6717-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

18 CFR Part 40

[Docket No. RM24-8-000]

Virtualization Reliability Standards

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Federal Energy Regulatory Commission (Commission) proposes to approve four new definitions and 18 modified definitions in the North American Electric Reliability Corporation (NERC) Glossary of Terms Used in Reliability Standards. The Commission also proposes to approve eleven modified Critical Infrastructure Protection (CIP) Reliability Standards. NERC, the Commission-certified electric reliability organization, submitted the proposed modifications to update the CIP Reliability Standards to enable the application of virtualization and other new technologies in a secure manner.

DATES: Comments are due **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Comments, identified by docket number, may be filed in the following ways. Electronic filing through http://www.ferc.gov, 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, N.E., Washington, DC 20426.
- Hand (including courier) delivery: Deliver to: Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, MD 20852.

The Comment Procedures Section of this document contains more detailed filing procedures.

FOR FURTHER INFORMATION CONTACT:

Mayur Manchanda (Technical Information)

Office of Electric Reliability

Federal Energy Regulatory Commission

888 First Street, NE

Washington, DC 20426

(202) 502-6166

Mayur.Manchanda@ferc.gov

Chanel Chasanov (Legal Information)

Office of General Counsel

Federal Energy Regulatory Commission

888 First Street, NE

Washington, DC 20426

(202) 502-8569

Chanel.Chasanov@ferc.gov

Alan J. Rukin (Legal Information)

Office of General Counsel

Federal Energy Regulatory Commission

888 First Street, NE

Washington, DC 20426

(202) 502-8502

Alan.Rukin@ferc.gov

SUPPLEMENTARY INFORMATION:

I. Introduction

1. Pursuant to section 215(d)(2) of the Federal Power Act (FPA),[1] we propose to approve the addition of four new and 18 proposed revisions to the North American Electric Reliability Corporation (NERC) Glossary of Terms Used in Reliability Standards (Glossary). We also propose to approve 11 proposed Critical Infrastructure Protection (CIP) Reliability Standards. NERC submitted the proposed modifications to update the CIP Reliability Standards to enable the application of virtualization and other new technologies in a secure manner.[2] We also propose to approve the associated violation risk factors, violation severity levels, implementation plans, and effective dates for the

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

[2] *See* NERC Petition at 2-5. Virtualization is "the process of creating virtual, as opposed to physical, versions of computer hardware to minimize the amount of physical hardware resources required to perform various functions." NERC Petition at 12 (quoting National Institute of Standards and Technology (NIST), Guide to Security for Full Virtualization Technologies, Special Publication 800-125 (Jan. 2011) (NIST Virtualization Security Special Publication)).

proposed Reliability Standards, as well as to approve the retirement of the currently effective version of each proposed Reliability Standard.

2. We support NERC's efforts to update the CIP Reliability Standards to accommodate virtualization and other nascent technologies. These proposed updates will allow responsible entities to enhance their reliability and security posture by adapting to emerging risks with forward-looking security models. As NERC explains, the current framework for CIP Reliability Standards "was designed around the concept that devices have a one-to-one relationship between software and hardware,"[3] and CIP-mandated controls such as perimeter-based security were designed to fit this concept. However, "technology supporting and enabling the industrial control systems that operate the Bulk-Power System has evolved rapidly."[4] To accommodate this evolution, NERC has updated the CIP Reliability Standards to provide responsible entities the flexibility to adopt virtualization and other new technologies "to operate their systems effectively and efficiently while maintaining a robust security posture."[5] The proposed modifications do not obligate entities to adopt virtualization, rather, if approved, the proposed CIP Reliability Standards would accommodate responsible entities that choose to do so. NERC highlights the reliability benefits of virtualization, including "increased uptime, fast recovery capability, and flexible architecture that can instantly adapt to changing workloads."[6] We agree that these potential reliability benefits are worth pursuing, and

---

[3] NERC Petition at 4.

[4] *Id.* at 2.

[5] *Id*. at 16 & Ex. D (standard drafting team white paper titled Virtualization and Future Technologies: The Case for Change).

[6] *Id*. at 16.

we continue to support efforts by NERC and responsible entities to facilitate the use of technological advancements that enhance the reliability and security of the Bulk-Power System.

3. While we propose to approve the proposed CIP Reliability Standard modifications, we have questions regarding the proposed language (repeated in multiple Requirements) that would replace the phrase where technically feasible with the phrase per system capability.[7] NERC explains that the revision would eliminate the technical feasibility exceptions and associated reporting and approval process. Going forward, responsible entities would still be required to document an identified limit to a system capability and simply retain the documentation for review upon audit or other compliance activity.[8] We recognize NERC's efforts to alleviate administrative burdens associated with the current technical feasibility exception process. Nonetheless, we are concerned that the proposed phrase per system capability would eliminate transparency and meaningful Commission and NERC oversight by introducing a self-implementing exceptions process with no reporting obligations. Thus, as discussed below, we seek comments on this aspect of the NERC proposal, including alternative approaches, which will assist the Commission in formulating a possible directive in a final rule.

---

[7] *See* NERC Rules of Procedure section 412 (Requests for Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Reliability Standards), Appendix 4D (Procedure for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Reliability Standards).

[8] *See* NERC Petition at 29-30; *see also* NERC Supplemental Petition at 26 (an entity relying on the system capability exception "will need to document the limit to the system's capability and demonstrate during compliance monitoring activities that the system's incapability prevents the Responsible Entity from implementing the control within the requirement").

II. Background

A. Section 215 and Mandatory Reliability Standards

4. Section 215 of the FPA provides that the Commission may certify an Electric Reliability Organization (ERO), the purpose of which is to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval.[9] Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[10] Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[11] and subsequently certified NERC.[12]

B. Virtualization

5. Virtualization is the process of creating virtual, as opposed to physical, versions of computer hardware to minimize the amount of physical computer hardware resources required to perform various functions.[13] NERC explains three virtualization concepts: (1) shared resources; (2) virtual machines; and (3) containers. First, virtualization allows the sharing of hardware, central processing units, memory, storage, and other resources

---

[9] 16 U.S.C. 824o(c).

[10] *Id.* 824o(e).

[11] *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); *see also* 18 CFR 39.4(b).

[12] *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).

[13] *See Virtualization & Cloud Computing Servs.*, Notice of Inquiry, 170 FERC ¶ 61,110, at P 4 (2020) (Virtualization and Cloud NOI) (citing NIST Virtualization Security Special Publication).

among various operating systems (i.e., guest operating systems).[14] Second, a virtual machine is a software version of a single physical computer and performs all the same functions. Virtual machines have operating systems and can run application programs, store data, connect to networks, and perform functions identical to a physical computer. Third, containers are considered software that encapsulate applications and their dependencies in isolated environments, separate from other applications or containers. A container is not a virtual machine; a container shares operating system resources from the host computer in which it resides. The host computer can be either a physical or virtual machine. Containers interact with other applications and services on the host computer through defined interfaces.

C. NERC Petition and Supplement

6. On July 10, 2024, as supplemented on May 20, 2025,[15] NERC submitted for Commission approval four newly defined terms (Cyber System, Management Interface, Shared Cyber Infrastructure, and Virtual Cyber Asset) to support the virtualization-related modifications to the proposed CIP Reliability Standards. Likewise, NERC submitted 18 proposed revisions to defined terms within the NERC Glossary (BES Cyber Asset, BES Cyber System, BES Cyber System Information, CIP Senior Manager, Cyber Assets, Cyber Security Incident, Electronic Access Control or Monitoring Systems, Electronic Access Point, External Routable Connectivity, Electronic Security Perimeter, Interactive Remote Access, Intermediate System, Physical Access Control Systems,

---

[14] *See* NERC Petition at 13.

[15] On May 20, 2025, NERC submitted a supplemental petition identifying errata to proposed Reliability Standards CIP-006-7, CIP-007-7, CIP-008-7, CIP-009-7, and CIP-011-4, as well as additional justifications for technical concepts within the proposed Standards.

Physical Security Perimeter, Protected Cyber Asset, Removable Media, Reportable Cyber Security Incident, and Transient Cyber Asset).

7. NERC submitted 11 proposed CIP Reliability Standards and the associated violation risk factors and violation severity levels, implementation plans, and effective dates for the relevant CIP Standards.[16] Finally, NERC proposed the retirement of the corresponding versions of the currently effective Reliability Standards.[17]

8. Specifically, NERC seeks Commission approval of the following 11 modified CIP Reliability Standards:

- CIP-002-7 (Cyber Security – BES Cyber System Categorization)
- CIP-003-10 (Cyber Security - Security Management Controls)[18]
- CIP-004-8 (Cyber Security – Personnel & Training)
- CIP-005-8 (Cyber Security – Electronic Security Perimeter(s))
- CIP-006-7.1 (Cyber Security – Physical Security of BES Cyber Systems)[19]

---

[16] The proposed Reliability Standards are not attached to this notice of proposed rulemaking (NOPR). The proposed Reliability Standards are available on the Commission's eLibrary document retrieval system in Docket No. RM24-8-000 and on the NERC website, www.nerc.com.

[17] *See* NERC Petition at 1-2. In addition to the virtualization-related modifications in the proposed Reliability Standards, NERC included administrative revisions throughout the proposed Reliability Standards. For example, some revisions aligned the proposed Reliability Standards to other Standards or NERC initiatives. *Id.* at 55-56.

[18] On December 24, 2024, NERC submitted a petition for approval of proposed Reliability Standard CIP-003-11 (Cyber Security - Security Management Controls), in Docket No. RM25-8-000. In the NOPR for Docket No. RM25-8-000 issued concurrent with this NOPR, the Commission proposes to take action on proposed Reliability Standard CIP-003-11, *Critical Infrastructure Protection Reliability Standard CIP-003-11*, 192 FERC ¶ 61,227 (2025).

[19] *See* NERC Supp. Petition at 3 (making errata corrections to several CIP Standards, designated with a ".1" in the version number, e.g., CIP-006-7.1).

- CIP-007-7.1 (Cyber Security – Systems Security Management)
- CIP-008-7.1 (Cyber Security – Incident Reporting and Response Planning)
- CIP-009-7.1 (Cyber Security – Recovery Plans for BES Cyber Systems)
- CIP-010-5 (Cyber Security – Configuration Change Management and Vulnerability Assessments)
- CIP-011-4.1 (Cyber Security – Information Protection)
- CIP-013-3 (Cyber Security – Supply Chain Risk Management)

9. NERC asserts that the proposed Reliability Standards would facilitate the use of the full range of virtualization technologies.[20] According to NERC, the proposed Reliability Standards would allow responsible entities to fully implement virtualization and address risks associated with virtualized environments, such as "side channel" attacks where virtual systems executing on the same hardware could affect one another.[21] NERC also states that the use of security objectives within the CIP Reliability Standards establishes a framework adaptable to newer technologies.[22]

10. NERC explains that its revisions would: (1) support different security models by adjusting language around perimeter-based models to accommodate other security models; (2) recognize "virtualization infrastructure and virtual machines through new and revised terms in the NERC Glossary;" (3) broaden "change management approaches beyond a baseline-only configuration to recognize the dynamic nature of virtualized technologies," e.g., where such virtualized systems are no longer installed on specific

---

[20] *See* NERC Petition at 4.

[21] NERC Petition at 4.

[22] *Id.* at 5.

servers; and (4) manage "accessibility and attack surfaces of a virtualized configuration."[23] In addition to the changes to facilitate virtualization, the proposed Reliability Standards incorporate clarifications found during the implementation of prior versions of the CIP Standards.[24]

11. NERC explains that to accommodate different security models, the proposed revisions would allow responsible entities to either continue to use a perimeter-model or more policy-based controls through virtual environments. For example, NERC explains that the requirement in currently effective Reliability Standard CIP-005-7 (to implement a perimeter-based network security model) limited responsible entities to a single security model, and so NERC proposed to revise the standard to focus on the security objective of securing communications to and from BES Cyber Systems. The standard drafting team updated language that removes the concepts of "inside" an electronic security perimeter and replaces it with broader language, such as "protected by" an electronic security perimeter and revised the definitions of Electronic Security Perimeter, Electronic Access Point, and External Routable Connectivity.[25]

12. To better recognize virtualization infrastructure and address how hardware relates to the software and data, NERC explains that the proposed Reliability Standards permit responsible entities to use protections that are appropriate and secure for virtualization by applying protections where they are needed rather than relying on a one-to-one relationship between hardware and software in the currently defined cyber assets. To

---

[23] *Id.*

[24] *Id.* at 6.

[25] *Id.* at 21-22.

account for virtual machines and their underlying infrastructure, the standard drafting team also revised the definition of Cyber Asset and Virtual Cyber Asset, Shared Cyber Infrastructure, Management Interface, and Cyber Systems.[26]

13. NERC explains that the proposed Reliability Standards broaden configuration change management to reflect characteristics of the technologies enabled by virtualization.[27] According to NERC, controlling configuration changes helps ensure that "neither adverse impacts nor unauthorized changes occur"[28] and that the proposed revisions to the Standards would let responsible entities "focus more on a forward-looking authorization of a change rather than a backward-looking baseline update for compliance purposes."[29]

14. Finally, NERC describes the updated approach to managing accessibility and reducing the attack surface in virtualized environments due to shared resources.[30] For example, where the currently-effective Reliability Standard CIP-007-6, Requirement R1 focuses on disabling or restricting unneeded ports or services, the proposed Reliability Standard CIP-007-7.1, Requirement R1, holds the security objective of preventing unneeded routable protocol network accessibility, thereby accommodating more varied security controls.

---

[26] NERC Petition at 22-24.

[27] *Id.* at 24-26.

[28] *Id.* at 25.

[29] *Id.* at 26.

[30] *Id.*

15. In addition to the virtualization modifications described above, NERC proposes to replace the phrase technical feasibility, which appears in nine Requirements of the currently effective CIP Standards, with the phrase per system capability.[31] NERC also proposes to add the phrase per system capability in six Requirements with no existing technical feasibility exception language.[32] NERC explains that the phrase per system capability is used to "account for different types of technology that will be expected to meet the security objective of a particular CIP Reliability Standard."[33] According to NERC, "should a Responsible Entity choose to rely on the new term, the Responsible Entity will need to document the limit to the system's capability and demonstrate during compliance monitoring activities that the system's incapability prevents the Responsible Entity from implementing the control within the requirement."[34] NERC adds that it and the Regional Entities have observed a significant decrease in the number of submitted technical feasibility exceptions and the replacement with the phrase per system capability would ease the administrative burden associated the current process.

16. NERC's proposed implementation plan provides that the proposed Reliability Standards and definitions shall become effective on the later of April 1, 2026, or the first day of the first calendar quarter that is 24 months after the effective date of the applicable governmental authority's order approving the Reliability Standards and definitions, or as

---

[31] NERC Petition at 28-29.

[32] In all, NERC proposes to add the phrase per system capability to proposed Reliability Standards as follows: CIP-005-8, Requirements R1.3, R1.4, R2; CIP-006-7.1, Requirement R1.3; CIP-007-7.1, Requirements R1.1, R4.1, R4.2, R4.3, R5.1, R5.4, R5.6, R5.7; CIP-009-7.1 Requirement R1.5; and CIP-010-5, Requirements R2.1, R3.2.

[33] NERC Petition at 28.

[34] NERC Supplemental Petition at 26.

otherwise provided for by the applicable governmental authority. NERC states that its proposed implementation plan balances the urgency to implement the requirements with the time needed to develop any relevant capabilities.[35]

III. Discussion

17. Pursuant to section 215(d)(2) of the FPA, we propose to approve the 11 proposed modified CIP Reliability Standards, as well as four newly proposed definitions and 18 proposed revisions to the definitions set forth in the NERC Glossary, as just, reasonable, not unduly discriminatory or preferential, and in the public interest. The proposed new and revised definitions should provide a clear and consistent understanding of the terms across all Reliability Standards. We also propose to approve the associated violation risk factors, violation severity levels, implementation plans, and effective dates of the 11 modified CIP Reliability Standards, as well as to approve the retirement of the associated currently effective Reliability Standards.

18. As described by NERC, the proposed CIP Reliability Standards would provide the opportunity for responsible entities to implement virtualization technologies in a secure manner. We are supportive of NERC's efforts to allow responsible entities to take advantage of the efficiencies and flexibilities afforded by virtualization and other emerging technologies, and encourage interested responsible entities to do so, while mindful of the need for a secure electric grid. We believe that the proposed modifications represent a necessary and forward-looking progression of cybersecurity requirements for the bulk electric system, designed to enhance reliability and accommodate technological advancements. While below we solicit comment regarding our concerns pertaining to

[35] NERC Petition at 59.

one proposed modification, we seek comments on all aspects of these proposed Reliability Standards and definitions.

19. The initial (version 1) set of eight CIP Reliability Standards, submitted by NERC in 2006, included the phrase technical feasibility to allow an exception from compliance with certain CIP Standard provisions based on the concern that strict compliance would force the early retirement of some long-life legacy equipment. In Order No. 706, the Commission approved the version 1 CIP Reliability Standards but expressed concern about self-implementing technical feasibility exceptions.[36] To assure accountability, the Commission directed NERC to develop procedures for an entity to seek approval by submitting an application to the ERO that includes justification for the technical feasibility exception, plans for alternative mitigation, and remediation plans to eventually eliminate use of the technical feasibility exception.[37] Order No. 706 also required that the ERO submit to the Commission an annual report on the use of technical feasibility exceptions and reliability impacts. NERC developed and the Commission approved the directed technical feasibility procedures.[38]

20. NERC now proposes to replace technical feasibility exception language within currently effective CIP Reliability Standards with the phrase per system capability. We are mindful that the NERC proposal would eliminate the administrative burden

---

[36] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 73 FR 7368 (Feb. 7, 2008), 122 FERC ¶ 61,040, *order on clarification*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 74 FR 12544 (Mar. 25, 2009), 126 FERC ¶ 61,229, *order deny'g request for clarification*, Order No. 706-C, 74 FR 30067 (Jun. 24, 2009), 127 FERC ¶ 61,273 (2009).

[37] *Id*. PP 192-194, 209-211, 222.

[38] *E.g.*, *N. Am. Elec. Reliability Corp*., 130 FERC ¶ 61,050 (2010).

associated with the technical feasibility exception process, which requires a responsible entity to submit a request with supporting documentation to a Regional Entity for review and approval. Nonetheless, we are concerned that the replacement language, "per system capability" within certain of the proposed CIP Reliability Standards, would allow responsible entities to self-implement an exception with marginal oversight and no alternative mitigation obligation, in contrast to the current accountability-based process for technical feasibility exceptions.[39]

21. As we understand NERC's petition, responsible entities declaring the new system capability exceptions must document them. This documentation must be made available if and when audited by a Regional Entity (or other compliance activity). We are concerned that under NERC's proposal neither the ERO nor the Commission would have any information on the number of exceptions that entities have taken and in what circumstances, except for those that were identified during an audit (or other compliance activity). Further, because neither the proposed Reliability Standards nor the NERC petition provides any definition or parameters for entities to self-declare a capability exception,[40] we are concerned about potential inconsistent outcomes both in the entity self-implementation and Regional Entity audits. Based on similar concerns, the

---

[39] *Id*. at section 3.2 ("A [Technical Feasibility Exception] does not relieve the Responsible Entity of its obligation to comply with the Applicable Requirement. Rather, a [Technical Feasibility Exception] authorizes an alternative … means of compliance with the Applicable Requirement through the use of compensating measures and/or mitigating measures that achieve at least a comparable level of security…."); *see also* Order No. 706, 122 FERC ¶ 61,040 at P 222.

[40] *Cf.*, *id*. at section 3.1 (delineating six parameters for seeking a Technical Feasibility Exception).

Commission has demurred on previous proposals to allow self-implementing CIP exceptions.[41]

22. Moreover, we note that the technical feasibility exception process was initiated in the earliest versions of the CIP Reliability Standards to primarily address legacy equipment that was incapable of CIP compliance without early retirement or other unduly burdensome costs.[42] It has been over 15 years since NERC began to approve technical feasibility exceptions; thus, it is reasonable to think that legacy equipment would have been replaced, absolving the need for *any* sort of exception language. Yet technical feasibility exceptions continue.[43]

23. In light of the above discussion, we are inclined to direct that NERC develop modifications that would either remove any form of exception (i.e., technical feasibility and per system capability) or reinstate the technical feasibility language. Considering the

---

[41] *See, e.g.*, Order No. 706, 122 FERC ¶ 61,040 at P 150 (directing NERC to remove "acceptance of risk" language from CIP Standards because the term represents "an uncontrolled exception from compliance that creates unnecessary uncertainty about the existence of potential vulnerabilities. Responsible entities should not be able to opt out of compliance with mandatory Reliability Standards"); *Version 5 CIP Standards Infrastructure Protection Reliability Standards,* Order No. 791, 78 FR 72756 (Dec. 3, 2013), 145 FERC ¶ 61,160, at PP 67-71 (2013) (rejecting proposed "identify, assess, and correct" language within CIP Standards as "ambiguous and results in an unacceptable amount of uncertainty with regard to consistent application, responsible entities understanding their obligations, and NERC and the regions providing consistent application in audits and other compliance settings.").

[42] *See* Order No. 706, 122 FERC ¶ 61,040 at P 181 (explaining that "the justification for technical feasibility exceptions is rooted in the problem of long-life legacy equipment and the economic considerations involved in the replacement of such equipment before the end of its useful life" and eventually all equipment should achieve full compliance when legacy equipment is retired or upgraded).

[43] *See N. Am. Elec. Reliability Corp.*, Annual Report of the North American Electric Reliability Corporation on Wide-Area Analysis of Technical Feasibility Exceptions, Docket Nos. RR10-1-000, RR13-3-000 at 7-8 (filed Sept. 27, 2024).

maturity of the technical feasibility exception program over the past 15 years and NERC's interest in minimizing the administrative burden, the Commission is also interested in comments on a potential streamlined process that satisfies the fundamental needs for consistency, oversight and alternative mitigation. To assist the Commission in determining the need for a directive on this matter in a final rule and fashioning its content, we seek comment on the following three areas of inquiry.

24. First, regarding the efficacy of the technical feasibility exception program: (1) why is there still a need to maintain an exception process for legacy equipment after 15 years; and (2) specify the administrative burdens associated with the current Technical Feasibility Exception program—have the burdens changed with the maturity of the program?

25. Second, regarding the proposed per system capability language, do NERC or stakeholders anticipate that the proposed CIP changes to accommodate virtualization technology would result in responsible entities seeking new exceptions using the per system capability language (beyond the legacy technical feasibility exceptions)? For new exceptions: (1) how will NERC and/or the Regional Entities monitor system capability exceptions other than through CIP compliance activities (i.e., audits); (2) what parameters or guidance will inform responsible entities on legitimate circumstances to self-implement a system capability exception; (3) what obligations does a responsible entity have to implement alternative mitigation measures in lieu of strict compliance;[44] and

[44] *See* NERC Rules of Procedure App. 4D at 3.2 (stating that a technical feasibility exception does not relieve an entity from a CIP compliance obligation but rather authorizes an *alternative* to strict compliance).

(4) how will NERC assure consistency in the review of system capability exceptions across all Regional Entities?

26. Third, we seek comment on possible alternative approaches that would streamline the process while also satisfying the need for effective regulatory oversight. For example, we would be interested in comments on an approach that would streamline the administrative burden of the current technical feasibility exception process for system capability exceptions while maintaining a requirement to mitigate the noncompliance and reporting of exceptions (and material changes thereto) to the applicable Regional Entity. Comments supporting an alternative approach should include an estimate of the administrative burden, the periodicity for reassessment (if any) and Regional Entity validation (if any), and any other relevant features or details (e.g., reporting requirements to the Commission).

IV. Information Collection Statement

27. The Commission bases its paperwork burden estimates on the additional paperwork burden presented by the proposed revisions to Reliability Standards filed by NERC for Commission approval. Proposed revisions focus on security objectives rather than specific controls for system security management to accommodate virtualized environments. Proposed Reliability Standards are objective-based and allow entities to choose compliance approaches best tailored to their systems. The proposed revisions to the CIP Reliability Standards would allow responsible entities the opportunity to take advantage of the benefits of advanced virtualization features while also preserving their choice to maintain current secure perimeter-based network architecture, which continues to be a valid network security model.

28. Proposed Reliability Standards do not require responsible entities to submit any filings with either the Commission or NERC as the ERO. Entities, however, are required to maintain documentation adequate to demonstrate compliance with the proposed Reliability Standards. Commission and NERC staff conduct periodic audits of entities and auditors rely on the entity's documentation in determining compliance with Reliability Standards. While entities retain flexibility on how they choose to demonstrate compliance, the Reliability Standards include Compliance Measures providing examples of the type of documentation an entity may want to develop and maintain to demonstrate compliance. The reporting burden below is based on the Compliance Measurements provided in the revised Reliability Standards.

29. As of June 2025, the NERC Compliance Registry identifies approximately 1,673 unique U.S. entities that are subject to mandatory compliance with CIP Reliability Standards. All 1,673 entities would need to conform to modifications proposed under Reliability Standard CIP-002-7. However, as stated in NERC petition, the revisions in proposed Reliability Standard CIP-002-7 are minor, mostly aligning the standard with updates to the NERC Glossary.[45] Therefore, we do not envision an increased paperwork burden specifically pertaining to any modifications in proposed Reliability Standard CIP-002-7. However, of the 1,673 total entities, we estimate that 400 entities will face an increased paperwork burden under the revisions proposed in Reliability Standards CIP-003-10, CIP-004-8, CIP-005-8, CIP-006-7.1, CIP-007-7.1, CIP-008-7.1, CIP-009-7.1, CIP-010-5, CIP-011-4.1, and CIP-013-3. Based on these assumptions, the estimated reporting burden is as follows:

[45] NERC Petition at 38.

Total Changes Proposed by the NOPR in Docket RM24-8-000[46]						
	Number of Respondents (1)	Annual Number of Responses per Respondent (2)	Total Number of Responses (1)*(2)=(3)	Average Burden & Cost Per Response[47] (4)	Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)	Cost per Respondent ($) (5)÷(1)
Conforming to	1673	1	1673	Commission does not	Commission does not	Commission does not

[46] The paperwork burden estimate includes costs associated with the initial development of a policy to address the requirements.

[47] This burden applies in Year One to Year Three.

The loaded hourly wage figure (includes benefits) is based on the average of three occupational categories for May 2024 Wages found on the Bureau of Labor Statistics website (http://www.bls.gov/oes/current/naics2_22.htm). The loaded hourly wage includes fringe benefits divided by 81.70 percent. *See* https://data.bls.gov/oes/#/industry/000000:

Legal Occupations (90th percentile) (Occupation Code: 23-0000): $140.76.

Electrical Engineer (mean) (Occupation Code: 17-2071): $71.19.

Office and Administrative Support (90th percentile) (Occupation Code: 43-0000): $43.83

($140.76 + $71.19 + $43.83) ÷ 3 = $85.26.

The figure is rounded to $85.00 for use in calculating wage figures in this NOPR.

Total Changes Proposed by the NOPR in Docket RM24-8-000[46]						
	Number of Respondents (1)	Annual Number of Responses per Respondent (2)	Total Number of Responses (1)*(2)=(3)	Average Burden & Cost Per Response[47] (4)	Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)	Cost per Respondent ($) (5)÷(1)
modifications proposed under Reliability Standard CIP-002-7				anticipate any material information collection costs associated with CIP-002-7.	anticipate any material information collection costs associated with CIP-002-7.	anticipate any material information collection costs associated with CIP-002-7.
Update compliance related documentation of one	400	1	400	577 hrs.; $49,045	230,800 hrs.; $19,618,000	$49,045

Total Changes Proposed by the NOPR in Docket RM24-8-000[46]						
	Number of Respondents (1)	Annual Number of Responses per Respondent (2)	Total Number of Responses (1)*(2)=(3)	Average Burden & Cost Per Response[47] (4)	Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)	Cost per Respondent ($) (5)÷(1)
or more process(es) pertaining to proposed Reliability Standards: CIP-003-10, CIP-004-8, CIP-005-8, CIP-006-7.1, CIP-007-7.1, CIP-008-7.1,						

Total Changes Proposed by the NOPR in Docket RM24-8-000[46]						
	Number of Respondents (1)	Annual Number of Responses per Respondent (2)	Total Number of Responses (1)*(2)=(3)	Average Burden & Cost Per Response[47] (4)	Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)	Cost per Respondent ($) (5)÷(1)
CIP-009-7.1, CIP-010-5, CIP-011-4.1, and CIP-013-3						
Total burden			400		230,800 hrs.; $19,618,000	$49,045

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

• Year 1-3 total: 400 responses; 230,800 hours.

The annual cost burden for each year One to Three is $6,539,333.

V. Environmental Analysis

30. 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.[48] 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.[49] The actions proposed herein falls within this categorical exclusion in the Commission's regulations.

VI. Regulatory Flexibility Act Analysis

31. The Regulatory Flexibility Act of 1980 (RFA)[50] generally requires a description and analysis of proposed rules that will have significant economic impact on a substantial number of small entities. The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.[51] The SBA revised its size standard for electric utilities (effective March 17, 2023) to a standard based on the number of employees, including affiliates (from the prior standard based on megawatt

---

[48] *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).

[49] 18 CFR 380.4(a)(2)(ii).

[50] 5 U.S.C. 601-612.

[51] 13 CFR 121.101.

hour sales).[52]

32. The SBA sets the threshold for what constitutes a small business. Under SBA's size standards, transmission owners all fall under the category of Electric Bulk Power Transmission and Control (NAICS code 221121), with a size threshold of 950 employees (including the entity and its associates). Based on the Compliance Registry, we have selected Generator Owner (GO) and Generator Operator (GOP) entities applicable of 288 entities and we have determined that approximately 87% GOs and 67% GOPs of the listed entities are small entities (i.e., with fewer than 950 employees).

33. According to SBA guidance, the determination of significance of impact "should be seen as relative to the size of the business, the size of the competitor's business, the number of filers received annually, and the impact this regulation has on larger competitors."[53]

34. Moreover, this NOPR involves voluntary actions by utilities for the purpose of accommodating virtualized environments. The proposal does not mandate or require action by any utility other than updating compliance documentation for processes related to the proposed Reliability Standards. As a result, we certify that the proposals in this NOPR will not have a significant economic impact on a substantial number of small entities.

35. NERC developed the proposed revisions through its consensus-based standard drafting and approval processes. The proposed revisions are expected to impose minimal obligations on the affected responsible entities. These burdens primarily involve updating compliance documentation for processes related to the proposed Reliability

---

[52] 13 CFR 121.201, Subsector 221 (Utilities).

[53] U.S. Small Business Admin., *A Guide for Government Agencies How to Comply with the Regulatory Flexibility Act*, 18 (Aug. 2017), https://advocacy.sba.gov/wp-content/uploads/2019/06/How-to-Comply-with-the-RFA.pdf.

Standards since the proposed revisions permit responsible entities the opportunity to take advantage of the benefits of advanced virtualization features while also preserving their choice to maintain current secure perimeter-based network architecture, which continues to be a valid network security model. We believe that because the obligations imposed upon industry are directed only at entities that own or operate high-impact or medium-impact BES Cyber Systems, only a minimal number of entities will meet the SBA revised standard for electric utilities. Only a minimal number of entities will satisfy the SBA revised standard because small entities do not typically own or operate any kind of high or medium impact BES Cyber Systems.

VII. Regulatory Planning and Review

36. 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 proposed regulatory action is not a "significant regulatory action," under section 3(f) of Executive Order 12866, as amended. Accordingly, OIRA has not reviewed this proposed regulatory action for compliance with the analytical requirements of Executive Order 12866.

VIII. Comment Procedures

37. The Commission invites interested persons to submit comments on the matters and issues proposed in this notice to be adopted, including any related matters or alternative proposals that commenters may wish to discuss. Comments are due **[INSERT DATE 60**

DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

Comments must refer to Docket No. RM24-8-000, 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.

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

39. 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.

IX. Document Availability

40. 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).

41. 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.

42. 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.

By direction of the Commission.

Issued: September 18, 2025.

Carlos D. Clay,

Deputy Secretary.

[FR Doc. 2025-18395 Filed: 9/22/2025 8:45 am; Publication Date: 9/23/2025]