. Our directive to NERC to develop a new or modified Reliability Standard that addresses the objectives outlined above balances the supply chain risks facing the bulk electric system against any potential challenges raised by vendor relationships. We believe that the concerns raised in comments with respect to responsible entities' relationships with vendors in relation to supply chain risks are valid. Our directive is informed by this concern and reflects a reasonable balance between the risks facing bulk electric system reliability from the supply chain and concerns over vendor relationships. The directive strikes this balance by addressing supply chain risks that are within responsible entities' control, and we do not expect a new or modified supply chain Reliability Standard to impose obligations directly on vendors. Moreover, entities will

[113] G&T Cooperatives NOPR Comments at 9.

not be responsible for vendor errors beyond the scope of the controls implemented to comply with the Reliability Standards.

89. With respect to concerns that the Commission's proposal could place compliance risk on responsible entities for actions beyond their control, which some commenters argue would prompt responsible entities to avoid upgrades that could trigger such compliance risk, we reiterate that the intent of the directive is to address supply chain risks that are within the responsible entities' control. As part of NERC's standard development process, we expect NERC to establish provisions addressing compliance obligations in a manner that avoids shifting liability from a vendor for its mistakes to a responsible entity. Finally, we view the argument that a new or modified Reliability Standard will result in a substantial increase in costs to be speculative because, beyond requiring NERC to address the four objectives discussed above, or some equally effective and efficient alternatives, our directive does not require NERC to develop a Reliability Standard that mandates any particular controls or actions.

III. Information Collection Statement

90. The Paperwork Reduction Act (PRA)[1] requires each federal agency to seek and obtain Office of Management and Budget (OMB) approval before undertaking a collection of information directed to ten or more persons or contained in a rule of general applicability. OMB regulations[2] require approval of certain information collection requirements imposed by agency rules. Upon approval of a collection of information,

[1] 44 U.S.C. 3507(d).

[2] 5 CFR 1320.

OMB will assign an OMB control number and an expiration date. Respondents subject to the filing requirements of an agency rule will not be penalized for failing to respond to the collection of information unless the collection of information displays a valid OMB control number.

91. The Commission will submit the information collection requirements to OMB for its review and approval. The Commission solicits public comments on its need for this information, whether the information will have practical utility, the accuracy of burden and cost estimates, ways to enhance the quality, utility, and clarity of the information to be collected or retained, and any suggested methods for minimizing respondents' burden, including the use of automated information techniques.

92. The information collection requirements in this Final Rule in Docket No. RM15-14-002 for NERC to develop a new or to modify a Reliability Standard for supply chain risk management, should be part of FERC-725 (Certification of Electric Reliability Organization; Procedures for Electric Reliability Standards (OMB Control No. 1902-0225)). However, there is an unrelated item which is currently pending OMB review under FERC-725, and only one item per OMB Control No. can be pending OMB review at a time. Therefore, the requirements in this Final Rule in RM15-14-002 are being submitted under a new temporary or interim collection number FERC-725(1A) to ensure timely submittal to OMB. In the long-term, Commission staff plans to administratively move the requirements and associated burden of FERC-725(1A) to FERC-725.

93. Burden Estimate and Information Collection Costs: The requirements for the ERO to develop Reliability Standards and to provide data to the Commission are

included in the existing FERC-725. FERC-725 includes information used by the Commission to implement the statutory provisions of section 215 of the FPA. FERC-725 includes the burden, reporting and recordkeeping requirements associated with: (a) Self-Assessment and ERO Application, (b) Reliability Assessments, (c) Reliability Standards Development, (d) Reliability Compliance, (e) Stakeholder Survey, and (f) Other Reporting. In addition, the Final Rule will not result in a substantive increase in burden because this requirement to develop standards is covered under FERC-725. However because FERC is using the temporary information collection number, FERC-725(1A), FERC will use "placeholder" estimates of 1 response and 1 burden hour for the burden calculation.

IV. Regulatory Flexibility Act Analysis

94. The Regulatory Flexibility Act of 1980 (RFA)[1] generally requires a description and analysis of final rules that will have significant economic impact on a substantial number of small entities. The Small Business Administration (SBA) revised its size standard (effective January 22, 2014) for electric utilities from a standard based on megawatt hours to a standard based on the number of employees, including affiliates.[2] The entities subject to the Reliability Standards developed by the North American Electric Reliability Corporation (NERC) include users, owners, and operators of the Bulk-Power System, which serves more than 334 million people. In addition, NERC's current responsibilities include the development of Reliability Standards. Accordingly,

[1] 5 U.S.C. 601-612.

[2] SBA Final Rule on "Small Business Size Standards: Utilities," 78 FR 77,343 (Dec. 23, 2013).

the Commission certifies that the requirements in this Final Rule will not have a significant economic impact on a substantial number of small entities, and no regulatory flexibility analysis is required.

V. Environmental Analysis

95. The Commission is required to prepare an Environmental Assessment or an Environmental Impact Statement for any action that may have a significant adverse effect on the human environment.[1] The Commission has categorically excluded certain actions from this requirement as not having a significant effect on the human environment. Included in the exclusion are rules that are clarifying, corrective, or procedural or that do not substantially change the effect of the regulations being amended.[2] The actions proposed herein fall within this categorical exclusion in the Commission's regulations.

VI. Effective Date and Congressional Notification

96. This Final Rule is effective **[INSERT DATE 60 days after publication in the FEDERAL REGISTER]**. The Commission has determined, with the concurrence of the Administrator of the Office of Information and Regulatory Affairs of OMB, that this rule is not a "major rule" as defined in section 351 of the Small Business Regulatory Enforcement Fairness Act of 1996. This Final Rule is being submitted to the Senate, House, and Government Accountability Office.

---

[1] *Regulations Implementing the National Environmental Policy Act of 1969*, Order No. 486, FERC Stats. & Regs. ¶ 30,783 (1987).

[2] 18 CFR 380.4(a)(2)(ii).

VII. Document Availability

97. In addition to publishing the full text of this document in the Federal Register, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the Internet through the Commission's Home Page (http://www.ferc.gov) and in the Commission's Public Reference Room during normal business hours (8:30 a.m. to 5:00 p.m. Eastern time) at 888 First Street, NE, Room 2A, Washington, DC 20426.

98. From the Commission's Home Page on the Internet, this information is available on eLibrary. The full text of this document is available on eLibrary in PDF and Microsoft Word format for viewing, printing, and/or downloading. To access this document in eLibrary, type the docket number of this document, excluding the last three digits, in the docket number field.

99. User assistance is available for eLibrary and the Commission's website during normal business hours from the Commission's Online Support at (202) 502-6652 (toll free at 1-866-208-3676) or e-mail at ferconlinesupport@ferc.gov, or the Public Reference

Room at (202) 502-8371, TTY (202) 502-8659. E-mail the Public Reference Room at public.referenceroom@ferc.gov.

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

Note: the following Appendix will not appear in the *Code of Federal Regulations*.

Appendix
Commenters

Abbreviation	Commenter
AEP	American Electric Power Service Corporation
ACS	Applied Control Solutions, LLC
APS	Arizona Public Service Company
Arkansas	Arkansas Electric Cooperative
BPA	Bonneville Power Administration
CEA	Canadian Electricity Association
Consumers Energy	Consumers Energy Company
CyberArk	CyberArk
EnergySec	Energy Sector Security Consortium, Inc.
Ericsson	Ericsson
Resilient Societies	Foundation for Resilient Societies
G&T Cooperatives	Associated Electric Cooperative, Inc., Basin Electric Power Cooperative, and Tri-State Generation and Transmission Association, Inc.
Gridwise	Gridwise Alliance
Idaho Power	Idaho Power Company
Indegy	Indegy
IESO	Independent Electricity System Operator
IRC	ISO/RTO Council
ISO New England	ISO New England Inc.
ITC	ITC Companies
Isologic	Isologic, LLC
KCP&L	Kansas City Power & Light Company and KCP&L Greater Missouri Operations Company
Luminant	Luminant Generation Company, LLC
NEMA	National Electrical Manufacturers Association
NERC	North American Electric Reliability Corporation
NextEra	NextEra Energy, Inc.
NIPSCO	Northern Indiana Public Service Co.
NWPPA	Northwest Public Power Association
Peak	Peak Reliability
PNM	PNM Resources
Reclamation	Department of Interior Bureau of Reclamation
SIA	Security Industry Association
SCE	Southern California Edison Company

Southern	Southern Company Services
SPP RE	Southwest Power Pool Regional Entity
SWP	California Department of Water Resources State Water Project
TVA	Tennessee Valley Authority
Trade Associations	Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Electric Power Supply Association, Transmission Access Policy Study Group, and Large Public Power Council
UTC	Utilities Telecom Council
Waterfall	Waterfall Security Solutions, Ltd.
Wisconsin	Wisconsin Electric Power Company

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Revised Critical Infrastructure Protection Reliability Standards — Docket No. RM15-14-002

(Issued July 21, 2016)

LaFLEUR, Commissioner *dissenting*:

In today's order, the Commission elects to proceed directly to a Final Rule and require the development of a new reliability standard on supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. I fully support the Commission's continued attention to the threat of inadequate supply chain risk management procedures, which pose a very real threat to grid reliability.

However, in my view, the importance and complexity of this issue should guide the Commission to proceed cautiously and thoughtfully in directing the development of a reliability standard to address these threats. I am concerned that the Commission has not adequately considered or vetted the Final Rule, which could hamper the development and implementation of an effective, auditable, and enforceable standard. I believe that the more prudent course of action would be to issue today's Final Rule as a Supplemental Notice of Proposed Rulemaking (Supplemental NOPR), which would provide NERC, industry, and stakeholders the opportunity to comment on the Commission's proposed directives. Accordingly, and as discussed below, I dissent from today's order.[1]

I. The Commission's Decision to Proceed Directly to Final Rule is Flawed and Could Delay Protection of the Grid Against Supply Chain Risks

Last July, as part of its NOPR addressing revisions to its cybersecurity critical infrastructure protection (CIP) standards, the Commission raised for the first time the prospect of directing the development of a standard to address risks posed by lack of controls for supply chain management.[1] The Commission indicated that new threats might warrant directing NERC to develop a standard to address those risks. While the Commission noted a variety of considerations that might shape the standard, including, among others, jurisdictional limits and the individualized nature of companies' supply

[1] I do agree with one holding in the order: that the Commission has authority under section 215 of the Federal Power Act to promulgate a standard on this issue.

[1] *Revised Critical Infrastructure Protection Reliability Standards*, Notice of Proposed Rulemaking, 80 Fed. Reg. 43,354 (July 22, 2015), 152 FERC ¶ 61,054 (2015). I will refer to the section of that order addressing supply chain issues as the "Supply Chain NOPR," and the remainder of the order as the "CIP NOPR."

chain management procedures, the Commission notably did not propose a specific standard for comment. Instead, the Commission sought comment on (1) the general proposal to require a standard, (2) the anticipated features of, and requirements that should be included in, such a standard, and (3) a reasonable timeframe for development of a standard.[2]

The record developed in comments responding to the Supply Chain NOPR and through the January 28, 2016 technical conference reflects a wide diversity of views regarding the need for, and possible content of, a reliability standard addressing supply chain management. Notwithstanding these diverse views, there was broad consensus on one point: that effectively addressing cybersecurity threats in supply chain management is tremendously complicated, due to a host of jurisdictional, technical, economic, and business relationship issues. Indeed, in the Supply Chain NOPR, the Commission recognized "that developing a supply chain management standard would likely be a significant undertaking and require extensive engagement with stakeholders to define the scope, content, and timing of the standard."[3]

Yet, the Commission is proceeding straight to a Final Rule without in my view engaging in sufficient outreach regarding, or adequately vetting, the contents of the Final Rule. As to those contents, it is worth noting that the four objectives that will define the scope and content of the standard were not identified in the Supply Chain NOPR. Therefore, even though the Final Rule reflects feedback received on the Supply Chain NOPR, and is not obviously inconsistent with the Supply Chain NOPR, no party has yet had an opportunity to comment on those objectives or consider how they could be translated into an effective and enforceable standard.[4] This is a consequence of: (1) the lack of outreach on supply chain threats prior to issuing the Supply Chain NOPR; (2) the lack of detail in the Supply Chain NOPR regarding what a standard might look like; and (3) the decision today to proceed straight to a Final Rule rather than provide additional opportunities for public feedback.

A. The Commission and the Public's Consideration of Supply Chain Risks Would Benefit from Additional Stakeholder Engagement

First, I believe that meaningful stakeholder input on the content of any proposed rule is essential to the Commission's deliberative process. This is especially important in our reliability work, as any standard developed by NERC must be approved by stakeholder consensus before it may be filed at the Commission. I do not believe that the

[2] *Id.* P 66.

[3] *Id.*

[4] To be clear, I am less concerned about whether the Final Rule satisfies minimal notice requirements than whether the Final Rule represents reasoned decision making by the Commission.

record developed to date establishes that the Final Rule will lead to an appropriate solution to address supply chain risks. I note that much of the feedback we received in response to the Supply Chain NOPR was not focused on the merits of particular approaches to address supply chain threats. Yet, in this order, the Commission directs the development of a standard based on objectives not reflected in the Supply Chain NOPR, depriving the public of the ability to comment, and the Commission of the benefit of that public comment.

In retrospect, given both the preliminary nature of the consideration of the issue and the lack of a concrete idea regarding what a proposed standard would look like, I believe that the Supply Chain NOPR was, in substance, a *de facto* Notice of Inquiry and should have been issued as such, rather than as a subsection of the broader CIP NOPR on changes to the CIP standards. For example, it is instructive to compare the Supply Chain NOPR with two other documents: (1) the Notice of Inquiry being issued today on cybersecurity issues arising from the recent incident in Ukraine,[5] and (2) the NOPR concerning the proposed development of a reliability standard to address geomagnetic disturbances.[6] The level of detail and consideration of the issues presented in the Supply Chain NOPR are much more consistent with that in a Notice of Inquiry than a traditional NOPR. As a result, I am concerned that the Commission, by styling its prior action as a NOPR, has skipped a critical step in the rulemaking process: the opportunity for public comment on its directive to develop a standard and the objectives that will frame the design and development of that standard. As explained below, I believe this procedural decision actually makes it less likely that an effective, auditable, and enforceable standard will be implemented on a reasonable schedule, particularly given the acknowledged complexity of this issue.[7]

---

[5] *Cyber Systems in Control Centers*, Notice of Inquiry, Docket No. RM16-18-000.

[6] *Reliability Standards for Geomagnetic Disturbances*, Notice of Proposed Rulemaking, 77 FR 64,935 (Oct. 24, 2012), 141 FERC 61,045 (2012).

[7] I believe that *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014) (Physical Security Directive Order), which is cited in the Final Rule as support for today's action, is primarily relevant to demonstrate a different point than the order indicates. The Physical Security Directive Order followed focused outreach with NERC and other stakeholders to discuss how a physical security standard could be designed and implemented within the parameters of section 215 of the Federal Power Act. As a result of that outreach, the directives in the Physical Security Directive Order were clear, targeted, and reflected shared priorities between the Commission and NERC. Physical Security Directive Order, 146 FERC ¶ 61,166 at PP 6-9. Consequently, NERC was able to develop and file a physical security standard with the Commission in less than three months, and the Commission ultimately approved that standard in November 2014, only roughly eight months after directing its development. *Physical Security Reliability Standard*, 149 FERC ¶ 61,140 (2014). In my view, this example demonstrates how essential outreach is to the timely and effective development of NERC standards.

B. The Lack of Adequate Stakeholder Engagement Will Have Negative Consequences for the Standards Development Process

I am also concerned about the consequences for the standards development process of the Commission's decision to proceed straight to a Final Rule. In particular, I am concerned that the combination of insufficient process and discussion to develop the record and inadequate time for standards development (since the Commission substantially truncated NERC's suggested timeline)[8] will handicap NERC's ability to develop an effective and enforceable proposed standard for the Commission to consider. As noted above, NERC, industry, and other stakeholders will have no meaningful opportunity before initiating their work to provide feedback on the contents of the rule, to seek clarification from the Commission, or to propose revisions to the rule. Yet, this type of feedback is a critical component of the rulemaking process, to ensure that the entities tasked with implementing the Commission's directive have been heard and understand what they are supposed to do. I believe that the Commission is essentially giving the standards development team a homework assignment without adequately explaining what it expects them to hand in.

I do not believe that the Final Rule's flexibility is a justification for proceeding straight to a Final Rule. Indeed, given the inadequate process to date, I fear that the flexibility is in fact a lack of guidance and will therefore be a double-edged sword. The Commission is issuing a general directive in the Final Rule, in the hope that the standards team will do what the Commission clearly could not do: translate general supply chain concerns into a clear, auditable, and enforceable standard within the framework of section 215 of the Federal Power Act. While the Commission need not be prescriptive in its standards directives, the Commission's order assumes that the standards development team will be able to take the "objectives" of the Final Rule and translate them into a standard that the Commission will ultimately find acceptable. I believe that issuing a Supplemental NOPR would benefit the standards development process by enabling additional discussion and feedback regarding the design of a workable standard.

---

[8] In its comments responding to the Supply Chain NOPR, NERC requested that, if the Commission decides to direct the development of a standard, the Commission provide *a minimum* of two years for the standards development process. However, the Commission disregards that request and directs NERC to develop a standard in just one year, apparently based solely on the Trade Associations' request that the Commission allow *at least* one year for the standards development process. I believe this timeline is inconsistent with the Commission's own recognition of the complexity of this issue, and, as discussed herein, likely to delay rather than expedite the implementation of an effective, auditable, and enforceable standard.

C. By Failing to Engage in Adequate Stakeholder Outreach Before Directing Development of a Standard, the Commission Increases the Likelihood that Implementation of a Standard Will be Delayed

A compressed and possibly compromised standards development process also has real consequences for the Commission's consideration of that proposed standard, whenever it is filed for our review. Unlike our authority under section 206 of the FPA, the Commission lacks authority under section 215 to directly modify a flawed reliability standard. Instead, to correct any flaws, the statute requires that we remand the standard to NERC and the standards development process.[9] Thus, notwithstanding the majority's desire to quickly proceed to Final Rule, the statutory construct constrains our ability to timely address a flawed standard, which could actually delay implementation of the protections the Commission seeks to put in place.

Given the realities of the standards development and approval process, we are likely years away from a supply chain standard being implemented, even under the aggressive schedule contemplated in the order. I believe that the Commission should endeavor to provide as much advance guidance as possible before mandating the development of a standard, to increase the likelihood that NERC develops a standard that will be satisfactory to the Commission and reduce the need for a remand. I worry that the limited process that preceded the Final Rule and the expedited timetable will make it extremely difficult for NERC to file a standard that the Commission can cleanly approve. Had the Commission committed itself to conducting adequate outreach, I believe we could have mitigated the likelihood of that outcome, and more effectively and promptly addressed the supply chain threat in the long term. "Delaying" action for a few months thus would, in the long run, lead to prompter and stronger protection for the grid.

II. Conclusion

The choice the Commission faces today on supply chain risk management is not between action and inaction. Rather, given the importance of this issue, I believe that more considered action and a more developed Commission order, even if delayed by a few months, is better than a quick decision to "do something." Ultimately, an effective, auditable, and enforceable standard on supply chain management will require thoughtful consideration of the complex challenges of addressing cybersecurity threats posed through the supply chain within the structure of the FERC/NERC reliability process. In my view, the Commission gains very little and does not meaningfully advance the security of the grid by proceeding straight to a Final Rule, rather than taking the time to build a record to support a workable standard.

Accordingly, I respectfully dissent.

---

[9] 18 U.S.C. § 824o(d)(4).

_____
Cheryl A. LaFleur
Commissioner