165 FERC ¶ 61,020
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM17-13-000; Order No. 850]

Supply Chain Risk Management Reliability Standards

(Issued October 18, 2018)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule.

SUMMARY: The Federal Energy Regulatory Commission (Commission) approves 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) submitted by the North American Electric Reliability Corporation (NERC). In addition, the Commission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems.

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

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

Patricia Eke (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-8388
patricia.eke@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:

165 FERC ¶ 61,020
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Cheryl A. LaFleur, Neil Chatterjee, and Richard Glick.

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

ORDER NO. 850

FINAL RULE

(Issued October 18, 2018)

1. Pursuant to section 215(d)(2) of the Federal Power Act (FPA), the Commission approves 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).[1] The North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), submitted the supply chain risk management Reliability Standards for approval in response to a Commission directive in Order No. 829.[2] As discussed below, we approve the supply

[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).

chain risk management Reliability Standards as they are responsive to Order No. 829 and improve the electric industry's cybersecurity posture by requiring that entities mitigate certain cybersecurity risks associated with the supply chain for BES Cyber Systems.[3]

2. The Commission has previously explained that the global supply chain affords significant benefits to customers, including low cost, interoperability, rapid innovation, and a variety of product features and choice.[4] Despite these benefits, the global supply chain creates opportunities for adversaries to directly or indirectly affect the management or operations of companies with potential risks to end users. Supply chain risks include insertion of counterfeits or malicious software, unauthorized production, tampering, or theft, as well as poor manufacturing and development practices. Based on the record in this proceeding, we conclude that the supply chain risk management Reliability Standards largely address these supply chain cybersecurity risks as set out within the scope of Order No. 829. Among other things, the supply chain risk management Reliability Standards are forward-looking and objective-based and 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

[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), 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, 152 FERC ¶ 61,054, at PP 61-62 (2015).

system operations.[5] Consistent with Order No. 829, the Reliability Standards focus on the following four security objectives: (1) software integrity and authenticity; (2) vendor remote access protections; (3) information system planning; and (4) vendor risk management and procurement controls.

3. The Commission also approves the supply chain risk management Reliability Standards' associated violation risk factors and violation severity levels. Regarding the Reliability Standards' implementation plan and effective date, we approve NERC's proposed implementation period of 18 months following the effective date of a Commission order. The NOPR proposed to reduce the implementation period to 12 months.[6] However, as discussed below, the NOPR comments provide sufficient justification for adopting the 18-month implementation period proposed by NERC. Specifically, the comments clarify that technical upgrades are likely necessary to meet the Reliability Standards' security objectives, which could involve longer time-horizon capital budgets and planning cycles.

4. While the supply chain risk management Reliability Standards address the Commission's directive in Order No. 829, we determine that there remains a significant cybersecurity risk associated with the supply chain for BES Cyber Systems because the approved Reliability Standards do not address Electronic Access Control and Monitoring

[5] Order No. 829, 156 FERC ¶ 61,050 at P 2.

[6] *Supply Chain Risk Management Reliability Standards*, Notice of Proposed Rulemaking, 83 FR 3433 (January 25, 2018), 162 FERC ¶ 61,044 (2018) (NOPR).

Systems (EACMS).[7] As we observed in the NOPR, 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.[8] Moreover, as stated in Order No. 848, EACMS, which include, for example, firewalls, authentication servers, security event monitoring systems, intrusion detection systems and alerting systems, control electronic access into Electronic Security Perimeters (ESP), play a significant role in the protection of high and medium impact BES Cyber Systems.[9] Once an EACMS is compromised, an attacker could more easily enter the ESP and effectively control the BES Cyber System or Protected Cyber Asset.[10] For example, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) identifies firewalls as "the first line of defense within an ICS network environment" that "keep the intruder out while allowing the authorized

[7] 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.

[8] NOPR, 162 FERC ¶ 61,044 at P 37.

[9] *Cyber Security Incident Reporting Reliability Standards*, Order No. 848, 164 FERC ¶ 61,033, at P 10 (2018). ESP is defined as "[t]he logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol." NERC Glossary.

[10] Order No. 848, 164 FERC ¶ 61,033 at P 10.

passage of data necessary to run the organization."[11] 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."[12] Accordingly, if EACMS are compromised, that could adversely affect the reliable operation of associated BES Cyber Systems.[13] Given the significant role that EACMS play in the protection scheme for medium and high impact BES Cyber Systems, we determine that EACMS should be within the scope of the supply chain risk management Reliability Standards to provide minimum protection against supply chain attack vectors.

5. To address this gap, pursuant to section 215(d)(5) of the FPA,[14] the Commission directs NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management

[11] *ICS-CERT, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies* at 23, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[12] *Id.*

[13] NOPR, 162 FERC ¶ 61,044 at P 37.

[14] 16 U.S.C. 824o(d)(5).

Reliability Standards.[15] We direct NERC to submit the directed modifications within 24 months of the effective date of this final rule.

6. Further, the NERC proposal does not address Physical Access Control Systems (PACS)[16] and Protected Cyber Assets (PCA),[17] with the exception of the modifications in Reliability Standard CIP-005-6, which apply to PCAs. We remain concerned that the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards. Nevertheless, in contrast to EACMS, we believe that more study is necessary to determine the impact of PACS and PCAs in the context of the supply chain risk management Reliability Standards. We distinguish among EACMS and the other Cyber Assets because compromise of PACS and PCAs are less likely. 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. In

[15] 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.

[16] 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.*

[17] 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.*

addition, PCAs typically become vulnerable to remote compromise only once EACMS have been compromised. Thus, we accept NERC's commitment to evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC Board of Trustees (BOT) in its resolutions of August 10, 2017.[18] The Commission further directs NERC to file the BOT-directed final report with the Commission upon its completion.[19]

I. Background

A. Section 215 and Mandatory Reliability Standards

7. 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.[20] Pursuant to section 215 of the FPA,

[18] NERC Board of Trustees, 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).

[19] As discussed later in this final rule, the NOPR proposed to direct NERC to file the BOT-directed interim report, due 12 months from the date of the BOT resolutions, as well as the final report, which is due 18 months from the date of the BOT resolutions. On September 7, 2018, NERC filed the BOT-directed interim report in this docket.

[20] 16 U.S.C. 824o(e).

the Commission established a process to select and certify an ERO,[21] and subsequently certified NERC.[22]

B. Order No. 829

8. 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.[23] 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.[24]

9. The Commission explained that verification of software integrity and authenticity 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

---

[21] *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).

[22] *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).

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

[24] *Id.* P 45.

Cyber System.[25] For 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.[26] As to 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.[27] For vendor risk management and procurement controls, the Commission explained that this objective is 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 compromised vendor would not provide adequate notice and related incident response to responsible entities with whom that vendor is connected.[28]

[25] *Id.* P 49.

[26] *Id.* P 52.

[27] *Id.* P 57.

[28] *Id.* P 60.

10. Order No. 829 stated that while responsible entities should be required to develop and implement a plan, NERC need not impose any specific controls or "one-size-fits-all" requirements.[29] 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.[30]

C. NERC Petition and Proposed Reliability Standards

11. 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 plan, and effective date.[31] NERC states that the purpose of the 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 Cyber Systems. NERC explains that the 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

[29] *Id.* P 13.

[30] *Id.* P 21.

[31] Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 are not attached to this final rule. The 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.

information and communications technology products and services procured to support reliable bulk electric system operations, consistent with Order No. 829.

12. NERC states that the supply chain risk management 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."[32] NERC further maintains that the standard drafting team chose to limit the applicability of the Reliability Standards to medium and high impact BES Cyber Systems because the supply chain risk management 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."[33]

13. NERC states that the standard drafting team also excluded EACMS, PACS, and PCAs from the scope of the supply chain risk management Reliability Standards, with the exception of the modifications in 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

[32] NERC Petition at 16-17.

[33] *Id.* at 18.

Systems (either by function or location), the standard drafting team determined that the 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."[34]

14. NERC asserts 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 Reliability Standard CIP-013-1. Specifically, NERC explains that "[r]esponsible [e]ntities may implement a single process for procuring products and services associated with their operational environments."[35] 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."[36] 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 impact BES Cyber Systems such that the same security considerations may be addressed for those Cyber Assets."[37]

---

[34] *Id.* at 20.

[35] *Id.*

[36] *Id.* at 19.

[37] *Id.* at 20.

Proposed Reliability Standard CIP-013-1

15. NERC states that the focus of proposed Reliability Standard CIP-013-1 is on the steps that responsible entities must take "to consider and address cybersecurity risks from vendor products and services during BES Cyber System planning and procurement."[38] 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."[39] NERC observes 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.

16. 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 Reliability Standard. In addition, NERC indicates that, consistent with the

[38] *Id.* at 22.

[39] *Id.* at 23.

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

17. With regard to assessing compliance with 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 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.

Proposed Modifications in Reliability Standard CIP-005-6

18. 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.

Proposed Modifications in Reliability Standard CIP-010-3

19. 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 that the publisher is identified and the integrity of all software and patches are confirmed. NERC explains that proposed Reliability Standard CIP-010-3, Requirement R1.6 requires responsible entities to verify software integrity and authenticity prior to a change from the existing baseline configuration, 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 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

20. In the petition, NERC states that in conjunction with the adoption of the supply chain risk management Reliability Standards, on August 10, 2017, the BOT adopted resolutions regarding supply chain risk management. In particular, the BOT directed NERC management, in collaboration with appropriate NERC technical committees, industry representatives, and appropriate experts, including representatives of industry vendors, to further study the nature and complexity of cybersecurity supply chain risks, including risks associated with low impact assets not currently subject to the supply chain risk management Reliability Standards. The BOT further directed NERC to develop recommendations for follow-up actions that will best address any issues identified. Finally, the BOT directed that NERC management provide an interim progress report no later than 12 months after the adoption of these resolutions (i.e., by August 10, 2018) and a final report no later than 18 months after the adoption of the resolutions (i.e., by February 10, 2019). 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."[40]

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

Implementation Plan

21. NERC's proposed implementation plan provides that the supply chain risk management 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.

D. Notice of Proposed Rulemaking

22. On January 18, 2018, the Commission issued a NOPR proposing to approve supply chain risk management Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3. The NOPR stated that the supply chain risk management 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."[41] Accordingly, the NOPR proposed to determine that the supply chain risk management Reliability Standards constitute

[41] NOPR, 162 FERC ¶ 61,044 at P 29.

substantial progress in addressing the supply chain cybersecurity risks identified by the Commission in Order No. 829.[42]

23. The NOPR proposed to approve the supply chain risk management Reliability Standards' associated violation risk factors and violation severity levels. However, with respect to the implementation plan and effective date, the NOPR proposed 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.[43]

24. The NOPR proposed to determine that a significant cybersecurity risk associated with the supply chain for BES Cyber Systems persists because the proposed supply chain risk management Reliability Standards exclude EACMS, PACS, and PCAs, with the exception of the modifications in Reliability Standard CIP-005-6, which apply to PCAs. To address this gap, pursuant to section 215(d)(5) of the FPA, the NOPR proposed 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. In addition, the Commission proposed to direct that NERC evaluate the cybersecurity supply chain risks presented by

[42] *Id.* P 30.

[43] *Id.* P 44.

PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.

25. The Commission received fifteen comments on the NOPR.

E. Interim BOT-Directed Report

26. On September 7, 2018, NERC submitted to the Commission an informational filing containing the BOT-directed interim report prepared by the Electric Power Research Institute (EPRI).[44] The interim report explains that EPRI analyzed: (1) information regarding bulk electric system products and manufacturers; (2) emerging vendor practices and industry standards; and (3) the applicability of the CIP Reliability Standards to supply chain risks. The interim report concludes with three categories of identified next steps for further analysis and investigation.

27. First, EPRI identifies four noteworthy industry practices, not already required by the CIP Reliability Standards, which may potentially reduce future supply chain risks if implemented correctly: (1) third-party accreditation processes; (2) secure hardware delivery; (3) threat-informed procurement language; and (4) processes related to unsupported or open-source technology. Second, EPRI recommends further study in modeling and assessing the potential impact of common-mode vulnerabilities, especially those targeting low-impact BES Cyber Systems. EPRI states that "risks of common-

[44] NERC, Informational Filing regarding Proposed Supply Chain Risk Management Reliability Standards, Docket No. RM17-13-000 (September 7, 2018) (NERC Interim Report).

mode vulnerabilities … can be mitigated if supply chain security practices are applied uniformly across cyber asset types."[45] Finally, EPRI recommends various methods to obtain additional data on industry practices. These methods included issuing pre-audit surveys and questionnaires; targeting outreach to bulk electric system vendors; developing standard vendor data sheets related to the CIP Reliability Standards; and independently testing legacy assets. In its accompanying filing, NERC states its intention to continue to study supply chain risks over the coming months, develop recommendations for follow-up actions, and present a final report to the NERC BOT at its February 2019 meeting.

II. Discussion

28. Pursuant to section 215(d)(2) of the FPA, the Commission approves 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. We determine that the supply chain risk management Reliability Standards will enhance existing protections for bulk electric system reliability by addressing the four objectives identified 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.

29. Reliability Standard CIP-013-1 addresses information system planning and vendor risk management and procurement controls by requiring that responsible entities develop

[45] *Id.* at 5-1.

and implement one or more documented supply chain cybersecurity 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: (1) vendor security event notification; (2) coordinated incident response; (3) vendor personnel termination notification; (4) product/services vulnerability disclosures; (5) verification of software integrity and authenticity; and (6) coordination of vendor remote access controls. 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. 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.

30. While we determine that the approved supply chain risk management Reliability Standards constitute substantial progress in addressing the supply chain cybersecurity risks identified in Order No. 829, as discussed below, we find that the exclusion of EACMS from the scope of the Reliability Standards presents risks to the cybersecurity of the bulk electric system. As explained in Order No. 848, EACMS are defined in the NERC Glossary 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." Among other things, EACMS include firewalls, authentication servers, security event monitoring systems, intrusion detection systems

and alerting systems. The purpose of an ESP, in turn, is to manage electronic access to BES Cyber Systems to support the protection of the BES Cyber Systems against compromise that could lead to misoperation or instability in the bulk electric system.[46] The record indicates that the vulnerabilities associated with EACMS are well understood and appropriate for mitigation. Thus, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop modifications to the CIP Reliability Standards to include EACMS within the scope of the supply chain risk management Reliability Standards. We direct NERC to submit the directed modifications within 24 months of the effective date of this final rule.

31. In addition, while PACS and PCAs also present concerns, we agree with NERC and others that further study is warranted with regard to the impacts and benefits of directing that the ERO address the risks associated with PACS and PCAs in the supply chain risk management Reliability Standards. Accordingly, we accept NERC's commitment to evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the cybersecurity supply chain risks study directed by the BOT. The Commission further directs NERC to file the BOT-directed final report with the Commission upon its completion.

32. In the sections 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-directed study on cybersecurity supply chain risks and filing of the

[46] Order No. 848, 164 FERC ¶ 61,033 at PP 39-40.

BOT-directed final report with the Commission; (C) supply chain risk management Reliability Standards' implementation plan and effective date; and (D) other issues raised in the NOPR comments.

A. Inclusion of EACMS in CIP Reliability Standards

1. NOPR

33. The NOPR observed that the supply chain risk management Reliability Standards 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 NOPR, however, recognized that the BOT-directed study on cybersecurity supply chain risks will examine the risks posed by low impact BES Cyber Systems.[47] While acknowledging NERC's commitment to study these issues, as evinced by the BOT-directed study, the NOPR proposed to direct NERC to modify the supply chain risk management Reliability Standards to include within their scope EACMS associated with medium and high impact BES Cyber Systems.[48]

34. Specifically, the NOPR explained that BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of, *inter alia*, the security control function they perform.[49] In particular, EACMS support BES Cyber Systems and are part of the network and security architecture that allows BES

[47] NOPR, 162 FERC ¶ 61,044 at P 33.

[48] *Id.* P 39.

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

Cyber Systems to work as intended by performing electronic access control or electronic access monitoring of the ESP or BES Cyber Systems.

35. The NOPR indicated that 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. The NOPR also explained that EACMS control electronic access, including interactive remote access, into the ESP that protects high and medium impact BES Cyber Systems. As the NOPR further noted, 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. The NOPR concluded that EACMS represent the most likely route an attacker would take to access a BES Cyber System or PCA within an ESP.[50]

2. Comments

36. NERC does not support the proposed directive to include EACMS within the scope of the supply chain risk management Reliability Standards at this time. NERC indicates that it is currently analyzing supply chain risks associated with EACMS, among other things, as part of the BOT-directed study of supply chain risks related to low impact BES Cyber Systems. NERC explains that the "study will help identify and differentiate the risks presented by various types of EACMS" to help in any directed standards

[50] NOPR, 162 FERC ¶ 61,044 at P 35.

development process.[51] NERC requests that the Commission refrain from issuing a directive on EACMS until the results of the BOT-directed study to assess supply chain risks associated with EACMS are received.[52]

37. Most commenters agree with NERC that the Commission should approve the supply chain risk management Reliability Standards as filed and not direct the inclusion of EACMS at this time. Instead, Trade Associations, EEI, ITC, IRC, and MISO TOs support evaluating in the BOT-directed study the possibility of including EACMS in the supply chain risk management Reliability Standards.[53]

38. Trade Associations contend that first allowing completion of the BOT-directed study would allow NERC to assess the diversity of EACMS that perform control or monitoring functions with varying risk levels and "is likely to provide more specific information and analysis concerning whether any category of EACMS might be appropriately included within the scope of the supply chain Reliability Standards."[54] Trade Associations also maintain that first having the BOT-directed study results will facilitate a more efficient and effective standards development process.

39. While also supportive of awaiting the results of the BOT-directed study, EEI asserts that EACMS are protected under existing CIP Reliability Standards. EEI cites

---

[51] NERC Comments at 6.

[52] *Id.* at 4-6.

[53] Trade Associations Comments at 10, EEI Comments at 10, ITC Comments at 5, IRC Comments at 3.

[54] Trade Associations Comments at 10.

Reliability Standards CIP-005-5, Requirements R1, Part 1.3 and R2, Parts 2.1-2.3, CIP-007-6, Requirements R1, Part 1.1, R2, R3, R4, and R5, and CIP-010-2, Requirement 2, Part 2.1 as protecting EACMS against compromise.[55] Moreover, EEI states that the likelihood of compromise of an EACMS from potential supply chain-derived threats was not addressed in the NOPR and "should be evaluated before directing a CIP Standard scope expansion."[56] Even so, EEI supports further evaluating the feasibility, as well as the benefits, of adding EACMS to the supply chain risk management Reliability Standards. EEI contends that waiting for the BOT-directed study will allow industry time to gain experience implementing the supply chain risk management Reliability Standard requirements as well as help identify potential follow-up actions.[57]

40. MISO TOs likewise aver that EACMS, while important, are "not unprotected" under currently-effective CIP Reliability Standards. MISO TOs, like EEI, reference Reliability Standard CIP-007-6 (Cyber Security — System Security Management), which requires responsible entities to manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems. MISO TOs state that this Reliability Standard applies to EACMS. AECC also contends that the existing CIP Reliability Standards already sufficiently cover any risks associated

[55] EEI Comments at 8.

[56] *Id*.

[57] *Id.* at 10.

with EACMS.[58] In particular, AECC states that "CIP-005-6 already addresses vendor-initiated remote access … [and] developing technology services for BEC Cyber Systems under CIP-010-3 inherently already requires coverage for EACMS, PACS, and PCAs due to the nature of the technology."[59]

41. ITC, IRC, and MISO TOs assert that including EACMS within the supply chain risk management Reliability Standards would constitute a substantial expansion of the Reliability Standards and would require significant additional resources for compliance, without a commensurate improvement in bulk electric system reliability. According to ITC, the record does not contradict NERC's technical assessment that inclusion of EACMS within the supply chain risk management Reliability Standards is not justified. ITC claims that the NOPR, while "descriptively accurate," misunderstands the purpose and function of EACMS, which, ITC states, are intended to protect the ESP and the BES Cyber Assets contained therein and are not intended to provide a reliability function. ITC concludes that misoperation of an EACMS, while serious, does not rise to the level of a direct threat to the reliability of the bulk electric system.

42. IRC similarly believes that including EACMS within the scope of the supply chain risk management Reliability Standards would require "significant resources and effort" and because EACMS vendors supply such systems to a larger market than just the power sector there would need to be coordination with other industries before implementing a

[58] AECC Comments at 2-3.

[59] *Id.* at 3.

supply chain risk management Reliability Standard for EACMS.[60] MISO TOs also contend that including EACMS would affect numerous pieces of equipment and assets, with associated costs, system changes, and other burdens, without showing commensurate benefits.[61]

43. Idaho Power, for its part, does not believe that EACMS should be included in the scope of the supply chain risk management Reliability Standards based on its view that EACMS are used in other industries and are not specific to critical infrastructure. Instead, Idaho Power states that the focus should be on correctly configuring EACMS devices as opposed to addressing procurement practices.[62]

44. Appelbaum, Reclamation, Resilient Societies, Isologic, Mabee, and MPUC support the NOPR directive regarding EACMS associated with medium and high impact BES Cyber Systems. In addition, the commenters urge the Commission to extend the scope of the supply chain risk management Reliability Standards to low impact BES Cyber Systems.[63] MPUC states, for example, that the supply chain risk management Reliability Standards should apply to all BES Cyber System assets, unless the specific asset can be shown to be completely isolated from the bulk electric system.[64] Resilient

---

[60] IRC Comments at 2-3.

[61] MISO TO Comments at 16.

[62] Idaho Power Comments at 2.

[63] Appelbaum Comments at 6, Reclamation Comments at 7, Resilient Societies Comments at 3-4, Isologic Comments at 3, Mabee Comments at 4, MPUC Comments at 6.

[64] MPUC Comments at 6.

Societies states that the supply chain risk management Reliability Standards should apply to low impact BES Cyber Systems since the compromise of a low impact BES Cyber System could lead to the compromise of medium or high impact BES Cyber Systems.[65]

45. APS states that it supports the NOPR proposal to direct NERC to modify the supply chain risk management Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems. However, APS contends that the Commission should delay their inclusion until NERC and industry complete their analysis of the potential need to separate the functions reflected in the current EACMS definition (e.g., electronic access control versus electronic access monitoring). APS states that, including EACMS that perform electronic access control functions within the scope of the supply chain risk management Reliability Standards "represents good cybersecurity posture … [h]owever, at this time, the definition of EACMS is not sufficiently mature to make the necessary distinction discussed above."[66]

3. Commission Determination

46. Pursuant to section 215(d)(5) of the FPA, we adopt the NOPR proposal and direct NERC to develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards. While we are sensitive to the position taken by NERC and other commenters that the Commission should not issue a directive until after completion of

[65] Resilient Societies Comments at 3.

[66] APS Comments at 5.

the BOT-directed final report, we conclude that the record before us supports directing NERC to include at least some subset of EACMS associated with medium and high impact BES Cyber Systems at this time. We are not persuaded by comments advocating delay in view of the forthcoming BOT-directed final report because the standard drafting team will have the benefit of the BOT-directed final report, which is due in February 2019, when developing the directed Reliability Standard modifications.[67]

47. We continue to believe that EACMS represent the most likely route an attacker would take to access a BES Cyber System or PCA within an ESP based on the functions they perform.[68] EACMS support BES Cyber Systems and are part of the network and security architecture that allows BES Cyber Systems to work as intended because they perform electronic access control or electronic access monitoring of the ESP or BES Cyber Systems. In particular, EACMS control electronic access, including interactive remote access, into the ESP that protects high and medium impact BES Cyber Systems. One specific 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.[69] Given the significant role that EACMS play in the protection scheme for medium and high impact BES Cyber Systems, we determine that EACMS should be within the scope of the

[67] As we have imposed a 24-month deadline for NERC to file the modified supply chain risk management Reliability Standards, the standard drafting team will have ample time to review and incorporate the findings in the BOT-directed final report.

[68] *See* NOPR, 162 FERC ¶ 61,044 at P 35.

[69] *Id.*

supply chain risk management Reliability Standards to provide minimum protection against supply chain attack vectors.

48. No commenter disagreed with the NOPR that misoperation or unavailability of EACMS that support a given BES Cyber System could contribute to the misoperation of the BES Cyber System or render it unavailable, which could pose a significant risk to reliable operation. Instead, commenters generally agree that EACMS perform important security-related functions.[70] For example, NERC states that a compromised firewall "may allow unfettered access to the ESP."[71] EEI also agrees that the compromise of certain EACMS that control access could adversely affect the reliable operation of an associated BES Cyber System, although EEI asserts that other CIP Reliability Standards adequately protect those EACMS.[72] Although some commenters, as discussed below, maintain that the reliability benefit of including EACMS in the supply chain risk management Reliability Standards is outweighed by the perceived costs, these commenters do not challenge the proposition that misoperation or unavailability of EACMS has negative reliability ramifications. For example, ITC, while opposing the NOPR directive, recognizes that misoperation of an EACMS is "serious" and "[w]ere

[70] *See* NERC Comments at 5-6, Appelbaum Comments at 5-6, APS Comments at 5, EEI Comments at 7-8, IRC Comments at 3, Idaho Power Comments at 2, MPUC Comments at 6.

[71] NERC Comments at 5.

[72] EEI Comments at 7-8.

CIP resources infinite, it would no doubt increase BES reliability by some degree to include EACMS within this Standard."[73]

49. We disagree with the comments asserting that existing CIP Reliability Standards adequately protect EACMS against supply chain-based threats. While existing CIP Reliability Standards include requirements that address aspects of supply chain risk management, existing Reliability Standards do not adequately protect EACMS based on the four security objectives in Order No. 829.[74] The CIP Reliability Standards cited by EEI, MISO TOs and AECC address aspects of electronic access control, systems security management, and configuration monitoring, but they do not address protection from supply chain threats such as insertion of counterfeits or malicious software, unauthorized production, tampering, or theft, as well as poor manufacturing and development practices. By contrast, the supply chain risk management Reliability Standards approved in this final rule specifically address the above listed supply chain threats, and, we determine, should be extended to at least some subset of EACMS.

50. Specifically, the goal of the supply chain risk management Reliability Standards is "to help ensure that responsible entities establish organizationally-defined processes that integrate a cybersecurity risk management framework into the system development life cycle."[75] The current CIP Reliability Standards identified in the comments, however, do not adequately address supply chain risks. For example, while Reliability Standard

---

[73] ITC Comments at 5.

[74] Order No. 829, 156 FERC ¶ 61,050 at P 71.

[75] NERC Comments at 23.

CIP-005-5 provides a level of electronic access protection for an ESP through controls applied to an Electronic Access Point associated with an EACMS, those controls would only apply after an asset is procured and deployed on a responsible entity's system. In this situation, the EACMS at issue could already contain built-in vulnerabilities making it susceptible to compromise or, in the worst-case scenario, could have been compromised before acquisition.

51. Given the documented risks to the cyber posture of the bulk electric system associated with EACMS, we are not persuaded to await the completion of the BOT-directed final report before issuing a directive regarding EACMS.[76] Instead, it is reasonable to initiate modification of the supply chain risk management Reliability Standards based on the conclusion that at least some categories of EACMS should be included. As discussed above, we are convinced that EACMS in general are a known risk that should be protected under the supply chain risk management Reliability Standards. But we leave it to the standard drafting team to assess the various types of EACMS and their associated levels of risk. We are confident that the standard drafting team will be able to develop modifications that include only those EACMS whose compromise by way of the cybersecurity supply chain can affect the reliable operation of high and medium impact BES Cyber Systems. While it will no doubt inform the standard drafting team's work, the BOT-directed final report is not, in our view, likely to alter the

[76] *See* NERC Comments at 4-6, EEI Comments at 7-10, IRC Comments at 3, ITC Comments at 5, Trade Associations at 8-12, MISO TOs Comments at 16-18.

conclusion that at least some EACMS functions should be included in the supply chain risk management Reliability Standards.[77]

52. The record does not support delaying a directive to modify the CIP Reliability Standards to include EACMS. While commenters opposing the NOPR proposal contend that the Commission should not act until NERC has the results of the BOT-directed final report, we note that: (1) NERC will have 24 months from the effective date of this final rule to develop and submit the modified Reliability Standards; and (2) the BOT-directed final report is due in the near term (i.e., February 2019). Nothing in our directive prevents the standard drafting team from using the findings in the BOT-directed final report to refine its understanding of which types of EACMS functions present the greatest risk and are worthy of inclusion in the supply chain risk management Reliability Standards. Indeed, as discussed below, in view of the BOT-directed study and the Commission's guidance, the standard drafting team could modify the supply chain risk management Reliability Standards to include an appropriate subset of EACMS functions similar to the approach in Order No. 848.[78]

53. As we have indicated above, including EACMS within the scope of the supply chain risk management Reliability Standards is consistent with the approach in Order No. 848 regarding cybersecurity incident reporting. In Order No. 848, the Commission

[77] The BOT-directed interim report provides the example of a situation where a firewall used to protect BES Cyber Systems within an ESP was compromised due to supply chain vulnerability, noting that each system within the ESP could be exposed due to its logical proximity to the compromised firewalls. NERC Interim Report at 4-4.

[78] Order No. 848, 164 FERC ¶ 61,033 at PP 53-54.

determined that EACMS that perform certain functions are significant to bulk electric system reliability so as to justify their being within the scope of the cybersecurity incident reporting Reliability Standards. Specifically, Order No. 848 addressed the identification of EACMS that should be subject to mandatory reporting requirements:

> With regard to identifying EACMS for reporting purposes, NERC's reporting threshold should encompass the functions that various electronic access control and monitoring technologies provide. Those functions must include, at a minimum: (1) authentication; (2) monitoring and logging; (3) access control; (4) interactive remote access; and (5) alerting.[79]

54. As with cybersecurity incident reporting, in the context of this proceeding, if, for example, a vulnerability in the supply chain for EACMS is found, we determine that responsible entities should have processes in place to be notified of such vulnerabilities by the vendor, as required by Reliability Standard CIP-013-1, Requirement R1.2.4. We recognize that including EACMS within the scope of the supply chain risk management Reliability Standards will impose a burden on responsible entities. Nonetheless, the burden of possible procurement inefficiencies or resource constraints must be weighed against the significant risk of a cyber incident resulting from unmitigated supply chain vulnerabilities.[80]

55. It is also important to consider that in Order No. 848 the Commission determined that the modified reporting Reliability Standard need not include all EACMS as currently

[79] *Id.* P 54.

[80] EEI Comments at 9, MISO TOs Comments at 16-17, ITC Comments at 5.

defined and, instead, the standard drafting team may analyze the matter to determine an appropriate subset of EACMS for reporting purposes.[81] Likewise, the standard drafting team that is formed in response to our present directive may determine, based on the work done in response to Order No. 848 as well as the results of the BOT-directed study, what EACMS functions are most important to the reliable operation of the Bulk-Power System and therefore should be included in the supply chain risk management Reliability Standards.

56. We find the remaining objections to our directive unpersuasive. BES Cyber Systems rely on EACMS to enable and secure the communications capability that these systems depend on to control their assigned portion of the bulk electric system. Commenters opposing the NOPR directive fail to provide convincing examples of why EACMS should not receive the same level of protection as the BES Cyber Systems with which they are associated. In addition, contrary to EEI's assertion that the "likelihood of compromise" is unclear, ample evidence exists that supply chain vulnerabilities are an active issue for vendors, whom malicious parties have intentionally targeted.[82] By contrast, commenters supporting the NOPR directive provided examples where notable vendors of EACMS functions announced vulnerabilities, specifically in firewall firmware.[83] Reliability Standard CIP-013-1, Requirement R1, Part 1.2.1, when applied to

[81] Order No. 848, 164 FERC ¶ 61,033 at P 53.

[82] EEI Comments at 8-9.

[83] Resilient Societies Comments at 3 (noting a February 2016 Cisco "critical" security advisory on a vulnerability that could allow an unauthenticated, remote attacker

certain EACMS functions, will require that responsible entities have processes to require notification by the vendor of the discovery of such vulnerabilities, representing a clear enhancement of the protections provided by the CIP Reliability Standards.

57. Although some commenters question the importance of the EACMS monitoring function, we note that these systems work in concert with access control systems to alert of possible intrusion.[84] Standard monitoring systems such as intrusion detection systems are an essential component designed to recognize suspicious activity and collect data used for incident reporting. A compromised intrusion detection system may provide false information and generate false alarms. Indeed, a compromised intrusion detection system may not only negate the value of the reported information, but could also potentially provide misleading information. Various intrusion detection system modules collect user logs, provide audit trails and indicate whether suspicious activity is malicious or normal. An attacker could change the various settings, removing or inserting false information. A compromised intrusion detection system may also allow the attacker to manipulate the system continuously without generating an alarm. In addition, an attacker may alter the compromised system such that it will deny legitimate activity and accept malicious activity.[85]

---

to obtain full control of its Industrial Security Appliance line of firewalls, and a December 2015 Juniper "out-of-cycle security advisory" on unauthorized code identified in a specific operating system that could allow an attacker to access some firewalls).

[84] EEI Comments at 7, APS Comments at 3-5, MISO TOs Comments 17-18.

[85] International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1/2, March 2016, Cyber Attacks on Intrusion Detection Systems at P 195, http://aircconline.com/ijist/V6N2/6216ijist20.pdf.

58. For the reasons discussed above, we adopt the NOPR proposal and, pursuant to section 215(d)(5) of the FPA, 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. We direct NERC to submit the directed modifications within 24 months of the effective date of this final rule.

B. Study of PACS and PCAs in the BOT-Directed Cybersecurity Supply Chain Risk Study

1. NOPR

59. The NOPR stated that it would be appropriate to await the findings from the BOT-directed study on cybersecurity supply chain risks before considering whether low impact BES Cyber Systems should be addressed in the supply chain risk management Reliability Standards. The NOPR explained that the BOT resolutions stated that the BOT-directed study should examine the risks posed by low impact BES Cyber Systems, but the BOT resolutions did not identify PACS and PCAs as subjects of the study. The NOPR noted, however, that NERC's petition suggests that NERC will evaluate PACS and PCAs as part of the BOT-directed study.[86]

60. The NOPR proposed to direct that NERC, consistent with the representation made in NERC's petition, include PACS and PCAs in the BOT-directed study and to await the

[86] NOPR, 162 FERC ¶ 61,044 at P 27 (citing 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")).

findings of the study's final report before considering further action. The NOPR indicated that the risks posed by EACMS also apply to varying degrees to PACS and PCAs. However, the NOPR explained the distinction between EACMS and the other Cyber Assets: for example, a compromise of a PACS through the supply chain, which would potentially grant an attacker physical access to a BES Cyber System or PCA, is more difficult since it would also require physical access. Physical access is not required to take advantage of a compromised EACMS. Accordingly, the NOPR proposed immediate action to provide for the protection of EACMS, because they represent the most likely route an attacker would take to access a BES Cyber System or PCA within an ESP, while possible action on other Cyber Assets can await completion of the BOT-directed study's final report.[87]

61. In addition to proposing to direct NERC to include PACS and PCAs in the BOT-directed study, the NOPR proposed to direct that NERC file the study's interim and final reports with the Commission upon their completion.[88]

2. Comments

62. NERC concurs with the NOPR proposal and states that the Commission should "await the results of the Board-requested study before considering whether low impact BES Cyber Systems, PACS, and PCAs should be addressed in the proposed Reliability

[87] NOPR, 162 FERC ¶ 61,044 at P 42.

[88] *Id.* P 43.

Standards."[89] NERC maintains that the BOT-directed report will help determine whether the supply chain risk management Reliability Standards are appropriately scoped to mitigate the risks identified by the Commission.[90]

63. EEI and Trade Associations support the supply chain risk management Reliability Standards' exclusion of low impact BES Cyber Systems. EEI agrees with the NOPR proposal to wait for NERC to study the supply chain risks posed by low impact BES Cyber Systems as well as PACS and PCAs before directing further modifications.[91] Trade Associations also "strongly support" limiting the supply chain risk management Reliability Standards' applicability to medium and high impact BES Cyber Systems.[92]

64. Other commenters contend that low impact BES Cyber Systems pose a significant risk and disagree with the view that excluding such assets will focus industry resources on protecting systems with heightened risk, while not being overly burdensome. For example, Resilient Societies maintains that cyber attackers could use low impact BES Cyber Systems as network entry points to attack high and medium impact BES Cyber Systems, with a potential coordinated cyberattack on multiple low impact facilities causing a cascading collapse.[93] Similarly, Appelbaum asserts that "if a large number of [low impact BES Cyber Systems] are compromised, then the effort to correct or replace

---

[89] NERC Comments at 4.

[90] *Id.* at 5.

[91] EEI Comments at 3.

[92] Trade Associations Comments at 7.

[93] Resilient Societies Comments at 3-4.

the compromised assets could be significant."[94] Reclamation also recommends including low impact BES Cyber Systems in the proposed Reliability Standards in order to avoid gaps that could compromise bulk electric system security.[95]

65. MPUC states that many of the concerns identified in the NOPR apply to all classifications of BES Cyber Systems and that responsible entities should be required to apply the supply chain risk management Reliability Standards to all BES Cyber System assets, unless the entities can show the assets in question to be completely isolated.[96] Reclamation has similar concerns and states that the supply chain risk management Reliability Standards should apply to all BES Cyber System impact ratings, including low impact.[97] Mabee cautions against giving industry the discretion to determine which cyber systems are "easy" to protect and which are "burdensome" to protect.[98] Isologic also disagrees with the exclusion of low impact BES Cyber Systems and contends that awaiting the BOT-directed final report would unduly delay an examination by the Commission of risks involving the "massive array of unprotected [low impact] transmission substations."[99]

---

[94] Appelbaum Comments at 6.

[95] Reclamation Comments at 1.

[96] MPUC Comments at 6.

[97] Reclamation Comments at 1.

[98] Mabee Comments at 4.

[99] Isologic Comments at 5.

3. Commission Determination

66. We accept NERC's commitment to evaluate the cybersecurity supply chain risks presented by low impact BES Cyber Systems, PACS, and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT. In light of that commitment, we conclude it is not necessary to separately direct that NERC expand the scope of the BOT-directed study. However, we adopt the NOPR proposal to direct NERC to file the BOT-directed study's final report with the Commission upon its completion.

67. We continue to believe that it is appropriate to await the findings from the BOT-directed final report on cybersecurity risks before considering whether low impact BES Cyber Systems, PACS and PCAs should be addressed in modified supply chain risk management Reliability Standards.[100] While we do not prejudge the findings from the forthcoming final report, at this time we find that NERC is taking adequate and timely steps to study whether low impact BES Cyber Systems, PACS and PCAs should be included in the supply chain risk management Reliability Standards. Given that the BOT-directed final report is scheduled to be completed in February 2019, we do not view our determination as unduly delaying consideration of this important issue. Once NERC submits the BOT-directed final report, the Commission will be in a better position to consider what further steps, if any, should be taken to provide for the reliability of the bulk electric system.

[100] NOPR, 162 FERC ¶ 61,044 at P 40.

C. Implementation Plan

1. NOPR

68. The NOPR stated that the 18-month implementation period proposed by NERC may not be justified based on the anticipated effort required to develop and implement a supply chain risk management plan. The NOPR explained that while, according to NERC, 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," the security objectives of the proposed Reliability Standards are process-based and do not prescribe technology that might justify an extended implementation period.[101] Accordingly, the NOPR proposed to reduce the time for implementation such that the supply chain risk management Reliability Standards would become effective the first day of the first calendar quarter that is 12 months, as opposed to NERC's 18 months, following the effective date of a Commission order approving the Reliability Standards.

2. Comments

69. NERC does not support the NOPR proposal to reduce the implementation period for the supply chain risk management Reliability Standards to 12 months. NERC states that the proposed 18-month implementation period is intended to give responsible entities adequate time to develop and implement a supply chain risk management plan required

[101] NOPR, 162 FERC ¶ 61,044 at P 44 (citing NERC Petition at 35).

under proposed Reliability Standard CIP-013-1, as well as to implement new controls required under proposed Reliability Standards CIP-005-6 and CIP-010-3. NERC explains that although proposed Reliability Standard CIP-013-1 is process-based, the development and implementation of the underlying Reliability Standard requirements "involves performing a complex risk assessment process for planning and procuring BES Cyber Systems."[102]

70. Other commenters support NERC's proposed 18-month implementation period and contend that 12 months is not enough time for responsible entities to develop and implement the plan and controls required under the supply chain risk management Reliability Standards. EEI, Idaho Power, IRSC, MISO TOs, and Trade Associations contend that while the Commission is correct that the requirements in the Reliability Standards are process-based, certain requirements will require technology enhancements, as well as coordination with vendors.[103] For example, Trade Associations state that Reliability Standard CIP-005-6 will require work with vendors to facilitate the ability to disable vendor remote access, while Reliability Standard CIP-010-3 will also require technology upgrades.[104] APS does not agree with the NOPR's assessment that a 12-month implementation period is reasonable, noting the potential need for new

[102] NERC Comments at 7.

[103] *See* EEI Comments at 3-4, Idaho Power Comments at 3-4, IRC Comments at 4, Trade Associations Comments at 12-13.

[104] Trade Associations Comments at 12-13 (citing NOPR, 152 FERC ¶ 61,054 at P 44).

technology and the limitations imposed by capital budget and planning cycles.[105] ITC and MISO TOs argue that the Commission does not have the legal authority to modify the implementation period unilaterally for a proposed Reliability Standard.

71. Appelbaum supports a shortened implementation period for proposed Reliability Standards CIP-010-3 and CIP-005-6, for the reasons stated in the NOPR, but contends that an 18-month implementation period for proposed Reliability Standard CIP-013-1 is more appropriate. Specifically, Appelbaum notes that the proposed Reliability Standard includes new risk planning and documentation requirements that will take time to implement. Appelbaum also contends that the risk assessment will likely involve multiple vendors and various different assets. Appelbaum states that an 18-month implementation period would provide the time to develop a supply chain risk management policy and associated processes, and then apply the processes to current and future procurement activities.[106]

3. Commission Determination

72. We do not adopt the NOPR proposal to reduce the implementation period and instead approve the implementation plan and effective date as proposed by NERC. The NOPR proposal was largely based on the premise that the security objectives of the supply chain risk management Reliability Standards are process-based and do not prescribe technology that might justify a longer implementation period. However, based

[105] APS Comments at 5-7.

[106] Appelbaum Comments at 4.

on the comments, we are persuaded that technical upgrades are likely necessary to meet the security objectives of the supply chain risk management Reliability Standards, which could involve longer time-horizon capital budgets and planning cycles.

73. While the Commission could, as Appelbaum suggests, direct an 18-month implementation period for Reliability Standard CIP-013-1 and a 12-month period for Reliability Standards CIP-005-6 and CIP-010-3, we conclude that different timelines could complicate implementation and potentially increase the administrative burden of implementation without a commensurate improvement in security.

74. Based on the discussion above, we do not adopt the NOPR proposal and approve NERC's proposed implementation plan whereby the supply chain risk management Reliability Standards will be effective on the first day of the first calendar quarter that is 18 months following the effective date of this final rule.

D. Other Issues

1. Comments

75. Certain commenters raised additional issues not addressed in the NOPR. MISO TOs, APS, and Trade Associations request clarification regarding the term "vendor." Specifically, APS seeks clarification of the definition of "vendor" and on the applicability of Reliability Standard CIP-013-1 to those vendors that would only provide services associated with a BES Cyber System that is already procured and in service.[107] APS also

[107] APS Comments at 9-11.

seeks clarification on whether responsible entities are required to perform individualized vendor assessments for every in-scope procurement activity.[108]

76. MISO TOs contend that the Commission should clarify that the supply chain risk management Reliability Standards do not apply to vendors and that responsible entities will not be responsible for vendor noncompliance. MISO TOs also request that the Commission clarify that responsible entities do not have any obligation to work only with compliant vendors.[109]

77. APS also seeks clarification regarding the scope of access intended within the term "system-to-system access."[110] As an example, APS asserts that, although there is a connection, User Datagram Protocol would not qualify as "system-to-system access" and seeks clarification regarding the scope of connections that would qualify as "system-to-system access."[111]

2. Commission Determination

78. The Supplemental Materials for Reliability Standard CIP-013-1 explain the meaning of the term "vendor." Specifically, the Supplemental Materials state that a vendor "is limited to those persons, companies, or other organizations with whom the [r]esponsible [e]ntity, or its affiliates, contracts with to supply BES Cyber Systems and

---

[108] *Id*.

[109] MISO TOs Comments at 7-9.

[110] APS Comments at 9-11.

[111] *Id.*

related services."[112] The Supplemental Materials also note that a vendor, for purposes of the supply chain risk management Reliability Standards, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.[113]

79. With regard to vendor-related compliance concerns, vendors are not subject to the supply chain risk management Reliability Standards. As NERC explains, "the proposed Reliability Standards apply only to registered entities and do not directly impose obligations on suppliers, vendors or other entities that provide products or services to registered entities."[114] This is consistent with the Commission's guidance in Order No. 829 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.'"[115]

80. As to the question of responsible entity liability for vendor noncompliance, NERC explains that "any resulting obligation that a supplier, vendor or other entity accepts in providing products or services to the registered entity is a contractual matter between the

[112] Reliability Standard CIP-013-1 at 12.

[113] *Id.*

[114] NERC Petition at 14.

[115] Order No. 829, 156 FERC ¶ 61,050 at P 21.

registered entity and the third party outside the scope of the proposed Reliability Standard[.]"[116] The security objective of the supply chain risk management Reliability Standards is to "ensure that [r]esponsible [e]ntities consider the security, integrity, quality, and resilience of the supply chain, and take appropriate mitigating action when procuring BES Cyber Systems to address threats and vulnerabilities in the supply chain."[117] Therefore, while a responsible entity is not directly liable for vendor actions, the responsible entity is required to mitigate any resulting risks. Finally, the supply chain risk management Reliability Standards do not dictate a responsible entity's contracting decision.

81. As to the term "system-to-system," NERC explains that the objective of Reliability Standard CIP-005-6, Requirement R2.4 is for entities to have visibility of active vendor remote access sessions, including Interactive Remote Access and system-to-system remote access, taking place on their system.[118] Reliability Standard CIP-005-6 requires entities to have a method to determine all active vendor remote access sessions.[119]

[116] NERC Petition at 17.

[117] *Id.* at 13.

[118] *Id.* at 31.

[119] *See* Reliability Standard CIP-005-6 at 28.

III. Information Collection Statement

82. The FERC-725B information collection requirements contained in this Final Rule are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.[120] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[121] 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. In the NOPR, the Commission solicited 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. The Commission did not receive any comments on the specific burden estimates discussed below.

83. The Commission bases its paperwork burden estimates on the changes in paperwork burden presented by the approved CIP Reliability Standard CIP-013-1 and the approved 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,

[120] 44 U.S.C. 3507(d).

[121] 5 CFR 1320.11.

respectively. As discussed above, the final rule addresses several areas of the CIP Reliability Standards through 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.

84. Separately, 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. 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. 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.

85. 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 the approved 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 Final Rule (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[122] (4)**	**Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)**	**Cost per Respondent ($) (5)÷(1)**
Create supply chain risk management plan (one-time)[123] (CIP-013-1 R1)	288	1	288	546 hrs.; $44,226	157,248 hrs.; $12,737,088	$44,226

[122] The loaded hourly wage figure (includes benefits) is based on the average of the occupational categories for 2017 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): $61.55

Computer and Information Systems Managers (Occupation Code: 11-3021): $96.51

Management (Occupation Code: 11-0000): $94.28

Electrical Engineer (Occupation Code: 17-2071): $66.90

Management Analyst (Code: 43-0000): $63.32

These various occupational categories are weighted as follows: [($94.28)(.10) + ($61.55)(.315) + ($66.90)(.02) + ($143.68)(.15) + ($96.51)(.10) + ($63.32)(.315)] = $81.30. The figure is rounded to $81.00 for use in calculating wage figures in this Final Rule.

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

Updates and reviews of supply chain risk management plan (ongoing)[124] (CIP-013-1 R2)	288	1	288	30 hrs.; $2,430	8,640 hrs.; $699,840	$2,430
Develop Procedures to update remote access requirements (one time) (CIP-005-6 R1-R4)	288	1	288	50 hrs.; $4,050	14,400 hrs.; $1,166,400	$4,050
Develop procedures for software integrity and authenticity requirements (one time) (CIP-010-3 R1-R4)	288	1	288	50 hrs.; $4,050	14,400 hrs.; $1,166,400	$4,050
TOTAL (one-time)			**864**		**186,048 hrs.; $15,069,888**	
TOTAL (ongoing)			**288**		**8,640 hrs.; $699,840**	

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.

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

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

- Year 1: $15,069,888
- Years 2 and beyond: $699,840
- 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 supply chain risk management plan and modifying it as necessary on a 15-month basis.

87. Title: FERC-725B (Mandatory Reliability Standards, Revised Critical Infrastructure Protection Reliability Standards).

Action: Information Collection, FERC-725B (Supply Chain Risk Management Reliability Standards).

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 final rule approves the requested modifications to Reliability Standards pertaining to critical infrastructure protection. As discussed above, the Commission approves NERC's 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 cybersecurity CIP Reliability Standards.

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

88. 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].

89. 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, 725 17th Street, NW, 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 and OMB Control Number 1902-0248.

IV. Environmental Analysis

90. 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.[125] The Commission has categorically excluded certain

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

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

V. Regulatory Flexibility Act Analysis

91. 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.[127] The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.[128] 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).[129]

92. Reliability Standards CIP-013-1, CIP-005-6, CIP-010-3 are expected to impose an additional burden on 288 entities[130] (reliability coordinators, generator operators,

[126] 18 CFR 380.4(a)(2)(ii).

[127] 5 U.S.C. 601-12.

[128] 13 CFR 121.101.

[129] 13 CFR 121.201, Subsection 221.

[130] 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).

generator owners, interchange coordinators or authorities, transmission operators, balancing authorities, and transmission owners).

93. 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 approved modifications to Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 apply will incur one-time costs of approximately $52,326 per entity to implement the approved Reliability Standards, as well as the ongoing paperwork burden reflected in the Information Collection Statement (approximately $2,430 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 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. Document Availability

94. 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.

95. 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. 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.

VII. Effective Date and Congressional Notification

96. The final rule is effective [**INSERT DATE 60 days from publication in FEDERAL REGISTER**]. The Commission has determined that this final rule imposes no substantial effect upon either NERC or NERC registered entities[131] and, 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.

By the Commission. Chairman McIntyre was not present at the Commission Meeting held on October 18, 2018 and did not vote on this item.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

[131] 5 U.S.C 804(3)c.

Appendix
Commenters

Abbreviation	Commenter
AECC	Arkansas Electric Cooperative Corporation
Appelbaum	Jonathan Appelbaum
APS	Arizona Public Service Company
EEI	Edison Electric Institute
Idaho Power	Idaho Power Company
IRC	ISO/RTO Council
Isologic	Isologic LLC
ITC	International Transmission Company
Mabee	Michael Mabee
MISO TOs	MISO Transmission Owners
MPUC	Maine Public Utilities Commission
NERC	North American Electric Reliability Corporation
Reclamation	U.S. Bureau of Reclamation
Resilient Societies	Foundation for Resilient Societies
Trade Associations	American Public Power Association, Electricity Consumers Resource Council, Large Public Power Council, National Rural Electric Cooperative Association, and Transmission Access Policy Study Group