192 FERC ¶ 61,230

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket Nos. RM24-4-000 and RM20-19-000; Order No. 912]

Supply Chain Risk Management Reliability Standards Revisions;

Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security

(Issued September 18, 2025)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule; notice terminating proceeding.

SUMMARY: The Federal Energy Regulatory Commission (Commission) directs the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization, to develop new or modified Reliability Standards that address the sufficiency of responsible entities' supply chain risk management plans related to the identification of and response to supply chain risks. Further, the Commission directs NERC to develop modifications related to supply chain protections for protected cyber assets. This final rule also terminates a related notice of inquiry.

DATES: This rule is effective **[INSERT DATE 60 DAYS AFTER DATE OF 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

Alan Rukin (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-8502
alan.rukin@ferc.gov

SUPPLEMENTARY INFORMATION:

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: David Rosner, Chairman;
Lindsay S. See and Judy W. Chang.

Supply Chain Risk Management Reliability Standards Revisions	Docket Nos.	RM24-4-000
Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security		RM20-19-000

ORDER NO. 912

FINAL RULE

(Issued September 18, 2025)

1. Pursuant to section 215(d)(5) of the Federal Power Act (FPA),[1] the Commission directs the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), to submit new or modified Reliability Standards within 18 months of the date of issuance of this final rule that address ongoing risks to the reliability and security of the Bulk-Power System posed by gaps in the Critical Infrastructure Protection (CIP) Reliability Standards related to supply chain risk management (SCRM) (collectively, the SCRM Reliability Standards).[2] The new or

[1] 16 U.S.C 824o(d)(5); *see also* 18 CFR 39.5(f).

[2] The phrase "SCRM Reliability Standards" as used in this final rule includes Reliability Standards CIP-005-7 (Electronic Security Perimeter(s)), CIP-010-4 (Configuration Change Management and Vulnerability Assessments), and CIP-013-2 (Supply Chain Risk Management).

modified Reliability Standards must address the: (A) sufficiency of responsible entities' SCRM plans related to the identification of and response to supply chain risks, and (B) applicability of SCRM Reliability Standards to protected cyber assets (PCA).[3]

2. While the final rule largely adopts the Notice of Proposed Rulemaking's[4] (NOPR) proposals, in response to concerns raised in NOPR comments and a Commission staff-led workshop, we decline to direct NERC to require responsible entities to validate data received from vendors. However, we encourage entities to voluntarily implement this security practice as appropriate.

3. As explained in the NOPR, while the currently effective SCRM Reliability Standards provide a baseline of protection against supply chain threats, there are increasing opportunities for attacks posed by the global supply chain.[5] For example, using the global supply chain, adversaries have inserted counterfeit and malicious software, tampered with hardware, and enabled remote access. Therefore, we are taking action in this final rule to address the increasing threat environment and the need for

---

[3] 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. …" Electronic Security Perimeters are defined as "[t]he logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol." *See* NERC, *Glossary of Terms Used in NERC Reliability Standards* (July 2024), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf (NERC Glossary).

[4] *Supply Chain Risk Mgmt. Reliability Standards*, Notice of Proposed Rulemaking, 89 FR 79794 (Oct. 1, 2024), 188 FERC ¶ 61,174, at PP 12-19 (2024) (NOPR).

[5] *Id.*

improved mitigation strategies. Directing NERC to address the identified gaps in the SCRM Reliability Standards enhances the security posture of the Bulk-Power System.

I. Background

A. Section 215 of the FPA and Mandatory Reliability Standards

4. Section 215 of the FPA provides that the Commission may certify an ERO, the purpose of which is to establish and enforce Reliability Standards, which are subject to Commission review and approval. Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[6] Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[7] and subsequently certified NERC as the ERO.[8]

B. SCRM Reliability Standards

5. The supply chain refers to the sequence of processes involved in the production and distribution of, *inter alia*, industrial control system hardware, software, and services.[9]

---

[6] 16 U.S.C. 824o(e).

[7] *Rules Concerning Certification of the Elec. Reliability Org. & Procs. for the Establishment, Approval, & Enf't of Elec. Reliability Standards*, Order No. 672, 71 FR 8662 (Feb. 17, 2006), 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 71 FR 19814 (Apr. 18, 2006), 114 FERC ¶ 61,328 (2006).

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

[9] *See, e.g.*, *Revised Critical Infrastructure Prot. Reliability Standards*, Order No. 829, 81 FR 49878 (July 29, 2016), 156 FERC ¶ 61,050, at P 4 (2016) (discussing the reliability concerns posed by the supply chain).

Such supply chains are complex, globally distributed, and interconnected systems with geographically diverse routes that consist of multiple tiers of suppliers who collectively build components necessary to deliver final products to customers. Further, the origins of products or components may be intentionally or inadvertently obscured. Certain foreign suppliers may also be subject to policies or laws that compel those suppliers to covertly provide their governments with customer data, trade secrets, and intellectual property obtained by embedding spyware or other compromising software in products, parts, or services.[10] Because the supply chain is so complex, it is extremely challenging to identify, assess, and respond to risk. The various processes, practices, and methodologies used to do so are collectively referred to as supply chain risk management or SCRM. SCRM includes implementing processes, tools, or techniques that minimize adverse impacts of adversary attacks.[11]

6. The currently effective SCRM Reliability Standards provide a baseline for supply chain risk protection for high and medium impact bulk electric system (BES) Cyber

[10] *See* Office of the Dir. of Nat'l Intelligence, *Protecting Critical Supply Chains: Risks from Foreign Adversarial Exposure* (2024), https://www.dni.gov/files/NCSC/documents/supplychain/Risks_From_Foreign_Adversarial_Exposure.pdf.

[11] *See* NIST, *Computer Security Resource Center - Definition of Supply Chain Risk Management*, https://csrc.nist.gov/glossary/term/supply_chain_risk_management.

Systems[12] and various associated systems and assets as outlined in each Standard.[13] First, Reliability Standard CIP-005-7 requires responsible entities to manage electronic access to their BES Cyber Systems and requires each responsible entity to have one or more methods to determine active vendor remote access sessions and one or more methods to disable vendor remote access. Second, Reliability Standard CIP-010-4 requires responsible entities to prevent and detect unauthorized changes to their BES Cyber Systems. Finally, Reliability Standard CIP-013-2 requires each responsible entity to develop a written SCRM plan for its high and medium impact BES Cyber Systems and their associated electronic access control or monitoring systems and physical access control systems. The SCRM Reliability Standards, except for Reliability Standard CIP-005-7, do not include protections for PCAs.[14]

[12] Each BES Cyber System, per Reliability Standard CIP-002-5.1a (BES Cyber System Categorization), is designated as one of three impact categories, high, medium, or low. The purpose of categorizing BES Cyber Systems is to apply cybersecurity requirements consistently, efficiently, and commensurate with the adverse impact that loss, compromise, or misuse of those systems could have on the reliable operation of the Bulk-Power System. At a minimum, all BES Cyber Systems must be categorized as low impact. *See* NERC, *Reliability Standard CIP-002-5.1a, Attachment 1*: *Impact rating Criteria*, https://nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf.

[13] *Supply Chain Risk Mgmt. Reliability Standards*, Order No. 850, 83 FR 53992 (Oct. 26, 2018), 165 FERC ¶ 61,020 (2018); Order No 829, 156 FERC ¶ 61,050. SCRM Reliability Standards require responsible entities to develop and implement SCRM plans that include supply chain management security controls for industrial control system hardware and software, as well as services associated with Bulk-Power System operations.

[14] *See* Reliability Standard CIP-005-7, Requirements R1, R2.

7. The SCRM Reliability Standards address four security objectives: (1) software integrity and authenticity to mitigate the risk of software made more vulnerable by the insertion of unauthorized malicious code or software patches into the software; (2) vendor remote access to mitigate the risk of malicious exploitation of a software backdoor by addressing responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions; (3) information system planning and procurement to ensure that responsible entities consider the risks associated with proposed information system planning and system development actions and to provide broad programmatic safeguards to mitigate vulnerabilities inserted into Bulk-Power System software or hardware throughout their life cycle; and (4) vendor risk management and procurement controls to address the risk that entities could enter into contracts with vendors who pose significant risks to their systems, as well as the risk that products procured by a responsible entity fail to meet minimum security criteria.[15]

C. Notice of Proposed Rulemaking

8. On September 19, 2024, the Commission issued a NOPR proposing to direct NERC to develop new or modified Reliability Standards addressing the sufficiency of responsible entities' SCRM plans related to the identification of, assessment of, and response to supply chain risks and the applicability of Reliability Standards' supply chain protections to PCAs. The Commission raised concerns that gaps exist in the SCRM Reliability Standards that may lead to a responsible entity's SCRM plan being

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

insufficient to identify, assess, and respond to supply chain risks and protect against the myriad of supply chain threats.[16] Further, the Commission explained that the concern with the exclusion of PCAs from the full suite of protections offered by the SCRM Reliability Standards has grown since initially discussed in Order No. 850.[17]

9. To address these concerns, the Commission proposed to direct NERC to submit for approval new or modified Reliability Standards that address the: (A) sufficiency of responsible entities' SCRM plans related to the identification of and response to supply chain risks, and (B) applicability of SCRM Reliability Standards to protected cyber assets (PCAs). More specifically, related to the identification of supply chain risks, the Commission proposed to require NERC to establish specific timing requirements for a responsible entity to evaluate its equipment and vendors to better identify supply chain risks.[18] Second, related to the assessment of supply chain risks, the Commission proposed to direct NERC to require responsible entities to establish steps in their SCRM plans to validate the completeness and accuracy of information received from vendors during the procurement process to better inform the identification and assessment of supply chain risks associated with vendors' software, hardware, or services.[19] Third, related to the response to supply chain risks, the Commission proposed to direct NERC to

[16] NOPR, 188 FERC ¶ 61,174 at P 20.

[17] *Id.*; *see also* Order No. 850, 165 FERC ¶ 61,020, at P 2.

[18] NOPR, 188 FERC ¶ 61,174 at P 32.

[19] *Id.* P 35.

require entities to establish a process to document, track, and respond to all identified supply chain risks. Finally, the Commission proposed to require NERC to include PCAs as applicable assets in the SCRM Reliability Standards.[20] The Commission proposed that NERC submit modifications within 12 months from the effective date of a final rule, while soliciting comment on whether a longer timeline for NERC's submission is appropriate.

10. The comment period ended on December 2, 2024, and the Commission received sixteen sets of comments, including one late-filed comment. Based on comments received, the Commission subsequently held a Supply Chain Workshop (Workshop) on March 20, 2025, which focused on the validation of vendor-provided information aspect of the proposed directive and accepted supplemental comments after the Workshop between March 20, 2025 and April 11, 2025.[21] The Commission received seven sets of post-workshop comments, and posted the Workshop transcript to e-Library.

D. Notice of Inquiry

11. In September 2020, the Commission issued a Notice of Inquiry, Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security, seeking comments on the potential risks posed by the use of equipment and services provided by certain entities identified as risks to national security, particularly

[20] *Id.* P 52.

[21] *Supply Chain Risk Mgmt. Reliability Standards Workshop*, Docket No. RM24-4-000 (Mar. 20, 2025), https://www.ferc.gov/news-events/news/ferc-staff-issues-agenda-notice-workshop-supply-chain-risk-management-reliability.

communication systems and other equipment and services that are critical to bulk electric system reliability provided by Huawei Technologies Company and ZTE Corporation.[22]

II. Discussion

12. Pursuant to section 215(d)(5) of the FPA, we largely adopt the NOPR proposal and direct NERC to submit new or modified Reliability Standards that address ongoing risks to the reliability and security of the Bulk-Power System posed by gaps in the SCRM Reliability Standards. As discussed in detail below, the new or modified Reliability Standards must address the: (A) sufficiency of responsible entities' SCRM plans related to the identification of and response to supply chain risks, and (B) applicability of SCRM Reliability Standards to PCAs.[23] However, we are persuaded by the record–including comments and workshop panels–not to adopt the NOPR proposal to require that SCRM plans include steps to validate the completeness and accuracy of information received from vendors during the procurement process. Further, we modify the NOPR proposal and, instead of the proposed 12-month deadline, direct NERC to submit responsive new or modified SCRM Reliability Standards within 18 months of the issuance of this final rule.

---

[22] *Equip. & Serv. Produced or Provided by Certain Entities Identified as Risks to Nat'l Sec.*, Notice of Inquiry, 172 FERC ¶ 61,224, at PP 1, 4 (2020).

[23] 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. …" Electronic Security Perimeters are defined as "[t]he logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol." *See* NERC Glossary.

13. While the SCRM Reliability Standards provide a strong foundation of protection against supply chain threats, we remain concerned that there are gaps in the requirements of those Reliability Standards that may lead to a responsible entity's SCRM plan being insufficient to identify, assess, and respond to SCRM risks. As discussed in the NOPR, we believe that the plans required by the currently effective SCRM Reliability Standards are insufficient to protect against the myriads of supply chain threats. Further, our concern with the exclusion of PCAs from the SCRM Reliability Standards has grown since initially discussed in Order No. 850.

14. Our action in this proceeding strengthens the SCRM Reliability Standards to improve the security posture of the Bulk-Power System. Below, we address the following topics: (A) sufficiency of SCRM plans related to identification of, assessment of, and response to supply chain risks; (B) applicability of SCRM requirements to PCAs; (C) Reliability Standard development timeline; (D) other issues raised by commenters; and (E) termination of notice of inquiry.

A. Sufficiency of SCRM Plans Related to the Identification of, Assessment of, and Response to Supply Chain Risks

15. In the NOPR, the Commission proposed to direct NERC to develop and submit for Commission approval new or modified Reliability Standards that address the sufficiency of responsible entities' SCRM plans related to the identification of, assessment of, and response to supply chain risks.[24] The Commission identified that the lack of specific

[24] NOPR, 188 FERC ¶ 61,174 at P 1.

requirements related to the identification of, assessment of, and response to risk is inconsistent with generally established risk management frameworks and may lead to installation of vulnerable products and incomplete or inaccurate risk assessments.[25] Further, the Commission described multiple gaps in SCRM plans observed by Commission audit staff, as set forth in staff's 2023 Lessons Learned Report.[26]

1. Identification of Supply Chain Risks

16. In the NOPR, the Commission proposed to direct NERC to submit for approval new or modified Reliability Standards that would establish specific timing requirements for a responsible entity to evaluate its equipment and vendors to better identify supply chain risks.[27] Specifically, the Commission proposed to direct NERC to establish a maximum time frame between when an entity performs its initial risk assessment during the procurement process and when it installs the equipment.[28] The Commission stated that an entity should be required to perform an updated risk assessment prior to installation if the entity does not install the equipment or software within a specified time

[25] *Id.* P 25 (citing NIST, *Special Publication 800-37, Revision 2: Risk Management Framework for Information Systems and Organizations*, Task R-3, Risk Response 72 (Dec. 2018)), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf).

[26] *Id*. PP 26-29 (citing FERC Staff Report, *2023 Lessons Learned from Commission-led CIP Reliability Audits* 17-19 (Dec. 12, 2023), https://www.ferc.gov/sites/default/files/2023-12/23_Lessons%20Learned_1211.pdf).

[27] *Id.* P 32.

[28] *Id*.

limit and explained that the lack of such a requirement could lead to an incomplete or inaccurate risk identification that may result in risk assessments that do not reflect the actual risk posed to the responsible entity.[29] The Commission sought comment on (1) what factors should be considered when developing a time frame between the initial risk assessment and installation before entities would be required to perform a subsequent risk assessment and (2) whether the time frame should vary based on certain factors (e.g., equipment type) and the reasons for any proposed time frame variation.[30]

17. The Commission also proposed to direct NERC to establish requirements for an entity to periodically reassess risks associated with vendors, products, and services procured under a contract for supply chain risks that may have developed since the contract commenced.[31] The Commission sought comment on what factors should be considered when developing this requirement and any specific circumstances that should trigger a reassessment (e.g., merger or acquisition of an existing supplier).[32] The NOPR made clear that the Commission proposal would not require responsible entities to renegotiate or abrogate contracts.

---

[29] *Id.*

[30] *Id.*

[31] *Id.* P 33.

[32] *Id.*

a. Comments

i. Specific Timing Requirements for a Responsible Entity to Evaluate its Equipment and Vendors

18. Commenters generally support a risk-based approach in establishing requirements for performing updated risk assessments and caution against prescriptive, time-based requirements.[33] Most commenters support an approach to reassessment based upon entity-defined criteria, event-based triggers, or both.[34]

19. AWS asserts that the Commission should permit NERC to consider and propose a risk-based reassessment approach based on the type of equipment or service in question and "significant supply chain risk events such as a change in supplier ownership, geopolitical events, or new security exploits."[35] For example, BES Cyber Systems could be subject to more strenuous re-assessment requirements than PCAs.[36] AWS states that rigid, time-based reassessment time frames could fail to identify sudden changes in risk and hinder an entity's ability to prioritize higher risk equipment.[37] While AWS agrees that periodic reassessments are valuable, it supports a flexible approach defined by

[33] AWS Comments at 4; Hitachi Comments at 2; Idaho Power Comments at 2; IRC Comments at 3; New England States Committee on Electricity (NESCOE) Comments at 3.

[34] *Id.*

[35] AWS Comments at 4, 6.

[36] *Id.* at 6.

[37] *Id.* at 5-6.

responsible entities as opposed to those "rigidly defined by regulation."[38] AWS advocates that continuous monitoring of assets is a more effective approach to SCRM.[39] Similarly, Idaho Power asserts that imposing a prescriptive time frame requirement for reassessment may be problematic, reducing "the flexibility entities have over the way they incorporate SCRM requirements into their purchasing processes."[40] IRC also asserts that responsible entities are best suited to determine when and how to evaluate their risk. Further, IRC states that any directive to NERC regarding the identification of risk should allow responsible entities to establish specific timing requirements in their SCRM plans to identify supply chain risks as opposed to establishing timing requirements in a Reliability Standard.[41]

20. While Trade Associations oppose the Commission's proposed directive to establish a maximum time frame between an initial risk assessment and installation, they argue that "periodic reassessments and event-based triggers can be implemented as a reasonable alternative to address" the Commission's concerns.[42] Trade Associations believe that the requirement for a strict reassessment time frame could hinder an entity's ability to replace faulty equipment and use assets in a timely manner due to the

[38] *Id.* at 6.

[39] *Id.* at 5.

[40] Idaho Power Comments at 2.

[41] IRC Comments at 3.

[42] Trade Associations Comments at 12.

compliance risk if they are required to perform a reassessment but are unable to complete it in the required time frame.[43] Trade Associations further believe such a requirement would be unpredictable and unworkable for spare stock equipment used in the event of equipment failure.[44] On the other hand, Hitachi Energy believes that risk assessments to optimize security and resources should be performed on both new and spare equipment based on preparing that equipment for deployment rather than upon a calendar date.[45] Hitachi Energy also asserts that emergency spare equipment should be subject to risk assessments before deployment.[46]

21. Ravnitzky avers that the timing requirements for risk assessments proposed in the NOPR are not clearly justified and that a rationale for the proposed requirement, such as type of equipment, criticality of the asset, or an evolving threat landscape, would strengthen the proposed directive.[47]

ii. Periodic Requirements for Reassessment of Risks Associated with Vendor Contracts

22. Similar to the issue of timing requirements for reassessment, most commenters are supportive of an approach of periodic reassessment of vendor risks based upon entity-

[43] *Id.*

[44] *Id.*

[45] Hitachi Energy Comments at 3.

[46] *Id.*

[47] Ravnitzky Comments at 1.

defined criteria, event-based triggers, or both.[48] Trade Associations state that while they do not support a requirement for entities to perform updated risk assessments after specific time periods, they do support "the establishment of periodic reassessments of vendors based on entity-defined criteria that consider the criticality of a supplier, product, or service to their organization and circumstances," including mergers and acquisitions of, or notification of, security events associated with existing vendors.[49] Trade Associations explain that this approach provides flexibility to allow entities to define criteria aligning with their own security philosophy in a risk-based and prioritized manner.[50]

23. AWS asks the Commission to allow NERC to develop a reassessment approach to review existing contracts with vendors based on "triggering events such as changes in supplier ownership, changes in a device's country of origin, or identification of new security exploits."[51] Regarding the factors to be considered in developing a requirement for reassessing supply chain risks associated with existing contracts with vendors, Idaho Power recommends entities consider whether security concerns exist or there have been breaches of a supplier's system, significant technology advancements, and the expiration

[48] AWS Comments at 6-7; Trade Association Comments at 12; Idaho Power Comments at 2; IRC Comments at 3; NESCOE Comments at 3.

[49] Trade Associations Comments at 11.

[50] *Id.*

[51] AWS Comments at 7.

or renewal of a vendor agreement.[52] Likewise, IRC cautions against a one-size-fits-all mandate and recommends that the maximum time frame between a risk assessment and contract implementation be determined on a case-by-case basis.[53]

24. Bonneville supports a 36-month time frame between an initial risk assessment and subsequent reassessment in instances in which a vendor has not changed.[54] Bonneville asserts that while a shorter time frame for reassessment may be necessary in certain circumstances such as a change in vendor, known risk factors, or mergers and acquisitions involving a vendor, a shorter time frame in the absence of such circumstances would be too burdensome.[55]

25. Trade Associations understand that the Commission did not propose to require entities to abrogate or renegotiate contracts with vendors, suppliers, or other entities but express their concern that it is unclear what actions an entity could or would be expected to take based on a periodic reassessment performed during an existing contract or how an entity could compel a vendor response to a reassessment within a certain timeframe.[56] Trade Associations state that finding a new vendor or renegotiating contracts due to a

[52] Idaho Power Comments at 2.

[53] IRC Comments at 3.

[54] Bonneville Comments at 2.

[55] Bonneville Comments at 2.

[56] Trade Associations Comments at 11-12

periodic risk assessment or lack of vendor response is often infeasible.[57] Ravnitzky, on the other hand, recommends that proposed directive should include requirements for reviewing and updating existing contracts, including legacy risks.[58]

b. Commission Determination

26. Pursuant to FPA section 215(d)(5), we adopt the NOPR proposal and direct NERC to develop and submit for Commission approval new or modified Reliability Standards that would establish specific timing requirements for a responsible entity to evaluate its equipment and vendors to better identify supply chain risks. We find that the lack of specific requirements in the SCRM Reliability Standards as to when in the procurement and deployment process an entity must apply its SCRM plan to identify supply chain risks can lead to incomplete or inaccurate risk identification, resulting in risk assessments that do not reflect the actual threat posed to the responsible entity. To satisfy these directives, NERC should establish (1) a maximum time frame between when an entity performs its initial risk assessment during the procurement process and when it installs the equipment and (2) periodic requirements for an entity to reassess the risk associated with vendors, products, and services procured under any contracts for supply chain risks that may have developed or changed since the contract commenced.

27. The SCRM Reliability Standards currently do not require a responsible entity to perform a reassessment of its equipment before installation, regardless of when that

[57] *Id.* at 11.

[58] Ravnitzky Comments at 2.

equipment was procured. While many of the commenters support a risk-based approach to reassessment based upon entity-defined criteria and/or event-based triggers as opposed to a time-based requirement, we believe that the directive can and should accommodate both approaches. We agree with commenters that entities are best positioned to understand their own risk and determine when equipment should be reassessed.[59] We also agree that the results of entity-defined criteria being incorporated into SCRM plans and implemented to reassess equipment in a risk-based manner will likely be more effective at identifying risk than a calendar-based reassessment.[60] As such, we encourage NERC and stakeholders to consider the comments submitted in this docket during the standard development process.

28. We believe, however, that a *maximum* time frame must be established that requires responsible entities to determine whether their risk assessment is still sound after the established time frame prior to installation in the event that entities' own SCRM plans are not triggered to reassess the equipment during that period. A maximum time frame for a risk assessment represents a backstop, outer limit by which responsible entities must reassess risk. As commenters suggest, there are ample reasons to perform more frequent

[59] *See, e.g.*, AWS Comments at 6-7; Idaho Power Comments at 2; IRC Comments at 3, and Trade Associations Comments at 12 (advocating for flexible approaches in which responsible entities evaluate their own risk and develop reassessment criteria prior to installation based on equipment type, criticality, vendor source, etc.). *See also* Hitachi Energy Comments at 3 (supporting an approach in which the reassessment of equipment is linked to project developments such as deployment as opposed to calendar dates).

[60] *See* Hitachi Energy Comments at 3.

risk assessments, i.e., on a periodic, event-, and project-based basis.[61] We believe a maximum time frame will ensure that all equipment is reassessed and reduce the opportunities for supply chain risks being inadvertently missed prior to deploying or installing that equipment. If a responsible entity does perform a reassessment during the period based on its own criteria defined by its SCRM plan (e.g., prior to installation, criticality of the asset), NERC could determine through the standard development process that such assessment would restart the clock as to when an entity would be required by the Reliability Standard to perform a subsequent time-based reassessment.

29. We clarify that our directive here already includes reassessment of spare equipment and emergency repairs. While Hitachi Energy believes that emergency spare equipment should be subject to risk assessments prior to deployment, Trade Associations are concerned that such a requirement would be unpredictable and unworkable for spare stock equipment used in the event of equipment failure.[62] While we appreciate the Trade Associations' concern, we do not believe that this directive would hinder a responsible entity's ability to ensure reliable operation of the Bulk-Power System. However, we encourage interested parties to participate in NERC's standard development process regarding this matter.

---

[61] For instance, if an organization refreshes its information technology equipment (e.g., workstations, network equipment) on a three-year cycle, a mandatory reassessment after two years, may give that organization sufficient time to assess any emergent risk that may influence whether it wants to use that vendor and equipment or next version of that equipment.

[62] Hitachi Energy Comments at 3; Trade Associations Comments at 12.

30. Further, we note Bonneville's concerns that a risk identification period requiring registered entities to perform risk assessments more frequently than every 36 months without extenuating circumstances may be burdensome. As discussed above, while we direct NERC to develop a maximum period for entities to update their risk assessment, we do not specify the appropriate periodicity, and we encourage interested parties to raise these concerns during the standard drafting process. We also note that, in developing the maximum time frame for reassessments, NERC may find it appropriate to tailor the periodicity of risk assessments according to equipment type (i.e. require different periodicities for workstations, servers, networking and security appliances, energy management systems, and substation equipment) because each type may have different cycles for risk re-assessments.

31. Regarding Trade Associations' concerns about how entities would comply with a requirement to periodically review risks associated with existing contracts, we clarify that if a responsible entity discovers a supply chain risk associated with an existing contract, the directive would not require a specific response from the entity. Rather, the responsible entity would respond to the identified risk in a manner consistent with its established SCRM plan, which would include documenting and tracking the risk, at minimum. As such, consistent with Order Nos. 829 and 850, we decline to require entities to update or renegotiate existing contracts as recommended by Ravnitzky.

32. For the reasons discussed above, pursuant to FPA section 215(d)(5), we direct NERC to develop new or modified Reliability Standards that establish a maximum time frame between when a responsible entity performs its initial vendor and equipment risk

assessment during the procurement process and when it deploys the equipment. If a responsible entity does not deploy the equipment or software within the specified time limit, the new or modified Reliability Standard should require responsible entities to perform an updated risk assessment prior to deployment.

2. Assessment of Supply Chain Risks and Validation of Vendor Information

33. In the NOPR, the Commission proposed to direct NERC to submit for approval new or modified Reliability Standards that require responsible entities to establish steps in their SCRM plans to validate the completeness and accuracy of information received from vendors during the procurement process to better inform the identification and assessment of supply chain risks associated with vendors' software, hardware, or services.[63] The Commission discussed its concern that a responsible entity's failure to take any steps to validate a vendor's information could lead to the entity failing to properly identify or assess risks posed by that vendor, installing vulnerable products that could compromise the entity's systems, or performing a risk assessment based on inaccurate or incomplete information.[64] The Commission sought comments on the steps an entity could take to validate data provided by vendors and how burdensome those steps might be.[65]

---

[63] NOPR,188 FERC ¶ 61,174 at P 35.

[64] *Id.* P 37.

[65] *Id.*

a. Comments

34. Comments were split between those who support,[66] do not oppose,[67] or oppose[68] the proposal. Based on the concerns raised about the proposed validation directive by commenters, Commission staff and NERC staff jointly held a Supply Chain Workshop, discussed below, to elicit feedback on the proposed directive.[69]

35. While AWS supports the proposed directive, it urges the Commission to grant NERC flexibility in the standard drafting process to avoid a one-size-fits-all approach.[70] AWS recommends that the Commission move forward with its proposed directive and "direct NERC to leverage the value, effectiveness, and efficiency" of existing third-party certifications that can provide cost-effective security controls to support SCRM objectives and streamline vendor validation processes.[71]

36. While not opposed to the proposed directive, IRC "cautions that validation of documentation provided by vendors for the purpose of evaluating supply chain risk is difficult and potentially cost prohibitive" and highlights established vendor validation

---

[66] AWS Comments at 3; Bonneville Comments at 2; NERC Comments at 1, 5; NESCOE Comments at 3.

[67] Idaho Power Comments at 1; IRC Comments at 4-6; Ravnitzky Comments at 1.

[68] Public Power Utilities Comments at 2; Trade Associations at 13-15; TAPS Comments at 3.

[69] *See Supply Chain Risk Mgmt. Reliability Standards Workshop*, Docket No. RM24-4-000.

[70] AWS Comments at 1.

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

practices such as internal audits, third-party audits, and attestations.[72] IRC discusses challenges with each approach and urges the Commission to recognize that responsible entities are best suited to determine when and how to evaluate their risk and to balance the scope of the proposed directive with the cost of validation.[73] Proposing more specifications rather than greater flexibility, Ravnitzky recommends the Commission provide more detail as to how entities should conduct risk assessments, including specific methodologies or best practices to ensure consistency and effectiveness.[74]

37. Public Power Utilities, Trade Associations, and TAPS, on the other hand, oppose the proposed validation directive and urge the Commission not to adopt it in the final rule. Public Power Utilities acknowledge the security risks that the Commission intended to address but underscore the limitations that entities have in dealing with vendors.[75] Further, Public Power Utilities and Trade Associations express concern with the auditability of such a proposed requirement and how an entity could sufficiently demonstrate compliance. These same commenters also outline their concerns with the limitations of third-party assessments, including both cost to entities and the entities' ability to rely on the assessments provided by third parties.[76] Instead of adopting the

[72] IRC Comments at 4.

[73] *Id.* at 2, 4

[74] Ravnitzky Comments at 1.

[75] Public Power Utilities Comments at 3.

[76] *Id.* at 4. *See also* Trade Associations Comments at 13-14.

NOPR proposal, Public Power Utilities believe that the development of supplier security protocols and a NERC- or government-approved set of vendor protocols would be a more effective approach.[77] In reply comments, TAPS supports the comments filed by Public Power Utilities and agrees that a centralized approach would better accomplish the Commission's goals.[78]

b. Supply Chain Workshop Testimony

38. Based on concerns raised in comments, Commission staff convened the Workshop on March 20, 2025, focused on the NOPR proposal to require responsible entities to validate vendor-provided information. During the Workshop, panelists discussed the various challenges associated with the Commission's proposed validation directive. While acknowledging that supply chain risk is a serious threat that must be managed, a general consensus arose that a validation requirement in the Reliability Standards is not the most effective approach to mitigate the identified risks.

39. Panelists cautioned against a one-size-fits all approach and recommended adopting a risk-based approach based on entity-defined criteria instead.[79] Panelists advocated for an approach in which entities can address known cybersecurity risks and prioritize meaningful threats while balancing against other business concerns unique to their

[77] *Id.*

[78] TAPS Reply Comments at 3.

[79] Tr. 12:25-13:12 (Cancel); Tr. 41:7-14 (Jacobs); Tr. 42:3-9 (Schepis); TR. 88:21-90:10 (Fee); Tr. 92:10-94:25, 101:5-9 (Gugel). *See Transcript of the Supply Chain Risk Mgmt. Reliability Standards Workshop*, Docket No. RM24-4-000 (2025).

organization.[80] Panelists cautioned against mandatory requirements for the use of third-party questionnaires or certifications, asserting that these techniques would hinder the responsible entity's ability to respond to emerging risks and threats. Instead, panelists asserted that responsible entities might be better served by having those tools in the Reliability Standards as an option or through guidance that is not part of the Standard, which would allow for more expeditious updates to best practices.[81]

40. Additionally, several panelists discussed efforts to harmonize and centralize the type of information collected as a scalable means of validating vendor supplied information, such as through a supply chain library or other repository.[82]

c. Post-Workshop Comments

41. The majority of post-workshop commenters reiterate their opposition to the proposed validation directive and urge the Commission not to adopt it.[83] Many commenters also recommend that the Commission work with industry and other federal partners towards a more comprehensive, centrally located information-sharing solution to support registered entities in evaluating vendor risks.[84]

---

[80] Tr. 75:20-78:9 (Schneider); Tr. 80:7-81:14 (Spross).

[81] Tr. 103:2-11 (Roeder); Tr. 104:4-105:1 (Spross); Tr. 105:3-106:5 (Fee).

[82] Tr. 31:18-32:25 (Kolasky); Tr. 37:12-39:4 (Jacobs); Tr. 53:20-55:2 (Schepis); Tr. 75:20-78:9 (Schneider); Tr. 92:10-94:25 (Gugel); Tr. 108:20-109:9 (Spross).

[83] Public Power Utilities and TAPS Joint Post-Workshop Comments at 1; Trade Associations Post-Workshop Comments at 2, 3; MISO Post-Workshop Comments at 2.

[84] Public Power Utilities and TAPS Joint Post-Workshop Comments at 7-8; BCG Post-Workshop Comments at 1-2; MISO Post-Workshop Comments at 3; NEMA Post-

42. In joint comments, Public Power Utilities and TAPS reiterate their opposition to the proposed directive that would require responsible entities to validate the completeness and accuracy of information received from vendors.[85] Public Power Utilities and TAPS assert that the proposed validation requirement would be unduly costly and unmanageable.[86] Similarly, Trade Associations oppose the validation requirement and believe it would be an unreasonable burden on individual entities based on supply chain, product, and component complexity, as well as the variation in entity risk postures.[87]

43. Asset 2 Vendor Network supports the use of third-party certifications as a means to validate vendor data.[88] MISO comments that while it is generally supportive of the use of third-party audits and certifications, it does not support mandating them in the CIP Reliability Standards. Instead, MISO recommends that each entity have the flexibility to determine validation methods in a risk-based matter that would be best suited for each individual entity.[89]

Workshop Comments at 2; Trade Associations Post-Workshop Comments at 9-10.

[85] Public Power Utilities and TAPS Joint Post-Workshop Comments at 1.

[86] *Id.* at 5.

[87] Trade Associations Post-Workshop Comments at 2.

[88] Asset 2 Vendor Network Post-Workshop Comments at 1.

[89] MISO Post-Workshop Comments at 2.

d. Commission Determination

44. We decline to adopt the NOPR proposal to direct NERC to develop new or modified Reliability Standards that require entities to establish steps in their SCRM plans to validate the completeness and accuracy of information received from vendors during the procurement process. Taking into consideration both initial and post-workshop comments, as well as panelist testimony at the Workshop, we are persuaded by concerns regarding the challenges associated with the development and implementation of the proposed validation directive.

45. Commenters and panelists do not dispute the security risk posed by relying solely on vendor responses to questionnaires, or lack thereof, without further vetting the vendor, product, or service.[90] They identified, however, various concerns with the development and implementation of a validation requirement in a mandatory Reliability Standard. Commenters and panelists are primarily concerned with the auditability of such a requirement (i.e., what entities would have to show to be compliant with the Standard), the burden on entities to validate vendor information,[91] the lack of leverage that responsible entities have when dealing with vendors,[92] and the commercial readiness and

[90] *See, e.*g., Tr. 26:7-28:15 (Adams); Tr. 28:17-30:12 (Jacobs); Public Power Utilities Post-Workshop Comments at 2; Trade Associations Post-Workshop Comments at 2-3. *See generally Transcript of the Supply Chain Risk Mgmt. Reliability Standards Workshop*, Docket No. RM24-4-000.

[91] *See, e.g.*, Public Power Utilities Post-Workshop Comments at 5-6; Tr. 66:25-67:19 (Ratliff); Tr. 76:20-78:9 (Schneider).

[92] *See, e.g.*, Tr. 87:24-88:19 (Roeder); Tr. 88:21-90:10 (Fee); Tr. 90:12-92:1 (Spross).

cost of third-party audits or certifications.[93] Instead of a one-size-fits-all requirement, commenters and panelists discussed various risk-based approaches in which entities could define their own criteria and process for vendor validation based on their resources and unique risk profile.

46. While we agree with commenters and panelists that a lack of due diligence on vendor responses presents a security risk, we find the comments and testimony explaining the challenges of implementing the proposed directive persuasive. We also agree with the robust discussion regarding various risk-based, entity-defined approaches to validating vendor responses that could be implemented to mitigate SCRM risks. As such, we urge NERC to consider the filed comments and testimony in this record to mitigate the concerns which prompted this proposal as the standard drafting team works through development of responsive SCRM Reliability Standards.

47. In addition, we agree with commenters on the potential value of a centrally located information-sharing solution. We encourage NERC to consider these comments and the potential value of information-sharing solutions when developing responsive Reliability Standards.

3. Response to Supply Chain Risks

48. In the NOPR, the Commission proposed to direct NERC to ensure that new or modified Reliability Standards require entities to establish a process to document, track,

[93] *See, e.g.*, Trade Associations Post-Workshop Comments at 7; Tr. 17:16-19:19 (Jacobs).

and respond to all identified supply chain risks.[94] The Commission expressed concern that the existing SCRM Reliability Standards lack a requirement that ensures consistent, timely, and appropriately documented responses to identified supply chain risks.[95]

49. The Commission proposed that while a responsible entity can respond to risks in a variety of ways, the entity should document and track its actions, regardless of the approach taken.[96] Documentation could include identifying what controls are in place or will be put in place to manage the risk while maintaining the overall reliability of the responsible entity's BES Cyber Systems and associated BES Cyber Assets.[97] The Commission then provided several examples, including the documentation approaches taken in the National Institute of Standards and Technology (NIST) Risk Management Framework and mitigation requirements set forth in Reliability Standard CIP-007-6, Requirement R2. Finally, the Commission sought comment on whether and how a uniform documentation process could be developed to ensure entities can properly track identified risks and mitigate those risks according to the entity's specific risk assessment.[98]

---

[94] NOPR, 188 FERC ¶ 61,174 at P 38.

[95] *Id.*

[96] *Id.* P 39.

[97] *Id.*

[98] *Id.*

a. Comments

50. NERC, Bonneville, IRC, Idaho Power and NESCOE support the directive.[99] AWS urges the Commission to allow registered entities to leverage existing tools to track and mitigate identified risks under their entity-defined SCRM programs, including standardized questionnaires and third-party certifications.[100] AWS further adds that NERC and the Commission can "support standardization of SCRM by simplifying access to quality supply chain risk information most relevant to the electric sector and by clarifying compliance expectations," such as building or endorsing supply chain risk registries and guidance resources or building upon existing risk registry models.[101] Similarly, IRC supports the proposed directive but asserts that the steps entities must take to identify and mitigate risks be aligned "with an industry-accepted risk management framework of the responsible entity's choice."[102] IRC cautions that the Commission should not establish in the final rule any specific documentation that an entity must use.[103]

[99] Bonneville Comments at 3; Idaho Power Comments at 2; IRC Comments at 6; NERC Comments at 5; NESCOE Comments at 3.

[100] AWS Comments at 10-11.

[101] *Id.* at 11.

[102] IRC Comments at 6.

[103] *Id.*

51. While Trade Associations support the proposed directive, they caution that the Reliability Standard CIP-007 Requirement R2 approach the Commission discussed in the NOPR would "be difficult to replicate for SCRM-related items and therefore should not be mandated in the final rule."[104] Trade Associations identify several concerns with replicating the CIP-007 R2 approach and argue that while the scope of Requirement R2 is clearly bound to "cyber security patches for applicable Cyber Assets," the scope of the proposed directive is neither defined nor clearly bounded.[105] As such, Trade Associations request that the Commission allow the standard drafting team to refine the scope of the supply chain risks that entities must identify, track, and respond to under the proposed directive.[106]

52. Ravnitzky notes that while the NOPR described various means that an entity may respond to risks, it did not provide guidance as to how an entity should select the appropriate response.[107] As such, he suggests the Commission include in the final rule decision-making criteria to guide entities, such as severity of the risk, impact on the Bulk-Power System, and feasibility of mitigation measures.[108]

---

[104] Trade Associations Comments at 16.

[105] *Id.*

[106] *Id.* at 17.

[107] Ravnitzky Comments at 2.

[108] *Id.*

b. Commission Determination

53. Pursuant to FPA section 215(d)(5), we adopt the NOPR proposal and direct NERC to develop and submit for Commission approval new or modified Reliability Standards that require responsible entities to establish a process to document, track, and respond to all identified supply chain risks. This directive should address the Commission's concern raised in the NOPR that existing SCRM Reliability Standards are inadequate to ensure consistent, timely, and appropriately documented responses to identified vendor risks.[109] We believe that the directive will strengthen the SCRM Reliability Standards and better align them with widely accepted risk management frameworks.

54. We agree with commenters who advocate against the Commission mandating specific mechanisms that entities must use to document, track, and respond to supply chain risks. Rather, we direct that the responsive SCRM Reliability Standards require entities to include in their SCRM plans a process to document, track, and respond to identified risks. While NERC may further refine this requirement through the standards development process, we decline to be prescriptive as to how entities implement this requirement. Similarly, while we decline to mandate any decision-making criteria to guide entities in determining how to respond to identified risks as recommended by Ravnitzky, we note that NERC may consider doing so through its standards development process. We believe this approach will ensure that entities appropriately document, track,

[109] NOPR, 188 FERC ¶ 61,174 at P 38.

and respond to supply chain risks, while maintaining their flexibility to best manage their unique risk environments while improving the SCRM Reliability Standards.

55. This approach should alleviate Trade Associations' concerns about applying the approach taken in Requirement R2 of Reliability Standard CIP-007-6 to the SCRM Reliability Standards. Rather, the NOPR referenced Reliability Standard CIP-007-6, Requirement R2 as an example for consideration of a process in which a responsible entity must track, evaluate, and respond to a risk.

56. Responsible entities should assess each identified risk and existing controls to decide on the appropriate response. While the Commission provided several examples of how an entity may choose to do this, we decline to mandate a specific framework, process, or compensating controls.[110] Regardless of the severity of the risk and the actions an entity decides to take to address it, the entity must document and track those risks as they may change due to external factors (e.g., newly discovered vulnerability, or vendor organizational change), or internal factors (e.g., changes in responsible entity's asset architecture).

B. Applicability of SCRM Requirements to PCAs

57. In the NOPR, the Commission preliminarily found that PCAs receive limited protections under the existing SCRM Reliability Standards and that addressing such unprotected PCAs is necessary to maintain the reliability and security of the Bulk-Power

[110] NOPR, 188 FERC ¶ 61,174 at P 39.

System in light of evolving threats.[111] As such, the Commission proposed to direct NERC to modify the SCRM Reliability Standards to include PCAs as applicable assets.[112] Further, the Commission proposed to direct NERC to protect PCAs from supply chain risk at the same level as the BES Cyber Systems inside an electronic security perimeter.[113] The Commission sought comment on potential comprehensive and scalable approaches that could be implemented to identify and assess supply chain risks posed by PCAs, given the wide range of assets that may be categorized as PCAs.[114]

58. The Commission explained that because PCAs are ancillary equipment that reside behind a responsible entity's electronic access point within a responsible entity's electronic security perimeter, the exploitation of PCAs directly puts at risk the interconnected BES Cyber Systems housed in the same electronic security perimeter. A supply chain attack could potentially make use of a compromised PCA to bypass the electronic security perimeter to directly attack medium and high impact BES Cyber Systems within the same electronic security perimeter.

[111] *Id.* P 44 (explaining that PCAs are subject to vendor remote access protections but no other types of protections specified in the SCRM Reliability Standards).

[112] *Id.* P 52.

[113] *Id.*

[114] *Id.*

59. The Commission explained that since the 2018 issuance of Order No. 850, its concerns regarding the risks associated with PCAs have grown.[115] And that recent supply chain attacks that targeted or could have implicated PCAs, supported the preliminary findings that unprotected PCAs present a risk to the security of the Bulk-Power System. The Commission also noted in the NOPR that extending supply chain protections to PCAs is consistent with risk management practices required for federal agencies.[116]

1. Comments

60. NERC, IRC, Idaho Power, Bonneville, and NESCOE support the proposed directive to revise the SCRM Reliability Standards to include PCAs as applicable assets.[117] No commenters oppose the proposed directive. NERC states, for example, that the inclusion of PCAs in the SCRM Reliability Standards would help prevent threats or system compromises by complementing internal network security monitoring requirements.[118]

61. Ravnitzky states that the Commission in the NOPR does not clearly define the criteria as to what constitutes a PCA and that such a definition could help ensure

[115] *Id*. at 51.

[116] *Id.* at 50.

[117] Bonneville Comments at 3; Idaho Power Comments at 2; IRC Comments at 7; NERC Comments at 6; NESCOE Comments at 3.

[118] NERC Comments at 5-6.

consistent application.[119] Bonneville asserts that because PCA is already a NERC-defined term, adding that term to the requirements of Reliability Standard CIP-013 would accomplish the directive's goal.[120] Bonneville also asserts that it is appropriate to apply SCRM Reliability Standards protections to all PCAs associated with medium and high impact BES Cyber Systems without exception.[121]

62. Secure the Grid suggests that the Commission should require that all imported equipment, particularly from China (and including PCAs), undergo mandatory testing and risk assessment processes to help address concerns about backdoors[122] and potential hardware tampering.[123] Secure the Grid recommends expanding the scope of SCRM Reliability Standards to include comprehensive protection measures for PCAs, regardless of their impact rating classification, to close this security gap and enhance overall grid resilience.[124]

[119] Ravnitzky Comments at 1.

[120] Bonneville Comments at 3.

[121] *Id.*

[122] *See* NIST, *NIST SP 800-82r3, Guide to Operational Technology (OT) Security* 160 (2023), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf (defining a backdoor as an undocumented way of gaining access to a computer system).

[123] Secure the Grid Comments at 5.

[124] *Id.*

2. Commission Determination

63. Pursuant to FPA section 215(d)(5), we adopt the NOPR proposal and direct NERC to modify the SCRM Reliability Standards to include PCAs as applicable assets. Based on the comments received, we affirm our preliminary finding that PCAs receive limited protections under the existing SCRM Reliability Standards and that including them as applicable assets in the SCRM Reliability Standards is necessary to maintain the reliability of the Bulk-Power System.

64. We agree with Ravnitzky that a clear, concise definition of PCAs is important for a consistent application of the SCRM Reliability Standards; however, as Bonneville noted in its comments, PCAs are already a NERC-defined term.[125] Additionally, in response to Secure the Grid's request, we decline to expand the scope of the directive as proposed in the NOPR to include low impact assets. We believe that the recommendations made by Secure the Grid to require mandatory testing on imported items and to include PCAs regardless of the classification of their associated systems exceed the scope of the proposed directive. As such, we do not believe the record is sufficient to consider such modifications in this proceeding.

C. Reliability Standard Development Timeline

65. In the NOPR, the Commission proposed to direct NERC to submit new or modified Reliability Standards in response to the Commission's directives within 12 months of the effective date of a final rule in the proceeding. The Commission sought

[125] *See supra* note 3.

comment on whether a longer timeline (e.g., 18 months) for NERC to submit responsive modifications would be necessary.

1. Comments

66. Commenters support a longer timeline for NERC to submit new or modified Reliability Standards, with most commenters supporting an 18-month standard development timeline.[126] Commenters believe that an 18-month time frame is more appropriate due to the complexity of the issues at hand, the need for thorough industry input, and the coordination with ongoing standards development efforts.

67. NERC requests that the Commission consider the "totality of standards development, both current projects and those pending Commission approval, in directing a deadline."[127] NERC requests that the Commission consider no less time than proposed in the NOPR (i.e., 12 months) and suggests that the Commission could consider a timeline of 12 months after the effective date of a final rule issued in Docket No. RM24-8-000.[128] NERC asserts that this timeline would provide the standard drafting team with more certainty as to which version of the CIP Reliability Standards to revise.

68. Idaho Power expresses concern that 12 months is not sufficient time for adequate industry input to develop those modifications to the Standards. Moreover, Idaho Power

[126] AWS Comments at 12; Bonneville Comments at 3; Trade Associations Comments at 19; Idaho Power Comments at 1-2; NEMA Comments at 2.

[127] NERC Comments at 8.

[128] *Id.* at 9.

recommends that any Reliability Standard directing the inclusion of PCAs have an implementation time frame of at least 24 months.[129]

2. Commission Determination

69. Pursuant to section 215(d)(5) of the FPA and § 39.5(g) of our regulations, we direct NERC to develop and submit for Commission approval new or modified Reliability Standards within 18 months of the effective date of this final rule. We are persuaded by commenters that 18 months is a more appropriate deadline than 12 months given NERC's ongoing standard development projects and the need for collaboration in drafting effective modifications to the Reliability Standards. An 18-month timeframe strikes an appropriate balance between providing more flexibility to NERC and industry while not unduly delaying the strengthened SCRM protections directed in this final rule. Regarding NERC's suggestion that we consider a timeline of 12 months after the effective date of the final rule in RM24-8-000, we find such an approach would result in undue uncertainty into when the SCRM protections would be in place. Moreover, the additional time provided in this final rule together with our concurrent action in other proceedings on CIP Reliability Standards[130] should provide NERC with the certainty it seeks regarding which version of the CIP Reliability Standards to revise.

[129] Idaho Power Comments at 2.

[130] *Virtualization Reliability Standards*, 192 FERC ¶ 61,228 (2025); *Critical Infrastructure Protection Reliability Standard CIP-003-11*, 192 FERC ¶ 61,227 (2025).

70. As to Idaho Power's recommendation for a 24-month implementation time frame, we decline to direct NERC on the development of the implementation timeline and encourage entities to participate in the standard drafting process.

D. Other Issues Raised by Commenters

1. Comments

71. Various commenters urge greater collaboration between the Commission, NERC, federal agencies, state regulators, and industry to develop guidance and best practices for responsible entities.[131] BSA and BCG recommend that the Commission leverage existing frameworks such as those developed by NIST and the Cybersecurity and Infrastructure Security Agency pursuant to OMB memorandums M-22-18 and M-23-16 to comply with Executive Order 14028, to manage supply chain risk.[132] These commenters urge greater federal harmonization to reduce the risk of duplicative or conflicting supply chain guidance. Hitachi Energy recommends regional and national standardization bodies align local standards with international standards to optimize resource utilization for technology providers.[133] Hitachi also supports the Supply Chain Cybersecurity Principles for Suppliers and End Users published by the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response.[134] Hitachi recommends

[131] Hitachi Comments at 5.

[132] BSA Comments at 1-2; BCG Comments at 1.

[133] Hitachi Energy Comments at 5.

[134] *Id.* at 3.

"guidance from the DOE Principles supported by established technical standards like ISA/IEC 62443 Series for Industrial Automation Control Systems should be leveraged when developing new" or modified Reliability Standards.[135] Similarly, Secure the Grid recommends that the Commission direct NERC to engage with state-level regulators to promote the adoption of robust SCRM standards across the entire U.S. electric grid.[136]

72. Secure the Grid filed comments in response to the NOPR based upon the denial of a complaint in Docket No. EL21-99-000. Secure the Grid states that while the NOPR takes steps to improve Bulk-Power System security, it does not address several concerns outlined in the referenced complaint. Secure the Grid provides recommendations to address those complaints, such as SCRM for station power transformers, risks posed by foreign entities of concern, namely China, and promotion of domestic transformer manufacturing.[137] Secure the Grid also identifies shortcomings and opportunities for improvement of the NOPR, including a lack of requirements for a comprehensive survey of Chinese equipment, lack of coordination with state public utility commissions, and insufficient testing and verification requirements for imported Chinese equipment.[138]

---

[135] *Id.*

[136] Secure the Grid Comments at 6.

[137] *Id.* at 6-14.

[138] *Id.* at 3-6.

2. Commission Determination

73. We appreciate comments that encourage federal harmonization and collaboration. As discussed above and in the NOPR,[139] we are monitoring and participating in cybersecurity efforts by federal counterparts, including the development of guidance and frameworks. Our actions in this proceeding strive to complement those efforts to strengthen cybersecurity protections of those responsible entities under the Commission's jurisdiction. We also appreciate the comments urging the Commission to collaborate on this issue with industry and state regulators and will continue to consider such opportunities.

74. Regarding Secure the Grid's recommendations for improvement of the NOPR to address concerns raised in another proceeding, we find the recommended action to be outside the scope of the directives as proposed in the NOPR. While the location of vendors is a consideration for responsible entities when identifying, assessing, and responding to risk, the Commission did not propose specific restrictions by a vendor's country of origin in the NOPR, and we decline to add such a requirement at this time.

E. Termination of the Notice of Inquiry Proceeding

75. On September 17, 2020, the Commission issued a notice of inquiry seeking comments on the potential risks to the bulk electric system posed by the use of telecommunications equipment and services produced or provided by foreign entities identified as risks to national security. The Commission also sought comments on

[139] *See*, *e.g.*, NOPR, 188 FERC ¶ 61,174 at PP 12-14.

strategies to mitigate any potential risks posed by such telecommunications equipment and services, including but not limited to potential modifications to the CIP Reliability Standards.[140]

1. Comments

76. In response to the notice of inquiry, the Commission received 24 sets of comments.[141] Most commenters recognize the risk to the security of the bulk electric system posed by using equipment, equipment components, and services from entities identified as national security risks and express their support for the voluntary collaboration now taking place between the federal government and the utilities to address this risk. While some commenters suggest it may be appropriate to address this risk through the CIP Reliability Standards framework,[142] several trade associations, utilities, and other commenters reject the need for additional mandatory requirements,

[140] Notice of Inquiry, 172 FERC ¶ 61,224.

[141] Comments were received from: ABB Enterprise Software, Inc.; American Public Power Association; jointly, Anmol Sahai and Jordan Sudol; Bonneville Power Administration; Bureau of Reclamation; Canadian Electricity Association; Edison Electric Institute; Electricity Consumers Resource Council; Electric Power Supply Association; Exelon Corporation; Finite State; Forescout Technologies, Inc.; ISO/RTO Council; MISO Transmission Owners; National Federation of Independent Business; jointly, NERC and the Regional Entities; North American Generator Forum; Reliable Energy Analytics LLC; Securing America's Future Energy; Tallahassee Electric Department; TIC Council Americas; UL LLC; U.S. Chamber of Commerce; U.S. Department of Energy.

[142] Department of Energy at 5; National Federation of Independent Business at 3.

generally contending that voluntary efforts and existing arrangements are sufficient to address this risk.[143]

2. Commission Determination

77. We appreciate the feedback that the Commission received in response to the notice of inquiry. After careful consideration of the record and the actions taken in this final rule to address issues core to the notice of inquiry, we exercise our discretion to withdraw the notice of inquiry and terminate the proceeding in Docket No. RM20-19-000. We believe that the actions taken in this final rule to strengthen the mandatory SCRM Reliability Standards, coupled with the actions taken by the FCC to restrict telecommunication and video surveillance equipment produced by entities that pose national security risks from being imported to or sold within the United States,[144] address the central issues contemplated by the notice of inquiry and associated comments received.

---

[143] Securing America's Future Energy Comments at 5.; City of Tallahassee Comments at 5-7.; Canadian Electricity Association Comments at 4; Joint Trade Associations Comments at 11-13; Edison Electric Institute Comments at 15; Exelon Corporation Comments at 3; North American Generator Forum Comments at 1-2; MISO Transmission Owners at 9.

[144] *See*, FCC, Protecting Against Nat'l Sec. Threats to the Commc'ns Supply Chain Through the Equip. Authorization Program, 88 FR 7592, 7593 (Feb. 6, 2023) (citing Secure Equipment Act of 2021, Public Law 117-55, 135 Stat. 423, (Nov. 11, 2021) that requires, among other things, that the FCC publish and periodically update a list of covered equipment that have been determined to pose national security risks and equipment or services produced or provided by entities that meet certain capabilities); *see also* FCC, Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program and the Competitive Bidding Program, 88 FR 14312 (Mar. 8, 2023).

III. Information Collection Statement

78. The information collection requirements contained in this final rule are subject to review by the OMB under section 3507(d) of the Paperwork Reduction Act of 1995.[145] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[146] 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 this collection of information unless the collection of information displays a valid OMB control number. Comments are solicited on the Commission's need for the information proposed to be reported, whether the information will have practical utility, ways to enhance the quality, utility, and clarity of the information to be collected, and any suggested methods for minimizing the respondent's burden, including the use of automated information techniques.

79. The directive to NERC to develop new, or to modify existing, Reliability Standards (and the corresponding burden) are covered by, and already included in, the existing OMB-approved information collection FERC-725 (Certification of Electric Reliability Organization; Procedures for Electric Reliability Standards; OMB Control No.

[145] 44 U.S.C. 3507(d).

[146] 5 CFR 1320.11.

1902-0225),[147] under Reliability Standards Development.[148] The reporting requirements in FERC-725 include the ERO's overall responsibility for developing Reliability Standards, including any Reliability Standards that relate to supply chain risk management.

IV. Environmental Analysis

80. 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.[149]

81. The Commission has categorically excluded certain actions from this requirement as not having a significant effect on the human environment. Included in the exclusion are rules that are clarifying, corrective, or procedural or that do not substantially change the effect of the regulations being amended.[150] The actions proposed herein fall within this categorical exclusion in the Commission's regulations.

---

[147] Another item for FERC-725 is pending review at this time, and only one item per OMB Control No. can be pending OMB review at a time. In order to submit this final rule timely to OMB, we are using FERC-725(1B) (a temporary, placeholder information collection number).

[148] Reliability Standards development as described in FERC-725 covers standards development initiated by NERC, the Regional Entities, and industry, as well as standards the Commission may direct NERC to develop or modify.

[149] *Reguls. Implementing the Nat'l Env't. Pol'y Act*, Order No. 486, 52 FR 47897 (Dec. 17, 1987), FERC Stats. & Regs. Preambles 1986-1990 ¶ 30,783 (1987) (cross-referenced at 41 FERC ¶ 61,284).

[150] 18 CFR 380.4(a)(2)(ii).

V. Regulatory Flexibility Act

82. The Regulatory Flexibility Act of 1980 (RFA)[151] generally requires a description and analysis of proposed rules that will have significant economic impact on a substantial number of small entities.

83. We are only directing NERC, the Commission-certified ERO, to develop modified Reliability Standards to improve the sufficiency of the SCRM Plans required by Reliability Standard CIP-013-2, and to protect PCAs under the SCRM Reliability Standards. These Standards are only applicable to high and medium impact BES Cyber Systems and their associated systems such as electronic access control or monitoring systems and physical access control systems.[152] Therefore, this action will not have a significant or substantial impact on entities other than NERC. Consequently, the Commission certifies that this action will not have a significant economic impact on a substantial number of small entities.

84. Any Reliability Standards proposed by NERC in compliance with this rulemaking will be considered by the Commission in future proceedings. As part of any future

[151] 5 U.S.C. 601-612.

[152] *Cf. Cyber Sec. Incident Reporting Reliability Standards*, Notice of Proposed Rulemaking, 82 FR 61499 (Dec. 28, 2017), 161 FERC ¶ 61,291 (2017) (proposing to direct NERC to develop and submit modifications to the Reliability Standards to improve mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the Bulk-Power System).

proceedings, the Commission will make determinations pertaining to the RFA based on the content of the Reliability Standards proposed by NERC.

VI. Document Availability

85. 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).

86. 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 excluding the last three digits of this document in the docket number field.

87. User assistance is available for eLibrary and the Commission's website during normal business hours from FERC Online Support at (202) 502-6652 (toll free at 1-866-208-3676) or email 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. Regulatory Planning and Review

88. Executive Orders 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563

emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. The Office of Information and Regulatory Affairs (OIRA) has determined this regulatory action is not a "significant regulatory action," under section 3(f) of Executive Order 12866, as amended. Accordingly, OIRA has not reviewed this regulatory action for compliance with the analytical requirements of Executive Order 12866.

VIII. Effective Date and Congressional Notification

89. This rule is effective **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**. The Commission has determined, with the concurrence of OIRA, that this action is not a "major rule" as defined in section 351 of the Small Business Regulatory Enforcement Fairness Act of 1996.

By the Commission.

(S E A L)

Debbie-Anne A. Reese,
Secretary.

Note: The following appendix will not appear in the Federal Register.

Appendix A

The following entities and individuals are referenced in the final rule:

- American Public Power Association and Large Public Power Council (collectively, Public Power Utilities)
- Amazon Web Services, Inc. (AWS)
- Asset 2 Vendor Network
- Bonneville Power administration (Bonneville)
- Business Software Alliance (BSA)
- Business Cyber Guardian (BCG)
- Edison Electric Institute, Electric Power Supply Association, and National Rural Electric Cooperative Association (collectively, Trade Associations)
- Hitachi Energy North America (Hitachi Energy)
- Idaho Power Company (Idaho Power)
- ISO/RTO Council (IRC)
- Michael Ravnitzky (Ravnitzky)
- Midcontinent Independent System Operator, Inc. (MISO)
- North American Transmission Forum (NATF)
- National Electrical Manufacturers Association (NEMA)
- North Electric Reliability Corporation (NERC)
- New England States Committee on Electricity (NESCOE)
- Secure the Grid Coalition (Secure the Grid)
- Transmission Access Policy Study Group (TAPS)

The following panelists participated in the Supply Chain Workshop:

- Roy Adams, Consolidated Edison, Inc. (Adams)
- Antiwon Jacobs, Sacramento Municipal Utility (Jacobs)
- Laura Schepis, NEMA (Schepis)
- Robert Kolasky, Exiger (Kolasky)
- Howard Gugel, NERC (Gugel)
- Landon Roeder, Nashville Electric System (Roeder)
- Darlington Fee, Entergy (Fee)
- Lance Spross, Oncor Electric Delivery (Spross)

Document Content(s)