162 FERC ¶ 61,044
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM17-13-000]

Supply Chain Risk Management Reliability Standards

(January 18, 2018)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Federal Energy Regulatory Commission (Commission) proposes to approve supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments). The North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization, submitted the proposed Reliability Standards for Commission approval in response to a Commission directive. In addition, the Commission proposes that NERC develop and submit certain modifications to the supply chain risk management Reliability Standards.

DATES: Comments are due **[INSERT DATE 60 days after publication in the FEDERAL REGISTER].**

ADDRESSES: Comments, identified by docket number, may be filed in the following ways:

- Electronic Filing through http://www.ferc.gov. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format.
- Mail/Hand Delivery: Those unable to file electronically may mail or hand-deliver comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE, Washington, DC 20426.

Instructions: For detailed instructions on submitting comments and additional information on the rulemaking process, see the Comment Procedures Section of this document.

FOR FURTHER INFORMATION CONTACT:

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:

162 FERC ¶ 61,044
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Supply Chain Risk Management Reliability Standards Docket No. RM17-13-000

NOTICE OF PROPOSED RULEMAKING

(January 18, 2018)

1. Pursuant to section 215(d)(2) of the Federal Power Act (FPA),[1] the Commission proposes to approve supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments). The North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), submitted the proposed Reliability Standards for Commission approval in response to a Commission directive in Order No. 829.[2] The proposed Reliability Standards are intended to augment the currently-effective CIP Reliability Standards to mitigate cybersecurity risks associated with the supply chain for BES Cyber Systems.[3]

[1] 16 U.S.C. 824o(d)(2).

[2] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 156 FERC ¶ 61,050, at P 43 (2016).

[3] BES Cyber System is defined as "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." Glossary of Terms Used in NERC Reliability Standards (NERC Glossary),

2. As the Commission previously recognized, the global supply chain provides the opportunity for significant benefits to customers, including low cost, interoperability, rapid innovation, a variety of product features and choice.[4] However, the global supply chain also enables opportunities for adversaries to directly or indirectly affect the management or operations of companies that may result in risks to end users. Supply chain risks may include the insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software, as well as poor manufacturing and development practices. We propose to determine that the supply chain risk management Reliability Standards submitted by NERC constitute substantial progress in addressing the supply chain cyber security risks identified by the Commission.

3. The Commission also proposes to approve the proposed Reliability Standards' associated violation risk factors and violation severity levels. With respect to the proposed Reliability Standards' implementation plan and effective date, the Commission proposes to reduce the implementation period from the first day of the first calendar quarter that is 18 months following the effective date of a Commission order approving the proposed Reliability Standards, as proposed by NERC, to the first day of the first calendar quarter that is 12 months following the effective date of a Commission order.

---

http://www.nerc.com/files/glossary_of_terms.pdf. The acronym BES refers to the bulk electric system.

[4] *Revised Critical Infrastructure Protection Reliability Standards*, Notice of Proposed Rulemaking, 80 FR 43,354 (July, 22, 2015), 152 FERC ¶ 61,054, at PP 61-62 (2015).

4. While the Commission proposes to determine that the proposed Reliability Standards address most aspects of the Commission's directive in Order No. 829, there remains a significant cyber security risk associated with the supply chain for BES Cyber Systems because the proposed Reliability Standards exclude Electronic Access Control and Monitoring Systems (EACMS),[5] Physical Access Control Systems (PACS),[6] and Protected Cyber Assets (PCAs),[7] with the exception of the modifications in proposed Reliability Standard CIP-005-6, which apply to PCAs. To address this gap, pursuant to section 215(d)(5) of the FPA,[8] the Commission proposes to direct NERC to develop

[5] EACMS are defined as "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems." NERC Glossary. Reliability Standard CIP-002-5.1a (Cyber Security — BES Cyber System Categorization) states that examples of EACMS include "Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems." Reliability Standard CIP-002-5.1a (Cyber Security — BES Cyber System Categorization) Section A.6 at 6.

[6] PACS are defined as "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers." NERC Glossary. Reliability Standard CIP-002-5.1a states that examples include "authentication servers, card systems, and badge control systems." *Id.*

[7] PCAs are defined as "[o]ne or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same [Electronic Security Perimeter]." NERC Glossary. Reliability Standard CIP-002-5.1a states that examples include, to the extent they are within the Electronic Security Perimeter, "file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems." *Id.*

[8] 16 U.S.C. 824o(d)(5).

modifications to the CIP Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.[9] In addition, the Commission proposes to direct NERC to evaluate the cyber security supply chain risks presented by PACS and PCAs in the study of cyber security supply chain risks requested by the NERC Board of Trustees (BOT) in its resolutions of August 10, 2017.[10] The Commission further proposes to direct NERC to file the BOT-requested study's interim and final reports with the Commission upon their completion.

I. Background

A. Section 215 and Mandatory Reliability Standards

5. Section 215 of the FPA requires a Commission-certified 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.[11] Pursuant to section 215 of the FPA,

[9] Reliability Standard CIP-002-5.1a (Cyber Security System Categorization) provides a "tiered" approach to cybersecurity requirements, based on classifications of high, medium and low impact BES Cyber Systems.

[10] Proposed Additional Resolutions for Agenda Item 9.a: Cyber Security – Supply Chain Risk Management – CIP-005-6, CIP-010-3, and CIP-013-1 (August 10, 2017), http://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf.

[11] 16 U.S.C. 824o(e).

the Commission established a process to select and certify an ERO,[12] and subsequently certified NERC.[13]

B. Order No. 829

6. In Order No. 829, the Commission directed 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.[14] Specifically, the Commission directed NERC to develop a forward-looking, objective-based Reliability Standard that would require responsible entities to develop and implement a plan with supply chain management security controls focused on four security objectives: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.[15]

7. The Commission explained that the first objective, verification of software integrity and authenticity, is intended to reduce the likelihood that an attacker could

---

[12] *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).

[13] *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).

[14] Order No. 829, 156 FERC ¶ 61,050 at P 43.

[15] *Id.* P 45.

exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System.[16]

8. With respect to the second objective, vendor remote access, the Commission stated that the objective is intended to address 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.[17]

9. For the third objective, information system planning, Order No. 829 indicated that the objective is intended to address 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.[18]

10. Vendor risk management and procurement controls, the fourth objective, the Commission explained, are intended to address the risk that responsible entities could enter into contracts with vendors that pose significant risks to the responsible entities' information systems, as well as the risk that products procured by a responsible entity fail to meet minimum security criteria. This objective also addresses the risk that a

[16] *Id.* P 49.

[17] *Id.* P 52.

[18] *Id.* P 57.

compromised vendor would not provide adequate notice and related incident response to responsible entities with whom that vendor is connected.[19]

11. Order No. 829 stated that while responsible entities should be required to develop and implement a plan, the Commission did not require NERC to impose any specific controls or "one-size-fits-all" requirements.[20] In addition, the Commission stated that NERC's response to the Order No. 829 directive should respect the Commission's jurisdiction under FPA section 215 by only addressing the obligations of responsible entities and not by directly imposing any obligations on non-jurisdictional suppliers, vendors or other entities that provide products or services to responsible entities.[21]

C. NERC Petition and Proposed Reliability Standards

12. On September 26, 2017, NERC submitted for Commission approval proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 and their associated violation risk factors and violation severity levels, implementation plans, and effective dates.[22] NERC states that the purpose of the proposed Reliability Standards is to enhance the cybersecurity posture of the electric industry by requiring responsible entities to take additional actions to address cybersecurity risks associated with the supply chain for BES

[19] *Id.* P 60.

[20] *Id.* P 13.

[21] *Id.* P 21.

[22] Proposed Reliability Standards CIP-013-1, CIP-005-6 and CIP-010-3 are not attached to this notice of proposed rulemaking (NOPR). The proposed Reliability Standards are available on the Commission's eLibrary document retrieval system in Docket No. RM17-13-000 and on the NERC website, www.nerc.com.

Cyber Systems. NERC explains that the proposed Reliability Standards are designed to augment the existing controls required in the currently-effective CIP Reliability Standards that help mitigate supply chain risks, providing increased attention on minimizing the attack surfaces of information and communications technology products and services procured to support reliable bulk electric system operations, consistent with Order No. 829. Each proposed Reliability Standard is summarized below.

13. NERC states that the proposed Reliability Standards apply only to medium and high impact BES Cyber Systems. NERC explains that the goal of the CIP Reliability Standards is to "focus[] industry resources on protecting those BES Cyber Systems with heightened risks to the [bulk electric system] … [and] that the requirements applicable to low impact BES Cyber Systems, given their lower risk profile, should not be overly burdensome to divert resources from the protection of medium and high impact BES Cyber Systems."[23] NERC further maintains that the standard drafting team chose to apply the proposed Reliability Standards only to medium and high impact BES Cyber Systems because the proposed Reliability Standards are "consistent with the type of existing CIP cybersecurity requirements applicable to high and medium impact BES Cyber Systems as opposed to those applicable to low impact BES Cyber Systems."[24]

14. NERC states that the standard drafting team also excluded EACMS, PACS, and PCAs from the scope of the proposed Reliability Standards, with the exception of the

[23] NERC Petition at 16-17.

[24] *Id.* at 18.

modifications in proposed Reliability Standard CIP-005-6, which apply to PCAs. NERC explains that although certain requirements in the existing CIP Reliability Standards apply to EACMS, PACS, and PCAs due to their association with BES Cyber Systems (either by function or location), the standard drafting team determined that the proposed supply chain risk management Reliability Standards should focus on high and medium impact BES Cyber Systems only. NERC states that this determination was based on the conclusion that applying the proposed Reliability Standards to EACMS, PACS, and PCAs "would divert resources from protecting medium and high BES Cyber Systems."[25]

15. NERC maintains that with respect to low impact BES Cyber Systems and EACMS, PACS, and PCAs, while not mandatory, NERC expects that these assets will likely be subject to responsible entity supply chain risk management plans required by proposed Reliability Standard CIP-013-1. Specifically, NERC asserts that "Responsible Entities may implement a single process for procuring products and services associated with their operational environments."[26] NERC contends that "by requiring that entities implement supply chain cybersecurity risk management plans for high and medium impact BES Cyber Systems, those plans would likely also cover their low impact BES Cyber Systems."[27] NERC also claims that responsible entities "may also use the same vendors for procuring PACS, EACMS, and PCAs as they do for their high and medium

[25] *Id.* at 20.

[26] *Id.*

[27] *Id.* at 19.

impact BES Cyber Systems such that the same security considerations may be addressed for those Cyber Assets."[28]

Proposed Reliability Standard CIP-013-1

16. NERC states that the focus of proposed Reliability Standard CIP-013-1 is on the steps that responsible entities take "to consider and address cybersecurity risks from vendor products and services during BES Cyber System planning and procurement."[29] NERC explains that proposed Reliability Standard CIP-013-1 does not require any specific controls or mandate "one-size-fits-all" requirements due to the differences in needs and characteristics of responsible entities and the diversity of bulk electric system environments, technologies, and risks. NERC states that the goal of the proposed Reliability Standard is "to help ensure that responsible entities establish organizationally-defined processes that integrate a cybersecurity risk management framework into the system development lifecycle."[30] NERC explains that, among other things, proposed Reliability Standard CIP-013-1 addresses the risk associated with information system planning, as well as vendor risk management and procurement controls, the third and fourth objectives outlined in Order No. 829.

17. NERC states that, consistent with the Commission's FPA section 215 jurisdiction and Order No. 829, the proposed Reliability Standard applies only to responsible entities and does not directly impose obligations on suppliers, vendors, or other entities that

[28] *Id.* at 20.

[29] *Id.* at 22.

[30] *Id.* at 23.

provide products or services to responsible entities. NERC explains that the focus of the proposed Reliability Standard is on the steps responsible entities take to account for security issues during the planning and procurement phase of high and medium impact BES Cyber Systems. NERC also explains that any resulting obligation that a supplier, vendor, or other entity accepts in providing products or services to the responsible entity is a contractual matter between the responsible entity and third parties, which is outside the scope of the proposed Reliability Standard.

18. NERC explains that the term "vendor" is used broadly to refer to any person, company or other organization with whom the responsible entity, or an affiliate, contracts with to supply BES Cyber Systems and related services to the responsible entity. NERC states that the use of the term "vendor," however, "was not intended to bring registered entities that provide reliability services to other registered entities as part of their functional obligations under NERC's Reliability Standards (e.g., a Balancing Authority providing balancing services for registered entities in its Balancing Authority Area) within the scope of the proposed Reliability Standards."[31]

19. NERC maintains that, consistent with Order No. 829, responsible entities need not apply their supply chain risk management plans to the acquisition of vendor products or services under contracts executed prior to the effective date of Reliability Standard CIP-013-1, nor would such contracts need to be renegotiated or abrogated to comply with the proposed Reliability Standard. In addition, NERC indicates that, consistent with the

[31] *Id.* at 21.

development of a forward looking Reliability Standard, if entities are in the middle of procurement activities for an applicable product or service at the time of the effective date of proposed Reliability Standard CIP-013-1, NERC would not expect entities to begin those activities anew to implement their supply chain cybersecurity risk management plan to comply with proposed Reliability Standard CIP-013-1.

20. NERC explains that, under Requirement R1 of this Reliability Standard, responsible entities would be required to have one or more processes to address, as applicable, the following baseline set of security concepts in their procurement activities for high and medium impact BES Cyber Systems: (1) vendor security event notification processes (Part 1.2.1); (2) coordinated incident response activities (Part 1.2.2); (3) vendor personnel termination notification for employees with access to remote and onsite systems (Part 1.2.3); (4) product/services vulnerability disclosures (Part 1.2.4); (5) verification of software integrity and authenticity (Part 1.2.5); and (6) coordination of vendor remote access controls (Part 1.2.6). NERC states that the intent of Part 1.2 of Requirement R1 is not to require that every contract with a vendor include provisions for each of the listed items, but to ensure that these security items are an integrated part of procurement activities, such as a request for proposal or in the contract negotiation process.

21. NERC states that Requirement R2 mandates that each responsible entity implement its supply chain cybersecurity risk management plan. NERC explains that the actual terms and conditions of a procurement contract and vendor performance under a contract are outside the scope of proposed Reliability Standard CIP-013-1. NERC states

that the focus of proposed Reliability Standard CIP-013-1 is "on the processes Responsible Entities implement to consider and address cyber security risks from vendor products or services during BES Cyber System planning and procurement, not on the outcome of those processes…."[32] NERC maintains that responsible entities must make a business decision on whether and how to proceed with an acquisition after weighing the risks associated with a vendor or product and making a good faith effort to include security controls in any agreement with a vendor, as required by proposed Reliability Standard CIP-013-1. In addition, NERC states that vendor performance is outside the scope of the proposed Reliability Standards and, while NERC expects responsible entities to enforce the provisions of their contracts, "a Responsible Entity should not be held responsible under the proposed Reliability Standard for actions (or inactions) of the vendor."[33]

22. With regard to assessing compliance with proposed Reliability Standard CIP-013-1, NERC states that NERC and Regional Entities would focus on whether responsible entities: (1) developed processes reasonably designed to (i) identify and assess risks associated with vendor products and services in accordance with Part 1.1 and (ii) ensure that the security items listed in Part 1.2 are an integrated part of procurement activities; and (2) implemented those processes in good faith. NERC explains that NERC and Regional Entities will evaluate the steps a responsible entity took to assess risks posed by

[32] *Id.* at 27.

[33] *Id.* at 28.

a vendor and associated products or services and, based on that risk assessment, the steps the entity took to mitigate those risks, including the negotiation of security provisions in its agreements with the vendor.

23. Finally, NERC explains that Requirement R3 requires a responsible entity to review and obtain the CIP Senior Manager's approval of its supply chain risk management plan at least once every 15 calendar months in order to ensure that the plan remains up-to-date.

Proposed Modifications in Reliability Standard CIP-005-6

24. Proposed Reliability Standard CIP-005-6 includes two new parts, Parts 2.4 and 2.5, to address vendor remote access, which is the second objective discussed in Order No. 829. NERC explains that the new parts work in tandem with proposed Reliability Standard CIP-013-1, Requirement R1.2.6, which requires responsible entities to address Interactive Remote Access and system-to-system remote access when procuring industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. NERC states that proposed Reliability Standard CIP-005-6, Requirement R2.4 requires one or more methods for determining active vendor remote access sessions, including Interactive Remote Access and system-to-system remote access. NERC explains that the security objective of Requirement R2.4 is to provide awareness of all active vendor remote access sessions, both Interactive Remote Access and system-to-system remote access, that are taking place on a responsible entity's system.

25. NERC maintains that proposed Reliability Standard CIP-005-6, Requirement R2.5 requires one or more methods to disable active vendor remote access, including Interactive Remote Access and system-to-system remote access. NERC explains that the security objective of Requirement R2.5 is to provide the ability to disable active remote access sessions in the event of a system breach. In addition, NERC explains that Requirement R2 was modified to only reference Interactive Remote Access where appropriate. Specifically, Requirements R2.1, R2.2, and R2.3 apply to Interactive Remote access only, while Requirements R2.4 and R2.5 apply both to Interactive Remote Access and system-to-system remote access.

Proposed Modifications in Reliability Standard CIP-010-3

26. Proposed Reliability Standard CIP-010-3 includes a new part, Part 1.6, to address software integrity and authenticity, the first objective addressed in Order No. 829, by requiring the identification of the publisher and confirming the integrity of all software and patches. NERC explains that proposed Reliability Standard CIP-010-3, Requirement R1.6 requires responsible entities to verify software integrity and authenticity in the operational phase, if the software source provides a method to do so. Specifically, NERC states that proposed Reliability Standard CIP-010-3, Requirement R1.6 requires that responsible entities must verify the identity of the software source and the integrity of the software obtained by the software sources prior to installing software that changes established baseline configurations, when methods are available to do so. NERC asserts that the security objective of proposed Requirement R1.6 is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the

software supplier and is not counterfeit. NERC contends that these steps help 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.

BOT Resolutions

27. In the petition, NERC states that in conjunction with the adoption of the proposed Reliability Standards, on August 10, 2017 the BOT adopted resolutions regarding supply chain risk management. In particular, the BOT requested that NERC management, in collaboration with appropriate NERC technical committees, industry representatives, and appropriate experts, including representatives of industry vendors, further study the nature and complexity of cyber security supply chain risks, including risks associated with low impact assets not currently subject to the proposed supply chain risk management Reliability Standards. The BOT further requested NERC to develop recommendations for follow-up actions that will best address any issues identified. Finally, the BOT requested that NERC management provide an interim progress report no later than 12 months after the adoption of these resolutions and a final report no later than 18 months after the adoption of the resolutions. In its petition, NERC states that "over the next 18 months, NERC, working with various stakeholders, will continue to assess whether supply chain risks related to low impact BES Cyber Systems, PACS, EACMS and PCA necessitate further consideration for inclusion in a mandatory Reliability Standard."[34]

[34] *Id.* at 20-21.

Implementation Plan

28. NERC's proposed implementation plan provides that the proposed Reliability Standards become effective on the first day of the first calendar quarter that is 18 months after the effective date of a Commission order approving them. NERC states that the proposed implementation period is designed to afford responsible entities sufficient time to develop and implement their supply chain cybersecurity risk management plans required under proposed Reliability Standard CIP-013-1 and implement the new controls required in proposed Reliability Standards CIP-005-6 and CIP-010-3.

II. Discussion

29. Pursuant to section 215(d)(2) of the FPA, the Commission proposes to approve supply chain risk management Reliability Standards CIP-013-1, CIP-005-6 and CIP-010-3 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. The proposed Reliability Standards will enhance existing protections for bulk electric system reliability by addressing the four objectives set forth in Order No. 829: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

30. The proposed Reliability Standards address the four objectives discussed in Order No. 829. Proposed Reliability Standard CIP-013-1 addresses information system planning and vendor risk management and procurement controls by requiring that responsible entities develop and implement one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. The required plans must address, as applicable, a baseline set of six security concepts: vendor

security event notification; coordinated incident response; vendor personnel termination notification; product/services vulnerability disclosures; verification of software integrity and authenticity; and coordination of vendor remote access controls. Proposed Reliability Standard CIP-005-6 addresses vendor remote access by creating two new requirements: for determining active vendor remote access sessions and for having one or more methods to disable active vendor remote access sessions. Proposed Reliability Standard CIP-010-3 addresses software authenticity and integrity by creating a new requirement that responsible entities verify the identity of the software source and the integrity of the software obtained from the software source prior to installing software that changes established baseline configurations, when methods are available to do so. Taken together, the proposed Reliability Standards constitute substantial progress in addressing the supply chain cyber security risks identified in Order No. 829.

31. While the Commission proposes to approve the proposed Reliability Standards, certain cyber security risks associated with the supply chain for BES Cyber Systems may not be adequately addressed by the NERC proposal. In particular, as discussed below, the Commission is concerned with the exclusion of EACMS, PACS, and PCAs from the scope of the proposed Reliability Standards.[35] To address this risk, pursuant to section 215(d)(5) of the FPA, the Commission proposes that NERC develop modifications to the CIP Reliability Standards to include EACMS within the scope of the supply chain risk

[35] As we noted previously, the only exceptions are the modifications in proposed Reliability Standard CIP-005-6, which apply to PCAs.

management Reliability Standards. In addition, the Commission proposes to direct NERC to evaluate the cyber security supply chain risks presented by PACS and PCAs in the cyber security supply chain risks study requested by the BOT. The Commission further proposes to direct NERC to file the BOT-requested study's interim and final reports with the Commission upon their completion.

32. Below, we discuss the following issues: (A) inclusion of EACMS in the supply chain risk management Reliability Standards; (B) inclusion of PACS and PCAs in the BOT-requested study on cyber security supply chain risks and filing of the study's interim and final reports with the Commission; and (C) NERC's proposed implementation plan.

A. Inclusion of EACMS in CIP Reliability Standards

33. The proposed Reliability Standards only apply to medium and high impact BES Cyber Systems; they do not apply to low impact BES Cyber Systems or Cyber Assets associated with medium and high impact BES Cyber Systems (i.e., EACMS, PACS, and PCAs). The BOT-requested study on cyber security supply chain risks will examine the risks posed by low impact BES Cyber Systems and, as discussed in the following section, we believe it is appropriate to await the outcome of that study's final report before considering whether low impact BES Cyber Systems should be addressed in the supply chain risk management Reliability Standards.

34. With respect to Cyber Assets associated with medium and high impact BES Cyber Systems, and EACMS in particular, we propose further action than what is requested in

the BOT resolutions.[36] As explained in current Reliability Standard CIP-002-5.1a, BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (1) their location within the Electronic Security Perimeter (i.e., PCAs), or (2) the security control function they perform (i.e., EACMS and PACS).[37] EACMS support BES Cyber Systems and are part of the network and security architecture that allow BES Cyber Systems to work as intended by performing electronic access control or electronic access monitoring of the Electronic Security Perimeter (ESP) or BES Cyber Systems.

35. Since EACMS support and enable BES Cyber System operation, misoperation and unavailability of EACMS that support a given BES Cyber System could also contribute to misoperation of a BES Cyber System or render it unavailable, which could adversely affect bulk electric system reliability. EACMS control electronic access, including interactive remote access, into the ESP that protects high and medium impact BES Cyber Systems. One function of electronic access control is to prevent malware or malicious actors from gaining access to the BES Cyber Systems and PCAs within the ESP. Once an EACMS is compromised, the attacker may gain control of the BES Cyber System or PCA. An attacker does not need physical access to the facility housing a BES Cyber System in order to gain access to a BES Cyber System or PCA via an EACMS compromise. By contrast, compromise of PACS, which could potentially grant an

[36] We address PACS and PCAs in the following section.

[37] Reliability Standard CIP-002-5.1a (Cyber Security — BES Cyber System Categorization), Background at 6.

attacker physical access to a BES Cyber System, requires physical access. Further, PCAs typically become vulnerable to remote compromise once EACMS have been compromised. Therefore, EACMS represent the most likely route an attacker would take to access a BES Cyber System or PCA within an ESP.

36. Currently-effective Reliability Standard CIP-010-2 applies to EACMS and the modifications proposed in Reliability Standard CIP-010-3 maintain the current coverage of EACMS, except for new Part 1.6 of Requirement R1, which addresses software integrity and authenticity. Moreover, NERC's petition acknowledges that requirements in the existing CIP Reliability Standards "require Responsible Entities to apply certain protections to PACS, EACMS, and PCAs, given their association with BES Cyber Systems either by function or location."[38] This statement suggests a recognition by NERC that EACMS, PACS, and PCAs warrant certain protections. We agree with NERC's statement, but we believe that the most important focus is on EACMS for the reasons described above.

37. In addition, while EACMS is a term unique to NERC-developed Reliability Standards, it is widely recognized that the types of access and monitoring functions that are included within NERC's definition of EACMS, such as firewalls, are integral to protecting industrial control systems. For example, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

[38] NERC Petition at 19.

identifies firewalls as "the first line of defense within an ICS network environment" that "keep the intruder out while allowing the authorized passage of data necessary to run the organization."[39] ICS-CERT further explains that firewalls "act as sentinels, or gatekeepers, between zones … [and] [w]hen properly configured, they will only let essential traffic cross security boundaries[,] … [i]f they are not properly configured, they could easily pass unauthorized or malicious users or content." Accordingly, if EACMS are compromised, that could adversely affect the reliable operation of associated BES Cyber Systems.

38. NERC explains that the standard drafting team chose to limit the scope of the proposed Reliability Standards to medium and high impact BES Cyber Systems, but not their associated Cyber Assets (e.g., EACMS), in order not to "divert resources from protecting medium and high BES Cyber Systems."[40] As noted above, EACMS include "authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems" that are integral to the security of the medium and high impact BES Cyber Systems to which they

[39] ICS-CERT, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, at 23 (September 2016), https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf. *See also* NIST, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, Revision 2, at Section 5 (ICS Security Architecture) (May 2015) (discussing importance of technologies and strategies, including firewalls, to secure industrial control systems), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[40] *Id.* at 20.

are associated.[41] While NERC states that it will continue to assess whether supply chain risks related to low impact BES Cyber Systems, PACS, EACMS, and PCAs necessitate further consideration for inclusion in a mandatory Reliability Standard, in view of the discussion above, we propose to determine that a sufficient basis currently exists to include EACMS associated with medium and high impact BES Cyber Systems in the supply chain risk management Reliability Standards.

39. Accordingly, pursuant to section 215(d)(5) of the FPA, the Commission proposes to direct NERC to develop modifications to the CIP Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards. The Commission seeks comment on this proposal.

B. BOT-Requested Cyber Security Supply Chain Risks Study

40. As discussed above, we believe it is appropriate to await the findings from the BOT-requested study on cyber security supply chain risks before considering whether low impact BES Cyber Systems should be addressed in the supply chain risk management Reliability Standards.

41. We note that while the BOT resolutions explicitly stated that the BOT-requested study should examine the risks posed by low impact BES Cyber Systems, the BOT resolutions did not identify PACS and PCAs as subjects of the study. However, NERC's

[41] Reliability Standard CIP-002-5.1a (Cyber Security — BES Cyber System Categorization), Section A.6 at 6.

petition suggests that NERC will be evaluating PACS and PCAs as part of the BOT-requested study.[42]

42. While many of the concerns expressed in the previous section with respect to the risks posed by EACMS also apply to varying degrees to PACS and PCAs, we propose to direct NERC, consistent with the representation made in NERC's petition, to include PACS and PCAs in the BOT-requested study and to await the findings of the study's final report before considering further action. We distinguish among EACMS and the other Cyber Assets because, for example, a compromise of a PACS, which would potentially grant an attacker physical access to a BES Cyber System or PCA, is less likely since physical access is also required. Therefore, while we believe that EACMS require immediate action, because they represent the most likely route an attacker would take to access a BES Cyber System or PCA within an ESP, possible action on other Cyber Assets can await completion of the BOT-requested study's final report.

43. In addition to proposing to direct NERC to include PACS and PCAs in the BOT-requested study, we propose to direct that NERC file the study's interim and final reports with the Commission upon their completion. The Commission seeks comment on these proposals.

[42] NERC Petition at 21 ("over the next 18 months, NERC, working with various stakeholders, will continue to assess whether supply chain risks related to low impact BES Cyber Systems, PACS, EACMS, and PCA necessitate further consideration for inclusion in a mandatory Reliability Standard").

C. Implementation Plan

44. The 18-month implementation period proposed by NERC does not appear to be justified based on the anticipated effort required to develop and implement a supply chain risk management plan.[43] While NERC maintains that the proposed implementation period is "designed to afford responsible entities sufficient time to develop and implement their supply chain cybersecurity risk management plans required under proposed Reliability Standard CIP-013-1 and implement the new controls required in proposed Reliability Standards CIP-005-6 and CIP-010-3,"[44] the security objectives of the proposed Reliability Standards are process-based and do not prescribe technology that might justify an extended implementation period. Instead, we propose that the proposed Reliability Standards become effective the first day of the first calendar quarter that is 12 months following the effective date of a Commission order approving the Reliability Standards. Our proposed implementation period is reasonable, given the nature of the requirements in the proposed Reliability Standards, and provides enhanced security for the bulk electric system in a timelier manner. We seek comment on this proposal.

[43] The 18-month implementation plan proposed by NERC may be longer given NERC's request that the effective date of the proposed Reliability Standards falls on the first day of the first calendar quarter that is 18 months after the effective date of a Commission order approving the proposed Reliability Standards.

[44] NERC Petition at 35.

III. Information Collection Statement

45. The FERC-725B information collection requirements contained in this notice of proposed rulemaking are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.[45] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[46] Upon approval of a collection of information, OMB will assign an OMB control number and expiration date. Respondents subject to the filing requirements of this rule will not be penalized for failing to respond to these collections of information unless the collections of information display a valid OMB control number. The Commission solicits comments on the Commission's need for this information, whether the information will have practical utility, the accuracy of the burden 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.

46. The Commission bases its paperwork burden estimates on the changes in paperwork burden presented by the newly proposed CIP Reliability Standard CIP-013-1 and the proposed revisions to CIP Reliability Standard CIP-005-6 and CIP-010-3 as compared to the current Commission-approved Reliability Standards CIP-005-5 and CIP-010-2, respectively. As discussed above, the notice of proposed rulemaking addresses

[45] 44 U.S.C. 3507(d).

[46] 5 CFR 1320.11.

several areas of the CIP Reliability Standards through proposed Reliability Standard CIP-013-1, Requirements R1, R2, and R3. Under Requirement R1, responsible entities would be required to have one or more processes to address the following baseline set of security concepts, as applicable, in their procurement activities for high and medium impact BES Cyber Systems: (1) vendor security event notification processes (Part 1.2.1); (2) coordinated incident response activities (Part 1.2.2); (3) vendor personnel termination notification for employees with access to remote and onsite systems (Part 1.2.3); (4) product/services vulnerability disclosures (Part 1.2.4); (5) verification of software integrity and authenticity (Part 1.2.5); and (6) coordination of vendor remote access controls (Part 1.2.6). Requirement R2 mandates that each responsible entity implement its supply chain cybersecurity risk management plan. Requirement R3 requires a responsible entity to review and obtain the CIP Senior Manager's approval of its supply chain risk management plan at least once every 15 calendar months in order to ensure that the plan remains up-to-date.

47. Separately, proposed Reliability Standard CIP-005-6, Requirement R2.4 requires one or more methods for determining active vendor remote access sessions, including Interactive Remote Access and system-to-system remote access. Proposed Reliability Standard CIP-005-6, Requirement R2.5 requires one or more methods to disable active vendor remote access, including Interactive Remote Access and system-to-system remote access. Proposed Reliability Standard CIP-010-3, Requirement R1.6 requires responsible entities to verify software integrity and authenticity in the operational phase, if the software source provides a method to do so.

48. The NERC Compliance Registry, as of December 2017, identifies approximately 1,250 unique U.S. entities that are subject to mandatory compliance with Reliability Standards. Of this total, we estimate that 288 entities will face an increased paperwork burden under proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3. Based on these assumptions, we estimate the following reporting burden:

RM17-13-000 NOPR (Mandatory Reliability Standards for Critical Infrastructure Protection Reliability Standards)						
	Number of Respondents (1)	**Annual Number of Responses per Respondent (2)**	**Total Number of Responses (1)*(2)=(3)**	**Average Burden & Cost Per Response[47] (4)**	**Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)**	**Cost per Respondent ($) (5)÷(1)**
Create supply chain risk management plan (one-time)[48] (CIP-013-1 R1)	288	1	288	546 hrs.; $44,772	157,248 hrs.; $12,894,336	$44,772

[47] The loaded hourly wage figure (includes benefits) is based on the average of the occupational categories for 2016 found on the Bureau of Labor Statistics website (http://www.bls.gov/oes/current/naics2_22.htm):

Legal (Occupation Code: 23-0000): $143.68

Information Security Analysts (Occupation Code 15-1122): $66.34

Computer and Information Systems Managers (Occupation Code: 11-3021): $100.68

Management (Occupation Code: 11-0000): $81.52

Electrical Engineer (Occupation Code: 17-2071): $68.12

Management Analyst(Code: 43-0000): $63.49

These various occupational categories are weighted as follows: [($81.52)(.10) + $66.34(.315) + $68.12(.02) + $143.68(.15) + $100.68(.10) + $63.49(.315)] = $82.03. The figure is rounded to $82.00 for use in calculating wage figures in this NOPR.

[48] One-time burdens apply in Year One only.

Updates and reviews of supply chain risk management plan (ongoing)[49] (CIP-013-1 R2)	288	1	288	30 hrs.; $2,460	8,640 hrs.; $708,480	$2,460
Develop Procedures to update remote access requirements (one time) (CIP-005-6 R1-R4)	288	1	288	50 hrs.; $4,100	14,400 hrs.; $1,180,800	$4,100
Develop procedures for software integrity and authenticity requirements (one time) (CIP-010-3 R1-R4)	288	1	288	50 hrs.; $4,100	14,400 hrs.; $1,180,800	$4,100
TOTAL (one-time)			**864**		**186,048 hrs.; $15,255,936**	
TOTAL (ongoing)			**288**		**8,640 hrs.; $708,340**	

The one-time burden of 186,048 hours will be averaged over three years (186,048 hours ÷ 3 = 62,016 hours/year over three years).

The ongoing burden of 8,640 hours applies to only Years 2 and beyond.

The number of responses is also average over three years (864 responses (one-time) + (288 responses (Year 2) + 288 responses (Year 3)) ÷ 3 = 480 responses.

The responses and burden for Years 1-3 will total respectively as follows:

Year 1: 480 responses; 62,016 hours

Year 2: 480 responses; 62,016 hours + 8,640 hours = 70,656 hours

Year 3: 480 responses; 62,016 hours + 8,640 hours = 70,656 hours

[49] Ongoing burdens apply in Year 2 and beyond.

49. The following shows the annual cost burden for each year, based on the burden hours in the table above:

- Year 1: $15,255,936
- Years 2 and beyond: $708,480
- The paperwork burden estimate includes costs associated with the initial development of a policy to address requirements relating to: (1) developing the supply chain risk management plan; (2) updating the procedures related to remote access requirements (3) developing the procedures related to software integrity and authenticity. Further, the estimate reflects the assumption that costs incurred in year 1 will pertain to plan and procedure development, while costs in years 2 and 3 will reflect the burden associated with maintaining the SCRM plan and modifying it as necessary on a 15 month basis.

50. Title: Mandatory Reliability Standards, Revised Critical Infrastructure Protection Reliability Standards

Action: Proposed Collection FERC-725B.

OMB Control No.: 1902-0248.

Respondents: Businesses or other for-profit institutions; not-for-profit institutions.

Frequency of Responses: On Occasion.

Necessity of the Information: This notice of proposed rulemaking proposes to approve the requested modifications to Reliability Standards pertaining to critical infrastructure protection. As discussed above, the Commission proposes to approve NERC's proposed CIP Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 pursuant to section

215(d)(2) of the FPA because they improve upon the currently-effective suite of cyber security CIP Reliability Standards.

Internal Review: The Commission has reviewed the proposed Reliability Standards and made a determination that its action is necessary to implement section 215 of the FPA.

51. Interested persons may obtain information on the reporting requirements by contacting the following: Federal Energy Regulatory Commission, 888 First Street, NE Washington, DC 20426 [Attention: Ellen Brown, Office of the Executive Director, e-mail: DataClearance@ferc.gov, phone: (202) 502-8663, fax: (202) 273-0873].

52. For submitting comments concerning the collection(s) of information and the associated burden estimate(s), please send your comments to the Commission, and to the Office of Management and Budget, Office of Information and Regulatory Affairs, Washington, DC 20503 [Attention: Desk Officer for the Federal Energy Regulatory Commission, phone: (202) 395-4638, fax: (202) 395-7285]. For security reasons, comments to OMB should be submitted by e-mail to: oira_submission@omb.eop.gov. Comments submitted to OMB should include Docket Number RM17-13-000.

IV. Environmental Analysis

53. 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.[50] The Commission has categorically excluded certain actions from this requirement as not having a significant effect on the human environment.

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

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.[51] The actions proposed herein fall within this categorical exclusion in the Commission's regulations.

V. Regulatory Flexibility Act Analysis

54. The Regulatory Flexibility Act of 1980 (RFA) generally requires a description and analysis of proposed rules that will have significant economic impact on a substantial number of small entities.[52] The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.[53] The SBA revised its size standard for electric utilities (effective January 22, 2014) to a standard based on the number of employees, including affiliates (from the prior standard based on megawatt hour sales).[54]

55. Proposed Reliability Standards CIP-013-1, CIP-005-6, CIP-010-3 are expected to impose an additional burden on 288 entities[55] (reliability coordinators, generator operators, generator owners, interchange coordinators or authorities, transmission operators, balancing authorities, and transmission owners).

[51] 18 CFR 380.4(a)(2)(ii).

[52] 5 U.S.C. 601-12.

[53] 13 CFR 121.101.

[54] 13 CFR 121.201, Subsection 221.

[55] Public utilities may fall under one of several different categories, each with a size threshold based on the company's number of employees, including affiliates, the parent company, and subsidiaries. For the analysis in this NOPR, we are using a 500 employee threshold due to each affected entity falling within the role of Electric Bulk Power Transmission and Control (NAISC Code: 221121).

56. Of the 288 affected entities discussed above, we estimate that approximately 248 or 86.2 percent of the affected entities are small entities. We estimate that each of the 248 small entities to whom the proposed modifications to Reliability Standards CIP-013-1, CIP-005-6, CIP-010-3 apply will incur one-time costs of approximately $52,972 per entity to implement the proposed Reliability Standards, as well as the ongoing paperwork burden reflected in the Information Collection Statement (approximately $2,460 per year per entity). We do not consider the estimated costs for these 248 small entities to be a significant economic impact. Accordingly, we certify that proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 will not have a significant economic impact on a substantial number of small entities.

VI. Comment Procedures

57. The Commission invites interested persons to submit comments on the matters and issues proposed in this notice to be adopted, including any related matters or alternative proposals that commenters may wish to discuss. Comments are due [**INSERT DATE 60 days after publication in the FEDERAL REGISTER**]. Comments must refer to Docket No. RM17-13-000, and must include the commenter's name, the organization they represent, if applicable, and address.

58. The Commission encourages comments to be filed electronically via the eFiling link on the Commission's web site at http://www.ferc.gov. The Commission accepts most standard word processing formats. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not

in a scanned format. Commenters filing electronically do not need to make a paper filing.

59. Commenters that are not able to file comments electronically must send an original of their comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE, Washington, DC 20426.

60. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability section below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

VII. Document Availability

61. 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.

62. 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.

63. 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 direction of the Commission. Commissioner LaFleur is concurring with a separate statement attached.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Supply Chain Risk Management Reliability Standards Docket No. RM17-13-000

(Issued January 18, 2018)

LaFLEUR, Commissioner *concurring*:

In today's order, the Commission proposes to approve the supply chain risk management standards filed by the North American Electric Reliability Corporation (NERC), and direct certain modifications to those standards. I write separately to explain my vote in support of today's order, given my dissent on the Commission order that directed the development of these standards.[1]

As I stated in my dissent, I shared the Commission's concern about supply chain threats and supported continued Commission attention to those threats. Indeed, I remain concerned that the supply chain is a significant cyber vulnerability for the bulk power system. However, I believed that the Commission was proceeding too quickly to require a supply chain standard, without having sufficiently worked with NERC, industry, and other stakeholders on how to design an effective, auditable, and enforceable standard. In my view, the directive that resulted was insufficiently developed and created a risk that needed protections against supply threats would be delayed, due in large part to the nature of the NERC standards process.

Given the limited guidance and timeline provided by the Commission in Order No. 829, the proposed standards are, unsurprisingly, quite general, focusing primarily "on the processes Responsible Entities implement to consider and address cyber security risks from vendor products or services during BES Cyber System planning and procurement, not on the outcome of those processes…."[2] The proposed standards would provide significant flexibility to registered entities to determine how best to comply with their requirements. In my view, that flexibility presents both potential risks and benefits. It could allow effective, adaptable approaches to flourish, or allow compliance plans that meet the letter of the standards but do not effectively address supply chain threats. I hope that we will see more of the former, but I believe the Commission, NERC, and the

[1] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 156 FERC ¶ 61,050 (2016) (LaFleur, Comm'r, *dissenting*).

[2] NERC Petition at 27.

Regional Entities should closely monitor implementation if the standards are ultimately approved.

In voting for today's order, I recognize that the choice before the Commission today is not the same as it was in July 2016. I acknowledge that a significant amount of time and effort have been committed to the development of these standards in response to a duly voted Commission order. Most importantly, I agree that they are an improvement over the *status quo*. I do not believe that remanding these standards or the larger supply chain issue to the NERC standards process would be a prudent step at this point. Rather, I believe the better course of action at this time is to move forward with these standards and, assuming the Commission ultimately proceeds to Final Rule, improve them over time as needed.

In that regard, I believe the Commission is appropriately proposing to direct a modification to the proposed standards to address an identified reliability gap regarding Electronic Access Control and Monitoring Systems. I also support the proposal to require NERC to include Physical Access Controls and Protected Cyber Assets within its ongoing assessment of the supply chain risks posed by low-impact Bulk Electric System Cyber Systems, which will help the Commission and NERC determine whether further revisions to the standards are needed.

More so than with most standards, I believe that whether these standards are effective will only reveal itself over time as we gain additional experience with them. I am therefore particularly interested in feedback from commenters on how the Commission, NERC, and industry should assess these standards, including any reporting obligations that might be appropriate.[3] In addition, given the very general process-oriented nature of the standard, I also support the proposal to shorten the implementation date for the new standards. If ultimately adopted, the revised deadline will allow industry, NERC, and the Commission to put the standards in place sooner while continuing to evaluate how best to protect the bulk power system against supply chain threats.

[3] I note that NERC has also developed draft implementation guidance that provides additional detail regarding possible compliance approaches. As NERC and the Regional Entities gain additional experience with assessing compliance under these standards, updating this implementation guidance could be an effective approach for quickly disseminating best practices and lessons learned.

For these reasons, I respectfully concur.

_____

Cheryl A. LaFleur
Commissioner