Emmonak VOR/DME and the McGrath VORTAC. As amended, V–510 would extend between the McGrath VORTAC and the Big Lake VORTAC.

Regulatory Notices and Analyses

The FAA has determined that this proposed regulation only involves an established body of technical regulations for which frequent and routine amendments are necessary to keep them operationally current. It, therefore: (1) is not a ''significant regulatory action'' under Executive Order 12866; (2) is not a ''significant rule'' under DOT Regulatory Policies and Procedures (44 FR 11034; February 26, 1979); and (3) does not warrant preparation of a regulatory evaluation as the anticipated impact is so minimal. Since this is a routine matter that will only affect air traffic procedures and air navigation, it is certified that this proposed rule, when promulgated, will not have a significant economic impact on a substantial number of small entities under the criteria of the Regulatory Flexibility Act.

Environmental Review

This proposal will be subject to an environmental analysis in accordance with FAA Order 1050.1F, ''Environmental Impacts: Policies and Procedures'' prior to any FAA final regulatory action.

List of Subjects in 14 CFR Part 71

Airspace, Incorporation by reference, Navigation (air).

The Proposed Amendment

In consideration of the foregoing, the Federal Aviation Administration proposes to amend 14 CFR part 71 as follows:

PART 71—DESIGNATION OF CLASS A, B, C, D, AND E AIRSPACE AREAS; AIR TRAFFIC SERVICE ROUTES; AND REPORTING POINTS

■ 1. The authority citation for 14 CFR part 71 continues to read as follows:

Authority: 49 U.S.C. 106(f), 106(g); 40103, 40113, 40120; E.O. 10854, 24 FR 9565, 3 CFR, 1959–1963 Comp., p. 389.

§ 71.1 [Amended]

■ 2. The incorporation by reference in 14 CFR 71.1 of FAA Order JO 7400.11J, Airspace Designations and Reporting Points, dated July 31, 2024, and effective September 15, 2024, is amended as follows:

Paragraph 6010(b) Alaskan VOR Federal Airways.

* * * * *

V–510 [Amended]

From McGrath, AK, INT McGrath 121° and Big Lake, AK 294° radials; Big Lake, AK.

* * * * *

Issued in Washington, DC, on September 24, 2024.

Frank Lias,

Manager, Rules and Regulations Group.

[FR Doc. 2024–22282 Filed 9–30–24; 8:45 am]

BILLING CODE 4910–13–P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

18 CFR Part 40

[Docket No. RM24–4–000]

Supply Chain Risk Management Reliability Standards

AGENCY: Federal Energy Regulatory Commission, DOE.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Federal Energy Regulatory Commission (Commission) proposes to direct the North American Electric Reliability Corporation, the Commission-certified Electric Reliability Organization, to develop and submit for Commission approval new or modified Reliability Standards that address the: sufficiency of responsible entities' supply chain risk management plans related to the identification of, assessment of, and response to supply chain risks, and applicability of Reliability Standards' supply chain protections to protected cyber assets.

DATES: Comments are due December 2, 2024.

ADDRESSES: Comments, identified by docket number, may be filed in the following ways. Electronic filing through *https://www.ferc.gov,* is preferred.

- *Electronic Filing:* Documents must be filed in acceptable native applications and print-to-PDF, but not in scanned or picture format.
- For those unable to file electronically, comments may be filed by USPS mail or by hand (including courier) delivery.

○ *Mail via U.S. Postal Service Only:* Addressed to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street NE, Washington, DC 20426.

○ *Hand (including courier) delivery*: Deliver to: Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, MD 20852.

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*

Alexandra Holmes (Legal Information), Office of the General Counsel, Federal Energy Regulatory Commission, 888 First Street NE, Washington, DC 20426, (202) 502–6229, *alexandra.holmes@ferc.gov*

SUPPLEMENTARY INFORMATION:

Notice of Proposed Rulemaking

(Issued September 19, 2024)

1. Pursuant to section 215(d)(5) of the Federal Power Act (FPA),[1] the Commission proposes to direct the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), to submit new or modified Reliability Standards within 12 months of the effective date of a 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] Specifically, we propose to direct NERC to develop new or modified Reliability Standards to address the: (A) sufficiency of responsible entities' SCRM plans related to their (1) identification of, (2) assessment of, and (3) response to supply chain risks, and (B) applicability of SCRM Reliability Standards to protected cyber assets (PCA).[3] Our proposed directives in this NOPR are forward-looking and objective-driven.[4]

2. Although the currently effective SCRM Reliability Standards provide a baseline of protection against supply chain threats, there are increasing

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

[2] In this notice of proposed rulemaking, the term SCRM Reliability Standards 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).

[3] The Glossary of Terms Used in NERC Reliability Standards (NERC Glossary) defines PCAs 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 NERC Glossary defines Electronic Security Perimeter 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.*

[4] *See Revised Critical Infrastructure Prot. Reliability Standards*, Order No. 829, 81 FR 49878 (July 29, 2016), 156 FERC ¶ 61,050, at P 43 (2016).

opportunities for attacks posed by the global supply chain. As we have observed in prior proceedings, while the global supply chain provides the opportunity for significant customer benefits such as low cost, variety of products, and rapid innovation, it also introduces risk to the security and reliability of the Bulk-Power System by facilitating attacks by adversaries.[5] Using the global supply chain, adversaries have inserted counterfeit and malicious software, tampered with hardware, and enabled remote access.[6] Based on these known risks, over the last decade, the Commission, other Federal agencies, and the energy industry have focused on SCRM and mitigating cybersecurity risks associated with the supply chain for critical infrastructure. In light of the increasing threat environment and the need for improved mitigation strategies, we have identified significant gaps in the provisions of the SCRM Reliability Standards. Specifically, we preliminarily find that gaps remain in the SCRM Reliability Standards related to the: (A) sufficiency of responsible entities' SCRM plans related to the (1) identification of, (2) assessment of, and (3) response to supply chain risks, and (B) applicability of SCRM Reliability Standards to PCAs.

3. We believe that directing NERC to address these gaps in the SCRM Reliability Standards will strengthen the reliability and security of the Bulk-Power System. These reliability gaps present an increasingly urgent threat to the Bulk-Power System that requires timely action. As such, we propose to direct NERC to file new or modified Reliability Standards with the Commission within 12 months of the effective date of a final rule addressing the reliability concerns discussed in this NOPR. We seek comments on all aspects of the proposed directive to NERC, including the appropriate deadline by which NERC would file the new or modified Reliability Standards.

I. Background

A. Legal Authority

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.[7] Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[8] and subsequently certified NERC as the ERO.[9]

5. The Commission has the authority pursuant to section 215(d)(5) of the FPA and consistent with § 39.5(f) of the Commission's regulations, upon its own motion or upon complaint, to order the ERO to submit to the Commission a proposed Reliability Standard or a modification to a Reliability Standard that addresses a specific matter if the Commission considers such a new or modified Reliability Standard appropriate to carry out section 215 of the FPA.[10] Further, pursuant to § 39.5(g) of the Commission's regulations, when ordering the ERO to submit to the Commission a proposed or modified Reliability Standard that addresses a specific matter, the Commission may order a deadline by which the ERO must submit such Reliability Standard.[11]

B. Supply Chain Risk Management

6. 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.[12] 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.[13] 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 ''SCRM.'' SCRM includes implementing processes, tools, or techniques that minimize adverse impacts of adversary attacks.[14]

C. SCRM Reliability Standards

7. The currently effective SCRM Reliability Standards provide a baseline for supply chain risk protection for high and medium impact bulk electric system (BES) Cyber Systems [15] and various associated systems and assets as outlined in each Standard.[16] The SCRM Reliability Standards, except for Reliability Standard CIP–005–7, do not include protections for PCAs.[17]

8. 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

[5] *See, e.g., Id.* at PP 11, 25; *see also, e.g., Supply Chain Risk Mgmt. Reliability Standards,* Order No. 850, 83 FR 53992 (Oct. 26, 2018), 165 FERC ¶ 61,020, at P 2 (2018).

[6] *See infra* n.80 (discussing SolarWinds Orion network management software compromise).

[7] 16 U.S.C. 824o(e).

[8] *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).

[9] *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).

[10] 16 U.S.C. 824o(d)(5); 18 CFR 39.5(f).

[11] 18 CFR 39.5(g).

[12] *See, e.g.,* Order No. 829, 156 FERC ¶ 61,050 at P 4 (discussing the reliability concerns posed by the supply chain).

[13] *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.*

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

[15] Each BES Cyber System, per Reliability Standard CIP–002–5.1a (BES Cyber System Categorization), is placed into 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* Reliability Standard CIP–002–5.1a (Cyber Security—BES Cyber System Categorization), Attachment 1: Impact rating Criteria, *https://nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf.*

[16] Order No. 850, 165 FERC ¶ 61,020; 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).

[17] *See* Reliability Standard CIP–005–7, Requirements R1 and R2.

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.[18]

1. Reliability Standard CIP–005–7 (Electronic Security Perimeter(s))

9. Reliability Standard CIP–005–7 is applicable to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber Systems with external routable connectivity and their associated PCAs. The Standard 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. Requirements R2 and R3 of Reliability Standard CIP–005–7 work in tandem with Requirement R1.2.6 of Reliability Standard CIP–013–2, described in more detail below, to address vendor remote access controls in the operational phase. Requirements R2 Parts 2.4 and 2.5 of Reliability Standard CIP–005–7 require one or more methods for determining and disabling, respectively, active vendor remote access sessions, including interactive remote access and system-to-system remote access, taking place on a responsible entity's system. Requirement R3 is applicable to the electronic access control or monitoring systems [19] and physical access control systems [20] associated with high impact BES Cyber Systems and medium impact BES Cyber Systems with external routable connectivity. Requirement R3 includes Parts 3.1 and 3.2 and addresses remote access controls for electronic access control or monitoring systems and physical access control systems associated with high impact BES Cyber Systems and medium impact BES Cyber Systems with external routable connectivity.

2. Reliability Standard CIP–010–4 (Configuration Change Management and Vulnerability Assessments)

10. Reliability Standard CIP–010–4 is applicable to high and medium impact BES Cyber Systems and their associated electronic access control or monitoring systems and physical access control systems and requires responsible entities to prevent and detect unauthorized changes to their BES Cyber Systems. This includes requiring that responsible entities verify the identity and integrity of software and its source, when possible, prior to installation. 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.

3. Reliability Standard CIP–013–2 (Supply Chain Risk Management)

11. 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. Reliability Standard CIP–013–2 focuses 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.[21] The goal of the Standard is to ensure that responsible entities establish organizationally-defined processes that integrate a cybersecurity risk management framework into the system development lifecycle.[22] The SCRM plan must include processes for procuring and installing vendor equipment and software; identifying and assessing cybersecurity risks; notification, coordination, and disclosure of known vendor vulnerabilities; and verification of the integrity and authenticity of software and patches provided by vendors for use in the BES Cyber Systems and their associated electronic access control or monitoring systems and physical access control systems.

D. Ongoing Activities To Mitigate Supply Chain Risks

1. Federal Efforts on SCRM

12. Since approving the SCRM Reliability Standards in 2018, the Commission has continued its focus on identifying additional improvements for addressing the risk posed by the global supply chain. For example, in December of 2022, the Commission convened a joint technical conference with the U.S. Department of Energy to discuss supply chain security challenges, the current SCRM Reliability Standards, and their challenges, gaps, and opportunities for improvement.[23] In December of 2023, Commission staff issued a report that included recommendations for users, owners, and operators of the Bulk-Power System to improve their compliance with CIP Reliability Standards generally, and SCRM specifically.[24] Among other things, the 2023 Lessons Learned Report recommended that entities enhance their SCRM programs to include evaluating the risks of existing vendors and developing a plan to mitigate those risks once identified. And in March 2023, the Commission approved modifications to Reliability Standard CIP–003–9 (Security Management Controls), which added new requirements focused on SCRM for low impact BES Cyber Systems.[25]

13. There has also been recent action in the Federal Government's broader effort to secure U.S. communications networks and prohibit the use of equipment that could give a foreign adversary the ability to exploit those networks. On May 12, 2021, the President issued Executive Order 14028 on improving the nation's cybersecurity that directed multiple government agencies to partner with the private sector to enhance cybersecurity through a variety of initiatives.[26] Executive Order 14028 requires the Secretary of Commerce and the Director of the National Institute of Standards and Technology (NIST) to create and publish supply chain guidelines that include criteria to evaluate software security, criteria to evaluate security practices of

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

[19] NERC defines electronic access control or monitoring systems 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.'' *See* NERC Glossary at 12. In Order No. 850, the Commission directed NERC to include electronic access control or monitoring systems within the scope of the SCRM Reliability Standards. Order No. 850, 165 FERC ¶ 61,020 at P 46. The Commission then later approved those modifications. *See N. Am. Elec. Reliability Corp.,* 174 FERC ¶ 61,193, at P 9 (2021).

[20] NERC defines physical access control systems 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.'' *See* NERC Glossary at 22.

[21] Order No. 850, 165 FERC ¶ 61,020 at P 15.

[22] *Id.*

[23] *Supply Chain Risk Mgmt. Tech. Conference,* Docket No. AD22–12–000 (Dec. 7, 2022), *https://www.ferc.gov/news-events/events/joint-ferc-doe-supply-chain-risk-management-technical-conference-12072022.*

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

[25] *N. Am. Elec. Reliability Corp.,* 182 FERC ¶ 61,155 (2023).

[26] E.O. 14028, 88 FR 26633, 26637 (May 12, 2021).

software developers and suppliers, and tools or methods to demonstrate conformance with security practices.[27] In response to Executive Order 14028, NIST and the Office of Management and Budget (OMB) issued several guidance and memoranda documents to enhance supply chain protections for Federal entities.[28]

14. Additionally, the Federal Communications Commission (FCC), an independent agency that regulates U.S. interstate and international communications, is also addressing supply chain risks and threats within its jurisdiction. Effective February 6, 2023, the FCC issued a new rule restricting telecommunication and video surveillance equipment produced by entities that pose national security risks from being imported to or sold within the United States.[29] Under the rule, the FCC will not issue authorizations for equipment on the ''Covered List'' that the FCC publishes under the Secure Networks Act.[30] On March 8, 2023, the FCC proposed an additional rulemaking seeking input on whether to extend the prohibition to component parts that pose an unacceptable risk to national security.[31]

[27] *Id. See also* NIST, *Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity.*

[28] *E.g.,* NIST, *Secure Software Development Framework (SSDF) Version 1.1* (Feb. 2022), *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf;* NIST, *Software Supply Chain Security Guidance Under Executive Order 14028 Section 4e* (Feb. 2022), *https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-E.O.-14028-section-4e.pdf;* OMB, *Memorandum for the Heads of Executive Departments and Agencies: Protecting Critical Software Through Enhanced Security Measures,* M–21–30, 2–3 (Aug. 10, 2021) (OMB Memorandum of August 2021), *https://whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf (*directing Federal agencies to comply with and implement the security measures developed by NIST outlined in the *NIST Security Measures for E.O.-Critical Software Use* and implement those protections in phases).

[29] Under its equipment authorization authority, the FCC requires radio-frequency devices to be authorized by the FCC before being imported or marketed into the United States.

[30] 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, Pub. L. 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).

[31] 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).

2. NERC Efforts on SCRM

15. Since the Commission directed and then approved the first set of SCRM Reliability Standards, NERC has independently taken additional actions to improve supply chain controls. For example, in 2019, NERC completed a study of supply chain risks including those associated with low impact assets not currently subject to Reliability Standard CIP–013.[32] Pursuant to this study, NERC modified Reliability Standard CIP–003 to include supply chain controls for vendor remote access, which the Commission approved in March of 2023.[33]

16. Separately, stemming in part from cybersecurity events such as the SolarWinds Orion compromise, the NERC Board of Trustees directed NERC staff to complete a review and analysis of the risk posed by low impact BES Cyber Assets and report on whether to modify criteria for determining whether a BES Cyber System be categorized as low impact.[34] Based on the resulting Low Impact Criteria Review Report,[35] NERC initiated a standards development project to modify Reliability Standard CIP–003. The stated purpose of the project is to further revise CIP–003 to, among other things, improve vendor remote access protections.[36]

17. Yet another effort regarding supply chain security was NERC's development of a draft standards authorization request (SAR) to revise Reliability Standard CIP–013–2. On September 20, 2023, NERC staff submitted a draft SAR to the NERC Standards Committee to revise Reliability Standard CIP–013–2.[37] The purpose of the standard development project was to revise ''CIP–013–2 to have complete and accurate assessments of supply chain security risks that reflect actual threat(s) posed to the entity'' and ''provide triggers on when the supply chain risk assessment(s) must be performed (*i.e.,* planning for procurement, procurement, and installation) and require a response to risks identified.'' [38] Specifically, the draft SAR project scope was to revise Reliability Standard CIP–013–2 to require entities to: (1) create specific triggers to activate the supply chain risk assessment(s); (2) include the performance of supply chain risk assessment(s) during the different phases of planning for procurement, procurement, installation of equipment/software/services, and post procurement assessment; (3) include steps to validate the completeness and accuracy of the data, assess the risks, consider the vendor's mitigation activities, and document and track any residual risks; (4) track and respond to all risks identified; (5) re-assess standing contract risks on a set timeframe; and (6) re-assess time delay installation beyond a set timeframe. The NERC Standards Committee declined to move forward with this SAR and there has been no further activity on this proposed project.

18. In addition to standards development projects, studies, and surveys, and pursuant to a resolution from the NERC Board of Trustees, NERC also initiated a collaborative SCRM program with industry, trade organizations, and key stakeholders to manage the effective mitigation of supply chain risks.[39] This program included a study of supply chain risks, communication of those risks to the electric industry, and the development of white papers on topics such as the effectiveness of the SCRM Reliability Standards and SCRM best practices.[40] Finally, NERC has also published voluntary security guidelines and whitepapers on topics relevant to supply chain risk management such as

[32] NERC, *Supply Chain Risk Assessment: Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request* (Dec. 9, 2019), *https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply%20Chain%20Risk%20Assesment%20Report.pdf.*

[33] *N. Am. Elec. Reliability Corp.,* 182 FERC ¶ 61,155 (2023).

[34] *See* NERC, *Minutes: Board of Trustees,* 7 (Feb. 4, 2021), *https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Minutes%20-%20BOT%20Open%20-%20Feb%204%202021.pdf.*

[35] NERC, *Low Impact Criteria Review Report: NERC Low Impact Criteria Review Team White Paper* (Oct. 2022), *https://www.nerc.com/pa/Stand/Project%202023%2004%20Modifications%20to%20CIP%20003%20DL/NERC_LICRT_White_Paper_clean.pdf.*

[36] NERC, *Project 2023–04 Modifications to CIP–003, https://www.nerc.com/pa/Stand/Pages/Project-2023-04-Modifications-to-CIP-003.aspx* (stating the purpose and industry need for the modifications to Reliability Standard CIP–003).

[37] *See* NERC, *Agenda: Standards Committee Meeting,* Agenda Item 6a, 2 (Sept. 20, 2023), *https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC_Agenda_Package_September_20_2023.pdf* (NERC Draft SAR).

[38] *Id.*

[39] *See* NERC, *Proposed Additional Resolutions for Agenda Item 9.a: Cyber Security—Supply Chain Risk Management—CIP–005–6, CIP–010–3, and CIP–013–1: Board of Trustees Meeting* (Aug. 10, 2017), *https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf* (NERC SCRM Board Resolution).

[40] *See* NERC, *Supply Chain Risk Mitigation Program, https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.*

key practices and guidance for responsible entities.[41]

3. Industry Efforts on SCRM

19. Industry stakeholders have also taken the initiative to develop various guidelines and best practice documents to improve SCRM. For example, the Electric Power Research Institute issued a 2018 report recommending that responsible entities develop and implement supply chain traceability of their systems and components and to consider cloud services as a part of an entity's supply chain.[42] Similarly, Edison Electric Institute released voluntary guidance with model procurement contract language to help responsible entities address cybersecurity supply chain risk with their vendors.[43] And the North American Transmission Forum (NATF) developed an ERO-endorsed CIP–013 Implementation Guide,[44] as well as several documents pertaining to supply chain risk management that represent approaches that responsible entities may take to comply with Reliability Standard CIP–013 in a systematic and comprehensive manner.[45]

II. Discussion

20. While the SCRM Reliability Standards provide a strong foundation of protection against supply chain threats, we are 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 below, we believe that the SCRM plans required by the currently effective SCRM Reliability Standards are insufficient to protect against the myriad 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. As such, pursuant to section 215(d)(5) of the FPA, we propose to direct NERC to develop new or modified Reliability Standards to address the: (A) sufficiency of responsible entities' SCRM plans related to the (1) identification of, (2) assessment of, and (3) response to supply chain risks; and (B) applicability of SCRM Reliability Standards to PCAs.

21. We are aware of and appreciate the continuing efforts of NERC, industry, and other Federal agencies to address supply chain risks. In particular, we note that NERC has identified areas for improvement of the SCRM Reliability Standards,[46] and NERC and industry continue to develop voluntary guidance or best practices to address supply chain risks. Nonetheless, we do not believe existing efforts sufficiently address known gaps in the SCRM Reliability Standards, and we believe further Commission action is warranted to address them.

22. Similarly, while we view the FCC's recent actions as beneficial for Bulk-Power System reliability, these actions address only certain aspects of identified supply chain risks. For example, the new FCC rules prohibit import and installation of telecommunications and video surveillance equipment and software produced by a relatively small number of entities. By contrast, the purpose of the SCRM Reliability Standards is to provide risk mitigation against a broader set of potential threats, including risks associated with entities that are not currently banned under the FCC's authority.[47] We therefore believe that it is appropriate to address SCRM gaps that are within our jurisdiction to better protect the security and reliability of the Bulk-Power System.

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

23. As discussed further below, we believe that the lack of clear requirements and criteria in the SCRM Reliability Standards as to how responsible entities should identify, assess, and respond to supply chain risks has left the Bulk-Power System vulnerable to attack. We believe that the proposed directives discussed in this NOPR will address these reliability gaps by providing responsible entities with clear and detailed requirements for what their SCRM plans should include and what their responsibilities are in carrying out those plans.

1. Commission Concerns Regarding Reliability Gaps Within the SCRM Reliability Standards

24. The SCRM Reliability Standards require each responsible entity to develop a SCRM plan to identify and assess supply chain and cybersecurity risks based on certain information collected from its vendors. While providing a baseline of protection, the Reliability Standards do not provide specific requirements as to when and how an entity should identify and assess supply chain risks, nor do the Standards require entities to respond to those risks identified through their SCRM plans.

25. The lack of specific requirements related to the (1) identification of, (2) assessment of, and (3) response to risk is also inconsistent with generally established risk management frameworks. Risk management frameworks generally follow three tenets: identify, assess, and respond.[48] A responsible entity's failure to properly identify and assess supply chain risks could lead to an entity installing vulnerable products and allowing compromise of its systems, ''effectively bypassing security controls established by CIP Reliability Standards.'' [49] Further, incomplete or inaccurate risk identification may result in entity assessments of the likelihood and potential impact of supply chain risks that do not reflect the actual threat and risk posed to the responsible entity. In the absence of clear criteria, procedures of entities with ad hoc approaches do not include steps to validate the completeness and accuracy of the vendor responses, assess the risks, consider the vendors' mitigation activities, or respond to any residual risks.[50]

26. As described in the 2023 Lessons Learned Report, Commission audit staff observed multiple gaps in SCRM. In Fiscal Year 2023, Commission staff

[41] The eight NERC-approved security guidelines include: (1) Cyber Security Risk Management Lifecycle; (2) Open Source Software; (3) Secure Equipment Delivery; (4) Supply Chain Procurement Language; (5) Vendor Incident Response; (6) Vendor Risk Management Lifecycle; (7) Supply Chain Provenance; and (8) Cloud Computing. NERC, *Reliability Guidelines, Security Guidelines, Technical Reference Documents, and White Papers, https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx.*

[42] Elec. Power Research Inst., *Supply Chain Risk Assessment: Final Report* (July 2018), *https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/EPRI_Supply_Chain_Risk_Assessment_Final_Report_public.pdf.*

[43] Edison Elec. Inst., *Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk* (Oct. 2022), *https://www.eei.org/-/media/Project/EEI/Documents/Issues-and-Policy/Model--Procurement-Contract.pdf.*

[44] *See* NATF, *NATF CIP–013 Implementation Guidance: Supply Chain Risk Management Plans* (Oct. 2023), *https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.*

[45] Additional NATF documents related to supply chain collaboration are available at *https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.*

[46] *See, e.g., infra* n.80 (discussing the Orion software attack); *infra* n.82 (discussing XZ Utils supply chain attack).

[47] *See supra* n.29.

[48] For example, the NIST Risk Management Framework includes these three tenants of risk and further breaks them down into a seven-step process that entities can use to manage information security and privacy risk for organizations and systems. NIST, *Special Publication 800–37, Revision 2: Risk Management Framework for Information Systems and Organizations,* Task R–3, Risk Response at 72 (Dec. 2018), *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.* (NIST Risk Management Framework).

[49] 2023 Lessons Learned Report at 17–18.

[50] *Id.*

completed non-public audits of several responsible entities to evaluate their compliance with the CIP Reliability Standards. While these audits found that most of the responsible entities were compliant with the SCRM Reliability Standards, there were nevertheless a number of security risks that remained due to the entities' SCRM processes and procedures.[51]

27. In particular, staff found a lack of consistency and effectiveness in SCRM plans for evaluating vendors and their supplied equipment and software. While a minority of audited entities had comprehensive vendor risk evaluation processes in place and displayed a consistent application of the risk identification process to each of their vendors, other entities displayed inconsistent and ad hoc vendor risk identification processes. These risk identification processes were typically completed by only using vendor questionnaires.[52] Further, using only vendor questionnaires resulted in inconsistency of the information collected and was limited to only ''yes/no'' responses regarding the vendors' security posture. Unlike the approach of relying on a vendor questionnaire, a comprehensive approach may validate the data provided by vendors and consider additional factors (*e.g.,* independent third-party evaluation of products and services) that inform how risks of individual assets impact other assets and systems of assets that reside in the same electronic security perimeter.

28. Commission staff also observed that many SCRM plans did not establish procedures to respond to risks once identified.[53] The 2023 Lessons Learned Report documented that audited entities' SCRM plans did not include processes or procedures to respond to risks identified pursuant to Reliability Standard CIP–013–2, Requirement R1.1.[54] A responsible entity has many options as to how it may respond to risks, including mitigation, acceptance, transfer, or avoidance. Regardless of the chosen option, however, a response typically includes documenting and tracking the risk.[55] In instances where a responsible entity has decided that the risk is sufficiently low that no mitigation is required, the entity should document and track its conclusions, such as in a risk register where identified and assessed risks are stored and monitored. As noted in the report, since the SCRM Reliability Standards do not require any action beyond the identification and assessment of risk, responsible entities are not required to take action to respond to or otherwise mitigate identified risks, regardless of severity. Further, staff also found that there were disparities in entity understanding and characterization of risk exposure from existing contracts and vendor relationships that were not fully considered by their supply chain risk management plans, versus those that had complete risk assessments under the parameters required by the criteria in CIP–013. This disparity resulted in entities not having a definitive strategy regarding how they would respond to various risk events posed by potential issues that may arise from existing contracts.[56]

29. Staff's observations in the 2023 Lessons Learned report are consistent with gaps identified by NERC staff in its draft SAR proposing to revise Reliability Standard CIP–013–2. Specifically, the draft SAR explained that ''the language in CIP–013–2 Requirement R1 lacks specificity to properly identify, assess, and respond to supply chain security risks.'' [57] The NERC draft SAR further identified that ''Requirement R1.1 does not indicate how to perform risk identification and assess vendor risks effectively,'' nor does CIP–013–2 ''contain sufficient triggers requiring [the activation of] an entity's [SCRM] plan.'' [58] The draft SAR goes on to explain that implementation of SCRM plans is ''wide ranging and variable'' and that ''the implemented [i]ndustry supply chain risk processes are ambiguous and generally lack rigor for validating the completeness and accuracy of the data, assessing the risks, considering the vendor's mitigation activities, and documenting and tracking residual risks.'' [59] Finally, the draft SAR proposed to initiate a standard development project to revise Reliability Standard ''CIP–013–2 to have complete and accurate assessments of supply chain security risks that reflect actual threat(s) posed to the entity'' and ''provide triggers on when the supply chain risk assessment(s) must be performed (*i.e.,* planning for procurement, procurement, and installation) and require a response to risks identified.'' [60]

30. In light of these identified gaps, we are concerned that the existing SCRM Reliability Standards lack a detailed and consistent approach for entities to develop adequate SCRM plans related to the (1) identification of, (2) assessment of, and (3) response to supply chain risk. Specifically, we are concerned that the SCRM Reliability Standards lack clear requirements for when responsible entities should perform risk assessments to identify risks and how those risk assessments should be conducted to properly assess risk. Further, we are concerned that the Reliability Standards lack any requirement for an entity to respond to supply chain risks once identified and assessed, regardless of severity.

2. Proposed Directives

31. To address the reliability and security gaps discussed above, we propose to direct NERC pursuant to section 215(d)(5) of the FPA, to develop new or modified Reliability Standards to address the sufficiency of SCRM plans related to the: (1) identification of, (2) assessment of, and (3) response to supply chain risks.

a. Identification

32. We propose to direct NERC to submit to the Commission 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. Specifically, we propose 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. If an entity does not install the equipment or software within the specified time limit, the entity should be required to perform an updated risk assessment prior to installation. As discussed above, we are concerned 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

[51] *Id.* at 1.

[52] *Id.* at 17–18.

[53] *Id.* Further, many entities did not include processes in their SCRM plans to identify, assess, or respond to risks associated with existing contracts prior to the effective date of the SCRM Reliability Standards, though the Standards neither require entities to respond to risk nor reassess existing contracts. *Id.*

[54] *Id.* Reliability Standard CIP–013–2, Requirement R1.1, requires entities to develop supply chain cyber security risk management plans that include:

[o]ne or more process(es) used in planning for the procurement of BES Cyber Systems and their associated [electronic access control or monitoring systems and physical access control systems] to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

[55] *See, e.g.,* NIST Risk Management Framework, Task R–3, Risk Response at 72.

[56] 2023 Lessons Learned Report at 17.

[57] *See* NERC Draft SAR, Agenda Item 6a, 2.

[58] *Id.*

[59] *Id.*

[60] *Id.* at 26.

incomplete or inaccurate risk identification that may result in assessments of supply chain risks that do not reflect the actual threat and risk posed to the responsible entity. We seek comment on what factors should be considered in developing a maximum time frame between the initial risk assessment and installation before entities would be required to perform a subsequent risk assessment. We also seek comment on whether this time frame should vary based on certain factors (*e.g.,* equipment type) and the reasons for any proposed time frame variation.

33. Further, to satisfy the Commission directive, the new or modified Reliability Standards must establish 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 since the contract commenced. For example, an entity that has a long-term contract with a vendor would be required to conduct a periodic risk assessment of that contract to identify any new or developed supply chain risks since the initial risk assessment. While this requirement would apply to all vendor, product, and service contracts, including existing contracts, we are not proposing to direct NERC to require entities to abrogate or renegotiate contracts with vendors, suppliers, or other entities.

34. We believe this proposed directive is consistent with Order Nos. 829 and 850 and would strengthen SCRM plans identification, assessment, and response to, evolving supply chain risks associated with long-term standing contracts that may not have been contemplated or in existence at the time the contract commenced. We seek comment on factors to be considered in developing a proposed requirement for entities to reassess their supply chain risks of existing contracts with vendors, including the frequency of those assessments and any specific changed circumstances that should trigger the need for a reassessment (*e.g.,* acquisition or merger of an existing supplier).

b. Assessment

35. Next, to satisfy the Commission directive, NERC must submit to the Commission for approval new or modified Reliability Standards that require a responsible entity to establish steps in its SCRM plan 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. While we are not proposing to require that entities guarantee the accuracy of information provided by their vendors, we do believe that entities should be required to take certain steps to validate such information.

36. For example, the SCRM plan could require an entity to secure from its vendors: (1) a self-attestation addressing all of the risk questions posed by the responsible entity accompanied by any relevant documentation to support the vendors' claims; or (2) a certification of an assessment from a qualified auditor, assessor, or other reputable third party addressing all risk questions posed by the responsible entity. Upon receipt of a self-attestation, the responsible entity would review and validate vendors' responses to ensure that it has complete information to ensure a rigorous risk assessment. This could represent a proactive effort to validate the information being provided by a vendor to ensure that the information the entity is using to identify and assess risks is accurate. In the absence of a self-attestation and supporting documentation provided by a vendor to the responsible entity, the responsible entity could instead accept an independent third-party certification that an assessment was conducted by a qualified auditor, assessor, or other reputable third-party addressing all risk questions posed by the responsible entity.

37. We are concerned that a responsible entity's failure to take any steps to validate a vendor's information could lead to an entity failing to properly identify or assess risk posed by that vendor and installing vulnerable products that allow compromise of its systems. Further, the lack of validation could result in entities performing risk assessments based on inaccurate or incomplete information which would not reflect the actual threat and risk posed to the responsible entity. We seek comment on what other types of steps an entity could take to validate the data provided by vendors and how burdensome those steps might be.

c. Response

38. Finally, we propose to direct NERC to ensure that the new or modified Reliability Standards require that entities establish a process to document, track, and respond to all identified supply chain risks. We are concerned that the existing SCRM Reliability Standards are inadequate to ensure consistent, timely, and appropriate documented responses to identified vendor risks. We believe that the proposed directive would better align with widely accepted risk management frameworks and address the lack of requirements in the SCRM Reliability Standards for entities to respond to risks once they are identified.

39. A responsible entity can respond to risk in a variety of ways, including by taking specific steps to mitigate the identified security risk (*e.g.,* implementing additional security monitoring of the associated asset or software), transferring the identified security risk (*e.g.,* to a security-as-a-service vendor or through cybersecurity insurance), avoiding the security risk (*e.g.,* by not deploying hardware or software associated with an identified risk), or accepting the security risk, in instances where none of the other responses are possible. Regardless of the approach taken, a responsible entity should document and track its actions.[61] Documentation should include what cybersecurity 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 Cyber Assets. For example, a SCRM plan could include defined processes and tasks to respond to the identified and assessed risk, including maintaining documentation, such as those discussed in table E–6 of the NIST Risk Management Framework.[62] Specific mitigation steps could be similar to the mitigation requirements described in Reliability Standard CIP–007–6, Requirement R2.[63] We seek comment on

[61] *Mandatory Reliability Standards for Critical Infrastructure Protection,* Order No. 706, 73 FR 7368 (Feb. 7, 2008), 122 FERC ¶ 61,040, at P 377 (2008) (discussing Reliability Standard CIP–003–1 requirement for the development and implementation of a security policy, the Commission states that the goal of documentation and justification for an exception to the policy be that there is ''reasoned decision-making, consistency, and subsequent effectiveness in implementing the policy'' and that the Commission require[s] that the reasoning be documented to ensure that the responsible entity is indeed implementing the security policy as required by Requirement R1 of CIP–003–1.'').

[62] *See* NIST Risk Management Framework at 136.

[63] Reliability Standard CIP–007–6 (Security Configuration Management), Requirement R2 (Security Patch Management). Requirement R2 Part 2.1 requires a patch management process for tracking, evaluation, and installing cyber security patches for applicable Cyber Assets. Requirement R2 Part 2.2 establishes a maximum window of 35 calendar days to evaluate the security patches that have been released for applicability. Building on Parts 2.1 and 2.2, Requirement R2 Part 2.3 requires one of the following actions: (1) apply the applicable patches; (2) create a dated mitigation plan; or (3) revise an existing mitigation plan. Building on Part 2.3, Requirement R2 Part 2.4 requires for each mitigation plan, to implement the plan within a specified timeframe.

whether and how a standard 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.

40. We further propose to direct NERC to submit responsive new or revised SCRM Reliability Standards within 12 months of the effective date of a final rule in this proceeding, given NERC has already begun the work to address several of the proposed directives in its 2023 draft SAR [64] which it may be able to leverage to timely address the risks identified in this NOPR. However, while we propose a compliance deadline of 12 months, we also seek comment on whether a longer timeline (*e.g.,* 18 months) is necessary, as we recognize that NERC is currently devoting resources to other standards development projects with Commission-imposed timelines.

B. Applicability of SCRM Requirements to PCAs

1. Prior Activity Regarding PCAs

41. PCAs are ancillary equipment that reside behind a responsible entity's electronic access point [65] within the responsible entity's BES Cyber Systems. Electronic access points, often firewalls, are important lines of defense for BES Cyber Systems that reside at an electronic security perimeter. The likelihood of PCAs' compromise through the supply chain has increased in recent years. Because PCAs are located within the 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.

42. The Commission initially considered the applicability of the SCRM Reliability Standards to PCAs in Order No. 850 but did not direct NERC to include them in the scope of the SCRM Reliability Standards. At that time, the Commission believed it was appropriate to await the findings of the study evaluating cybersecurity supply chain risks presented by low impact BES Cyber Systems, physical access control systems, and PCAs. [66] Reasoning that the likelihood of PCAs being compromised was lower than the likelihood that electronic access control or monitoring systems would be compromised, the Commission accepted NERC's commitment, as directed by the NERC Board of Trustees, to study the risk of PCAs in greater depth. The Commission expressed its concern, however, that excluding PCAs may leave a gap in the SCRM Reliability Standards and stated that it would be in a better position to consider whether the inclusion of PCAs would be warranted to protect the reliability of the Bulk-Power System after reviewing NERC's findings.[67]

43. In response to the Commission's directive, NERC submitted its Supply Chain Risk Report in May 2019.[68] The report contained recommendations for actions to address risks associated with certain categories of assets including, among others, PCAs.[69] The report stated that, due to the variety of assets that may be categorized as PCAs, it was not possible to clearly define a general risk posed by their potential supply chain vulnerabilities.[70] As such, NERC staff recommended that, as a best practice, entities should ''evaluate each PCA type on a case-by-case basis to identify any specific risks associated with [SCRM].'' [71] The NERC Supply Chain Risks Report also assessed the risks to PCAs posed by common mode vulnerabilities and found that as PCAs are ''often the same cyber asset type as many common BES Cyber Assets,'' they may act as an attack vector to BES Cyber Systems sharing the same electronic security perimeter.[72]

The report asserts that the SCRM plan required by Reliability Standard CIP–013–1, Requirement R1 could be used effectively to mitigate PCA risks for those PCAs ''obtained under the same [SCRM] procurement plan as BES Cyber Systems associated with high and medium impact BES Cyber Systems.'' [73] With respect to next steps, the report stated that NERC would continue to develop a guideline for entities to use when evaluating their PCAs and when determining what, if any, additional SCRM protections are needed. NERC added that it would also determine whether to collect additional data regarding PCAs.[74] NERC has not yet released any additional guideline documents on PCAs associated with SCRM protections, nor has NERC initiated any additional data collection.

2. Commission Concerns Regarding PCAs

44. Under the existing SCRM Reliability Standards, PCAs receive only limited protections. Specifically, while the SCRM Reliability Standards address four categories of SCRM protections: (1) software integrity and authenticity, (2) vendor remote access protections, (3) information system planning, and (4) vendor risk management and procurement controls—PCAs are only subject to the second category: vendor remote access protections. We believe that the additional protections should apply to PCAs to better mitigate the associated risks and close this known security gap. As such, we preliminarily find that addressing such unprotected PCAs within the SCRM Reliability Standards is necessary to maintain the reliability of the Bulk-Power System in light of evolving threats.

45. As mentioned above, the Commission in Order No. 850 considered but ultimately declined to direct that NERC develop SCRM Reliability Standards that apply to PCAs until the Commission could consider NERC's Board of Trustees-directed study. After reviewing NERC's findings, we preliminarily find that the risks associated with PCAs warrant their inclusion in the SCRM Reliability Standards. As discussed below, recent sophisticated supply chain incidents such as SolarWinds highlight the vulnerabilities and need to protect PCAs from supply chain threats. The NERC Supply Chain Risks Report submitted in response to the Commission's directive in Order No. 850 assessed the risks to PCAs posed by common mode vulnerabilities and found that PCAs share the same risk profile as many BES Cyber Assets that are protected under

[64] *See* NERC Draft SAR, Agenda Item 6a (including in its scope to: (1) create specific triggers to activate the supply chain risk assessment(s); (2) include the performance of supply chain risk assessment(s) during the different phases of planning for procurement, procurement of equipment/software/services, installation, and post procurement assessment; (3) include steps to validate the completeness and accuracy of the data, assess the risks, consider the vendor's mitigation activities, and document and track any residual risks; (4) track and respond to all risks identified; (5) re-assess standing contract risks on a set timeframe; (6) re-assess time delay installation beyond a set timeframe).

[65] NERC defines an electronic access point as a ''Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.'' *See* NERC Glossary at 12.

[66] Order No. 850, 165 FERC ¶ 61,020 at PP 66, 67. *See also NERC SCRM Board Resolution.*

[67] Order No. 850, 165 FERC ¶ 61,020 at P 66.

[68] NERC, *Cyber Security Supply Chain Risks: Staff Report and Recommended Actions,* Docket No. RM17–13–000 (May 28, 2019) (NERC Supply Chain Risks Report).

[69] *Id.* at 2.

[70] *Id.* at 21.

[71] *Id.*

[72] *Id.* at 22.

[73] *Id.*

[74] *Id.*

the SCRM Reliability Standards. NERC further found that due to their shared location within an electronic security perimeter, PCAs may be used as an attack vector to BES Cyber Systems.

46. Responsible entities that have robust processes for the identification and assessment of SCRM risks associated with PCAs are better protected against the unintentional procurement and installation of unsecure equipment or software that could serve as a potential attack vector to compromise medium or high impact BES Cyber Systems residing in the same electronic security perimeter. The Commission reasoned in Order No. 829 that without integrity and authenticity controls: (1) attackers could exploit the legitimate vendor patch management process to deliver compromised software updates or patches to applicable systems;[75] and (2) vendor credentials could be stolen and used to access a BES Cyber System without the responsible entities knowledge and traverse over an unmonitored connection into a responsible entity's BES Cyber System.[76] Responsible entities could unintentionally have procured and installed unsecure equipment or software and may fail to meet minimum security criteria.[77]

47. Upon reviewing NERC's report and gaining a better understanding of the risk profile associated with PCAs since Order No. 850, we believe that our reasoning as applied to BES Cyber Systems in Order No. 829 supports the inclusion of PCAs under the protection of the SCRM Reliability Standards because these assets also reside within the same electronic security perimeter as BES Cyber Systems. Accordingly, we believe that all assets within an electronic security perimeter should be assessed for supply chain risk.

48. Moreover, we are not persuaded by the NERC report which demurred from recommending additional SCRM Reliability Standard protections for PCAs. While the NERC report recognized the risks associated with PCAs, it asserted that it is not possible to clearly define a general risk to the Bulk-Power System in the event PCAs are compromised.[78] NERC did not recommend revising the SCRM Reliability Standards to include PCAs and instead recommended that entities evaluate PCAs on a voluntary, case-by-case basis for supply chain risks. While we agree with the NERC report that a wide range of assets fall under the category of PCA, we also believe that such a wide range of assets allows for a wide range of vulnerabilities, therefore proportionately increasing the risk associated with PCAs as an asset class. We further acknowledge that each PCA type may have a different risk profile based on how it interacts with BES Cyber Systems and their impact on the Bulk-Power System that may present unique challenges during risk assessment. However, because PCAs are a clearly defined class of assets, we are not persuaded that the inability to quantify the risk that PCAs present as an asset class renders infeasible the ability to develop a Reliability Standard that addresses the known SCRM risks associated with PCAs.

49. We do, however, agree with NERC's assessment in its report regarding the risk posed by common mode vulnerabilities of unprotected PCAs, *i.e.,* that they are often the same Cyber Asset type as many common BES Cyber Assets and that they may act as an attack vector to BES Cyber Systems sharing the same electronic security perimeter. For example, SolarWinds' Orion software, an enterprise infrastructure monitoring and management platform, was famously compromised by a foreign state actor in 2020. This software would likely be categorized as a PCA if used by a responsible entity and deployed inside an electronic security perimeter.[79] While NERC found that this event did not materially or adversely impact Bulk-Power System operations, a subsequent compromise impacting PCAs could have more severe consequences in the future, including material, adverse impacts on Bulk-Power System operations.[80] Similarly, the XZ Utils supply chain attack demonstrates another close call where PCAs could have been affected if the compromise had not been discovered and detected before further exploitation occurred.[81] Thus, addressing supply chain risk of unprotected PCAs that may perform security-critical functions or pose similar significant potential for harm if compromised is critical to maintaining the security of an electronic security perimeter and would improve an entity's overall security posture.

50. We also agree with NERC's assertion that the supply chain risks associated with PCAs could be mitigated if responsible entities include PCAs in their existing SCRM plans that inform the procurement of medium and high impact BES Cyber Systems.[82] We do not agree, however, that this should be done on a voluntary basis since many PCAs have a similar risk profile to BES Cyber Systems. Finally, we note that applying supply chain protections to PCAs is consistent with risk management practices required for Federal agencies. Specifically, extending supply chain related protections to PCAs aligns with the OMB Memorandum of August 2021 and its phased implementation strategy by ensuring that all software, especially those performing security-critical functions, is fortified against supply chain risks.[83] By proactively evaluating the supply chain risks posed by PCAs, the electric sector can address the risk of supply chain attacks, which have been exemplified by incidents like the SolarWinds breach. The OMB Memorandum of August 2021 provides instructions and creates a phased implementation plan for Federal agencies to adopt the security measures required by Executive Order 14028. Included in the initial phase of implementation are software applications that provide network monitoring and configuration services (*e.g.,* PCAs).[84] This directive, while binding only on Federal agencies, further supports the extension of SCRM protective measures to PCAs. PCAs, if compromised, could serve as conduits for adversaries to infiltrate BES Cyber Systems, potentially leading to breaches originating from within the electronic security perimeters.

3. Proposed Directives

51. For the reasons set forth above, we preliminarily find that the existing SCRM Reliability Standards are

[75] Order No. 829, 156 FERC ¶ 61,050 at P 49.

[76] *Id.* P 52.

[77] *Id.* PP 57, 60.

[78] NERC Supply Chain Risks Report at 21.

[79] FERC Staff and the Electricity Information and Analysis Sharing Center, *SolarWinds and Related Supply Chain Compromise* (July 6, 2021), *https://www.nerc.com/pa/CI/ESISAC/Documents/SolarWinds%20and%20Related%20Supply%20Chain%20Compromise%20White%20Paper.pdf.*

[80] Robert Walton, *NERC finding 25% of utilities exposed to SolarWinds hack indicates growing ICS vulnerabilities, analysts say,* Utility Dive (Apr. 15, 2021), *https://www.utilitydive.com/news/nerc-finding-25-of-utilities-exposed-to-solarwinds-hack-indicates-growing/598449/.*

[81] In this supply chain attack, an unidentified threat actor used social engineering to become an authorized maintainer of XZ Utils, a widely used data compression and decompression library found on many Linux systems. The threat actor then inserted a backdoor into legitimate software updates that would allow them to bypass Secure Shell Protocol authentication and conduct remote code execution on any infected device connected to the internet. *See* Cybersecurity and Infrastructure Security Agency, *Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library, CVE–2024–3094* (Mar. 29, 2024), *https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094.*

[82] NERC Supply Chain Risks Report at 22.

[83] *See supra* n.28.

[84] *See id.*

inadequate to ensure that PCAs are sufficiently protected from supply chain risk. Because PCAs represent an attack vector to BES Cyber Systems contained within the same electronic security perimeter as the PCAs, the Commission's concern about the threat that these unprotected assets present to the security and reliability of the Bulk-Power System has grown since initially discussed in Order No. 850. As discussed above, these risks are highlighted by recent sophisticated incidents such as the SolarWinds software vulnerability and the XZ Utils supply chain attack. While the current SCRM Reliability Standards require entities to protect PCAs' vendor remote access management, the Reliability Standards should provide a comprehensive protection of PCAs.

52. Accordingly, we propose to direct NERC, pursuant to section 215(d)(5) of the FPA, to modify the SCRM Reliability Standards to include PCAs as applicable assets. Further, we propose to direct NERC to protect PCAs from supply chain risk at the same level as other assets inside an electronic security perimeter (*i.e.,* high and medium impact BES Cyber Systems, electronic access control or monitoring systems, and physical access control systems located inside an electronic security perimeter). Given the broad range of assets that may be categorized as PCAs, we seek comment on potential comprehensive and scalable approaches that could be implemented for identifying and assessing supply chain risks posed by PCAs. Comments on such approaches may inform our directives in a final rule and may also provide valuable input for a possible future NERC standard drafting team tasked with developing directed modifications. Finally, we propose to direct NERC to submit these modifications within 12 months of the effective date of a final rule in this proceeding.

III. Information Collection Statement

53. The information collection requirements contained in this notice of proposed rulemaking are subject to review by the OMB under section 3507(d) of the Paperwork Reduction Act of 1995.[85] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[86] 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 proposed 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.

54. The proposal to direct 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. 1902–0225),[87] under Reliability Standards Development.[88] The reporting requirements in FERC–725 include the ERO's overall responsibility for developing Reliability Standards, such as any Reliability Standards that relate to supply chain risk management.

IV. Environmental Analysis

55. 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.[89]

56. 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.[90] The actions proposed herein fall within this categorical exclusion in the Commission's regulations.

V. Regulatory Flexibility Act

57. The Regulatory Flexibility Act of 1980 (RFA)[91] generally requires a description and analysis of proposed rules that will have significant economic impact on a substantial number of small entities.

58. We are proposing only to direct NERC, the Commission-certified ERO, to develop modified Reliability Standards to improve the sufficiency of the SCRM Plans required by 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.[92] Therefore, this NOPR will not have a significant or substantial impact on entities other than NERC. Consequently, the Commission certifies that this NOPR will not have a significant economic impact on a substantial number of small entities.

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

VI. Comment Procedures

60. The Commission invites interested persons to submit comments on the matters and issues proposed in this rulemaking to be adopted, including any related matters or alternative proposals that commenters may wish to discuss. Comments are due December 2, 2024. Comments must refer to Docket No. RM24–4–000, and must include the commenter's name, the organization they represent, if applicable, and their address in their comments. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability section below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

61. The Commission encourages comments to be filed electronically via the eFiling link on the Commission's website at *https://www.ferc.gov.* The Commission accepts most standard word processing formats. Documents

[85] 44 U.S.C. 3507(d).

[86] 5 CFR 1320.11.

[87] 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 NOPR timely to OMB, we are using FERC–725(1B) (a temporary, placeholder information collection number).

[88] 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.

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

[90] 18 CFR 380.4(a)(2)(ii) (2021).

[91] 5 U.S.C. 601–612.

[92] *Cf. Cyber Security 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).

created electronically using word processing software must be filed in native applications or print-to-PDF format and not in a scanned format. Commenters filing electronically do not need to make a paper filing.

62. Commenters that are not able to file comments electronically may file an original of their comment by USPS mail or by courier-or other delivery services. For submission sent via USPS only, filings should be mailed to: Federal Energy Regulatory Commission, Office of the Secretary, 888 First Street NE, Washington, DC 20426. Submission of filings other than by USPS should be delivered to: Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, MD 20852.

VII. Document Availability

63. 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 (*https://www.ferc.gov*). 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.

64. 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. Email the Public Reference Room at *public.referenceroom@ferc.gov.*

By direction of the Commission.

Dated: September 19, 2024.

Debbie-Anne A. Reese,

Acting Secretary.

[FR Doc. 2024–22230 Filed 9–30–24; 8:45 am]

BILLING CODE 6717–01–P

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 220

[Docket ID: DoD–2022–HA–0054]

RIN 0720–AB87

Medical Billing for Healthcare Services Provided by Department of Defense Military Medical Treatment Facilities to Civilian Non-Beneficiaries

AGENCY: Defense Health Agency (DHA), Department of Defense (DoD).

ACTION: Proposed rule.

SUMMARY: As required by the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (NDAA–23), this document proposes to reduce financial harm to civilians who are not covered beneficiaries of the Military Health System (MHS), and who receive healthcare services at DoD military medical treatment facilities (MTF). The rulemaking, once finalized, will implement the MHS Modified Payment and Waiver Program (MPWP) through which the DoD will apply a sliding fee scale and/or a catastrophic fee waiver to medical invoices of certain non-beneficiaries and will accept payments from health insurers of non-beneficiaries as full payment except for copays, coinsurance, deductibles, nominal fees and non-covered services.

DATES: This rulemaking, once finalized, will apply to non-beneficiary patient medical care provided on or after June 21, 2023. Comments to this proposed rule are being accepted and must be received by December 2, 2024.

ADDRESSES: You may submit comments, identified by docket number and/or Regulation Identifier Number (RIN) number and title, by any of the following methods:

- *Federal eRulemaking Portal: https://www.regulations.gov.* Follow the instructions for submitting comments.
- *Mail:* Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 08D09, Alexandria, VA 22350–1700.

Instructions: All submissions received must include the agency name and docket number or RIN. The general policy for comments is to make these submissions available for public viewing at *https://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Merlyn Jenkins, phone number: (703) 681–7346, mailing address: Office of the Secretary of Defense for Health Affairs, Health Resources Management and Policy, 1200 Defense Pentagon, Washington, DC 20301–1200; email address: *mailto:merlyn.jenkins.civ@health.mil.*

SUPPLEMENTARY INFORMATION: The NDAA–23 also grants the Director of DHA discretionary authority to waive assessment of medical fees of non-beneficiaries when the healthcare provided enhances the knowledge, skills, and abilities (KSAs) of healthcare providers, as determined by the Director of DHA. The DHA is proposing to implement the amendments to 10 U.S.C. 1079b enacted through the NDAA–23. By statute (Pub. L. 117–263, div. A, title VII, § 716(c), Dec. 23, 2022, 136 Stat. 2661), the sliding fee scale and/or catastrophic fee waivers apply to bills for healthcare services provided at MTFs on or after June 21, 2023.

I. Background and Authority

Title 10, United States Code (U.S.C.), section 1073d requires the Department of Defense (DoD) to maintain MTFs for the purposes of supporting the medical readiness of the armed forces and the readiness of deployable medical personnel. To maintain medical currency and bolster the KSAs of DoD healthcare providers, the DoD renders emergency, trauma, and other medical services to beneficiaries of the MHS which consist of service members and former service members, and their dependents. The MHS may provide healthcare services to other individuals who are not eligible beneficiaries, in certain circumstances, as authorized by law, and typically on a reimbursable basis (Pub. L. 114–328, 717(c), Dec. 23, 2016, as amended (10 U.S.C. 1071 note); and § 1074(c)).

Proposed rules implementing DoD's authority under 10 U.S.C. 1095 and related provisions of law to compute reasonable charges for inpatient and ambulatory (outpatient) care provided by MTFs, including charges for pharmaceuticals, durable medical equipment, supplies, immunizations, injections, or other medications, are at 32 CFR part 220, last updated on August 20, 2020 (55 FR 21742–21750). Medical billing is structured under three existing healthcare cost recovery programs: Third Party Collections (10 U.S.C. 1095); Medical Services Account (10 U.S.C. 1079b, 1085, and 1104); and Medical Affirmative Claims (42 U.S.C. 2651–2653). The rates used for billing are modeled after the rates published by