

194 FERC ¶ 61,209
DEPARTMENT OF ENERGY
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM24-8-000; Order No. 919]

Virtualization Reliability Standards

(Issued March 19, 2026)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule.

SUMMARY: The Federal Energy Regulatory Commission (Commission) approves 11 modified Critical Infrastructure Protection (CIP) Reliability Standards. The Commission also approves four new definitions and 18 modified definitions in the North American Electric Reliability Corporation (NERC) Glossary of Terms Used in Reliability Standards. To address concerns regarding a proposed self-implementing exception phrase (“per system capability”) that appears in multiple provisions of the modified CIP Reliability Standards, the Commission directs NERC to develop a clear set of criteria that satisfies the fundamental needs for oversight, consistency, and alternative mitigation when a responsible entity invokes the per system capability exception. NERC, the Commission-certified Electric Reliability Organization (ERO), 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: This rule is effective [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

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

Hampden T. Macbeth (Legal Information)
Office of General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-8957
Hampden.Macbeth@ferc.gov

SUPPLEMENTARY INFORMATION:

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

Virtualization Reliability Standards

Docket No. RM24-8-000

ORDER NO. 919

FINAL RULE

(Issued March 19, 2026)

1. Pursuant to section 215(d)(2) of the Federal Power Act (FPA),¹ the Federal Energy Regulatory Commission (Commission) approves 11 Critical Infrastructure Protection (CIP) Reliability Standards as well as the addition of four new and 18 proposed revisions to the North American Electric Reliability Corporation (NERC) Glossary of Terms Used in Reliability Standards (NERC Glossary). We also approve the associated violation risk factors, violation severity levels, implementation plans, and effective dates for the proposed Reliability Standards. In addition, we approve the retirement of the currently effective version of each proposed Reliability Standard. We approve the proposed definitions and 11 proposed Reliability Standards because collectively they will allow responsible entities the opportunity to adopt virtualization, improving the reliability of the

¹ 16 U.S.C. 824o(d)(2).

Bulk-Power System by providing significant cyber security benefits and flexibility in responding to cyber threats.

2. 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 As stated in the notice of proposed rulemaking (NOPR),³ 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, "[T]echnology 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. We agree that these potential

² See NERC Petition at 2-5.

³ *Virtualization Reliability Standards*, Notice of Proposed Rulemaking, 90 FR 45679 (Sept. 23, 2025), 192 FERC ¶ 61,228 (NOPR).

⁴ NERC Petition at 2.

⁵ *Id.*

reliability benefits are worth pursuing, and 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. However, as explained in the NOPR, we remain concerned that the proposed language (repeated in multiple Requirements) that would replace the phrase “where technically feasible”⁶ with the phrase “per system capability”⁷ would eliminate transparency and meaningful Commission and NERC oversight by introducing a self-implementing exceptions process with no reporting obligations.⁸ To address this concern, the Commission directs NERC to (1) develop a clear set of criteria that promote consistency and ensure that responsible entities understand the parameters for invoking the per system capability exception and the obligation to implement alternative mitigation; (2) develop mandatory reporting requirements to the Electric Reliability

⁶ See NERC Rules of Procedure, app. 4(d) (Procedure for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Standards), Section 3.0 (setting forth circumstances in which a technical feasibility exception may be warranted). See also *id.* Section 3.2 (“[A] TFE authorizes an alternative (to Strict Compliance) 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.”).

⁷ While NERC does not propose to define the term per system capability for the NERC Glossary, NERC explains in its Petition that “[t]he phrase ‘per system capability’ means that if a Responsible Entity can demonstrate that the applicable system is incapable of performing a required action (e.g., a firmware-based “black box” device with limited configuration capabilities),” then the responsible entity does not have to meet the CIP Requirement and will determine on its own an equally effective alternative mitigation measure. NERC Petition at 46-47.

⁸ See NOPR, 192 FERC ¶ 61,228 at PP 21-26.

Organization (ERO) Enterprise (i.e., the relevant Regional Entity, NERC, or both) for responsible entities that invoke the per system capability language; and (3) submit an annual report to the Commission that includes anonymized, aggregated data that indicates how entities are utilizing the exception language. These three elements will provide adequate ERO and Commission oversight, consistency in application, and assurance that entities implement appropriate alternative mitigation when invoking the per system capability exception. As discussed later, we are not directing NERC to modify the CIP Reliability Standards but rather leave to NERC's discretion the mechanism for development of the required criteria, i.e., through changes to the NERC Rules of Procedure, changes to the NERC guidance documents, modifications to the Reliability Standards, or some other mechanism. Moreover, while we direct NERC to develop mandatory reporting, we do not require that NERC develop an approval process akin to the current CIP technical feasibility exception process.

I. Background

A. Section 215 of the FPA and Mandatory Reliability Standards

4. Section 215 of the FPA provides that the Commission may certify an ERO, the purpose of which is to 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

⁹ 16 U.S.C. 824o(c).

¹⁰ *Id.* 824o(e).

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 Virtualization allows the sharing of hardware, central processing units, memory, storage, and other resources among various operating systems (i.e., guest operating systems).¹⁴ A virtual machine is a software version of a single physical computer and performs all the same functions.¹⁵ Containers are a virtualization concept and are considered software that encapsulate applications and their dependencies in isolated environments, separate from other applications or containers.¹⁶

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 and 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) (citing NIST Virtualization Security Special Publication).

¹⁴ NOPR, 192 FERC ¶ 61,228 at P 5 (citing NERC Petition at 13).

¹⁵ *Id.*

¹⁶ *Id.*

C. Technical Feasibility Exceptions and Order No. 706

6. As implemented by NERC in its Rules of Procedure, a technical feasibility exception is an alternative to strict compliance with a CIP Requirement through compensating measures and/or mitigating measures that achieve a comparable level of security for the bulk electric system (BES).¹⁷ Order No. 706 established technical feasibility exceptions to prevent the premature retirement or costly replacement of long-life, legacy operational technology that lacked the inherent technical capability to comply with Requirements in version 1 of the CIP Reliability Standards.¹⁸ Further, to assure accountability, the Commission in Order No. 706 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.¹⁹ As a result, when it is not able to satisfy strict compliance with a CIP

¹⁷ NERC Rules of Procedure, app. 4(d), § 3.2.

¹⁸ *Critical Infrastructure Protection*, Order No. 706, 73 FR 7368 (Feb. 7, 2008), 122 FERC ¶ 61,040, at P 181, *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)).

¹⁹ NOPR, 192 FERC ¶ 61,228 at P 19 (citing Order No. 706, 122 FERC ¶ 61,040 at PP 192-194, 209-211, 222).

Requirement, a responsible entity may now request and obtain approval for a technical feasibility exception that will not compromise safety in one of six listed circumstances.²⁰

D. NERC Petition and Supplement

7. On July 10, 2024, as supplemented on May 20, 2025,²¹ NERC submitted for Commission approval 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.²² NERC also submitted 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 proposed revisions to 18 defined terms within the NERC

²⁰ NERC Rules of Procedure, app. 4(d), § 3.0.

²¹ 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.

²² The proposed Reliability Standards are not attached to this final rule. 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.

Glossary.²³ Finally, NERC proposed the retirement of the corresponding versions of the currently effective Reliability Standards.²⁴

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

- CIP-002-7 (Cyber Security – BES Cyber System Categorization)²⁵
- CIP-003-10 (Cyber Security – Security Management Controls)²⁶
- CIP-004-8 (Cyber Security – Personnel & Training)
- CIP-005-8 (Cyber Security – Electronic Security Perimeter(s))

²³ The 18 defined terms subject to revision include: 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, Physical Security Perimeter, Protected Cyber Asset, Removable Media, Reportable Cyber Security Incident, and Transient Cyber Asset.

²⁴ See NERC Petition at 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.

²⁵ On December 20, 2024, NERC submitted a petition for approval of the modification of the definition of control center in the NERC Glossary and Reliability Standard CIP-002-8 (Cyber Security – BES Cyber System Categorization). We are approving the proposed control center definition and proposed Reliability Standard CIP-002-8 in a concurrent order. *N. Am. Elec. Reliability Corp.*, 194 FERC 61,211 (2026).

²⁶ On December 20, 2024, NERC submitted a petition for approval of proposed Reliability Standard CIP-003-11 (Cyber Security - Security Management Controls). We are approving proposed Reliability Standard CIP-003-11 in a concurrent order. *Critical Infrastructure Protection Reliability Standard CIP-003-11*, 194 FERC ¶ 61,210 (2026).

- CIP-006-7.1 (Cyber Security – Physical Security of BES Cyber Systems)²⁷
- 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. According to NERC, the Reliability Standards would allow responsible entities to fully implement virtualization and address risks associated with virtualized environments.²⁸ NERC also stated that the use of security objectives within the CIP Reliability Standards would establish a framework adaptable to newer technologies.²⁹

10. NERC explained 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

²⁷ 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).

²⁸ NERC Petition at 4.

²⁹ *Id.* at 5.

technologies,” e.g., where such virtualized systems are no longer installed on specific servers; and (4) manage “accessibility and attack surfaces of a virtualized configuration.”³⁰

11. In addition to the virtualization modifications described above, NERC proposed 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 proposed to add the phrase per system capability in six Requirements with no existing technical feasibility exception language. NERC explained that the phrase per system capability means that if a responsible entity can demonstrate that the applicable system is incapable of performing a required action (e.g., a firmware-based “black box” device with limited configuration capabilities), then the responsible entity does not have to meet the CIP Requirement and will determine on its own an equally effective alternative mitigation measure.³² NERC explained that the phrase per system capability is used to “account for the 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 that term, the Responsible Entity will need to document the limit to the system’s capability and demonstrate during compliance

³⁰ *Id.*

³¹ *Id.* at 28-29.

³² *Id.* at 46-47.

³³ *Id.* at 29.

monitoring activities that the system's incapability prevents the Responsible Entity from implementing the control within the requirement."³⁴ NERC added that it and the Regional Entities have observed a significant decrease in the number of submitted technical feasibility exceptions and replacement with the phrase per system capability would ease the administrative burden associated with the current process.

12. NERC's implementation plan provides that the Reliability Standards and definitions will 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 otherwise provided for by the applicable governmental authority. The implementation plan also allows responsible entities to comply with the proposed Reliability Standards prior to their effective date, after Commission approval, by notifying their Regional Entities. Early adoption can occur on one of three instances: six, 12, or 18 months after the effective date of this final rule. NERC stated that the implementation plan balances the urgency to implement the requirements with the time needed to develop any relevant capabilities.³⁵

E. NOPR

13. On September 18, 2025, the Commission issued the NOPR, proposing to approve the 11 modified virtualization Reliability Standards; the associated violation risk factors,

³⁴ NERC Supp. Petition at 26.

³⁵ NERC Petition at 59-60.

violation severity levels, implementation plans, and effective dates for the proposed Reliability Standards; the retirement of the currently effective version of each proposed Reliability Standard; and 22 new or modified definitions in the NERC Glossary.³⁶ The NOPR stated that the Commission supported NERC's work to update the CIP Reliability Standards to accommodate virtualization to enhance reliability.³⁷ However, the Commission expressed concern that the replacement of the technical feasibility exception program in the current CIP Reliability Standards with the proposed phrase per system capability would eliminate transparency and oversight.³⁸ Consequently, the Commission sought comments on the efficacy of the technical feasibility exception program and on the proposed per system capability language.³⁹ In response, the following seven entities submitted timely comments: Bonneville Power Administration (BPA); Edison Electric Institute (EEI); GE Vernova; Midcontinent Independent System Operator (MISO); Midwest Reliability Organization NERC Standards Review Forum (MRO NSRF); NERC; and Portland General Electric (PGE).

II. Discussion

14. Pursuant to section 215(d)(2) of the FPA, we adopt the NOPR proposal and approve the 11 proposed modified virtualization Reliability Standards and the four new

³⁶ NOPR, 192 FERC ¶ 61,228 at P 1.

³⁷ *Id.* P 2.

³⁸ *Id.* P 3.

³⁹ *Id.* PP 24-26.

proposed definitions and 18 proposed modified definitions in the NERC Glossary.

Below, we discuss the following matters: (A) our approval of the virtualization Reliability Standards; (B) directives related to the per system capability exception; and (C) our approval of the NERC Glossary definitions.

A. Virtualization Reliability Standards

1. NOPR

15. In the NOPR, the Commission proposed to approve NERC's petition as supplemented as just, reasonable, not unduly discriminatory or preferential, and in the public interest.⁴⁰ The Commission supported NERC's efforts to allow responsible entities to take advantage of the efficiencies and flexibilities afforded by virtualization and other emerging technologies, and encouraged interested responsible entities to do so, while being mindful of the need for a secure electric grid. The Commission saw NERC's proposed modifications as a necessary and forward-looking progression of cybersecurity requirements for the bulk electric system, designed to enhance reliability and accommodate technological advancements. The Commission also proposed 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.⁴¹

⁴⁰ *Id.* P 17.

⁴¹ *Id.*

2. Comments

16. Commenters generally support approval of the 11 modified CIP Reliability Standards.⁴² Specifically, commenters support the package of modifications because the modifications will allow responsible entities to adopt virtualization, which provides significant cyber security benefits and flexibility in responding to cyber threats and allows for the secure adoption of emerging technology.⁴³ For example, EEI states “The Commission should adopt these modifications because . . . [v]irtualization offers significant benefits including improved security posture through isolation and segmentation, greater resilience by reducing hardware dependency, and enhanced flexibility for adapting to evolving threats and operational needs.”⁴⁴

3. Commission Determination

17. Pursuant to section 215(d)(2) of the FPA, we approve the 11 proposed modified CIP Reliability Standards as just, reasonable, not unduly discriminatory or preferential, and in the public interest. Specifically, the 11 proposed virtualization Reliability Standards provide the opportunity for responsible entities to take advantage of the efficiencies and flexibilities afforded by virtualization in a secure manner. Further, we determine that the package of Reliability Standards is a forward-looking progression of

⁴² See BPA Comments at 1; EEI Comments at 3; GE Vernova at 1; MISO Comments at 1; NERC Comments at 2; PGE Comments at 1 (supporting the entirety of EEI Comments).

⁴³ EEI Comments at 3; NERC Comments at 2.

⁴⁴ EEI Comments at 3.

cybersecurity requirements for the Bulk-Power System, which will enhance the current reliability of the Bulk-Power System and accommodate future technological developments. We also approve the associated violation risk factors, violation severity levels, implementation plans, and effective dates of the 11 modified CIP Reliability Standards, as well as approve the retirement of the associated currently effective Reliability Standards.

B. Per System Capability Exception Process

1. NOPR

18. The Commission expressed concern in the NOPR that the proposed per system capability language “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.”⁴⁵ The Commission further explained 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.”⁴⁶

19. The Commission asked for comments on: (1) the efficacy of the existing technical feasibility exception program; (2) the parameters of the proposed per system capability language; and (3) alternative approaches “that would streamline the process while also

⁴⁵ NOPR, 192 FERC ¶ 61,228 at P 20.

⁴⁶ *Id.* P 21.

satisfying the need for effective regulatory oversight.”⁴⁷ The Commission stated that the comments would assist the Commission in determining the need for a directive in a final rule and its content.

2. Comments

20. Commenters claim that an exception process is still necessary 15 years after the development of the technical feasibility exception process to accommodate legacy and emerging technologies.⁴⁸ EEI explains that existing and emerging technologies cannot satisfy certain CIP Reliability Standards requirements due to “inherent design limitations.”⁴⁹ MRO NSRF states satellite clocks and door control panels for physical access control systems are unable to meet some of the CIP Requirements and would have no opportunity for mitigation without an exception.⁵⁰ BPA asserts that exceptions are also necessary because immediately replacing legacy equipment to comply with the CIP Reliability Standards on a particular system could affect a specific security control’s interoperability with other systems.⁵¹

⁴⁷ *Id.* P 26.

⁴⁸ BPA Comments at 1; EEI Comments at 1, 5; MISO Comments at 2; MRO NSRF Comments at 1; *see also* PGE Comments at 2 (stating its preference for per system capability exceptions).

⁴⁹ EEI Comments at 5.

⁵⁰ *See* MRO NSRF Comments at 1.

⁵¹ BPA Comments at 3.

21. Consequently, commenters believe that the per system capability language should be approved to ease burdens associated with the current technical feasibility exception process and to speed the adoption of new technologies.⁵² EEI urges the adoption of the proposed per system capability language because it will enable utilities to “self-assess and document inherent limitations” rather than seeking approval or re-approval of formal exceptions under the technical feasibility exception process that may delay implementation of security measures,⁵³ while preserving oversight, and enabling operational flexibility for utilities deploying virtualization.⁵⁴ MISO notes that its technical feasibility exception process is burdensome because it requires a lengthy, multistep process for securing an exception.⁵⁵ NERC asserts that the per system capability language will help ensure that the proposed CIP Reliability Standards are forward-looking and enable the secure adoption of new technologies.⁵⁶

22. MISO, MRO NSRF, and NERC believe that the adoption of the per system capability language will not lead to an increase in new exception requests from

⁵² EEI Comments at 1; MRO NSRF Comments at 2; PGE Comments at 4.

⁵³ EEI Comments at 4. EEI states that responsible entities must seek re-approval when adding assets to an existing technical feasibility exception, even when mitigation strategies remain unchanged. *Id.* See also MRO NSRF Comments at 4.

⁵⁴ EEI Comments at 3.

⁵⁵ MISO Comments at 3.

⁵⁶ NERC Comments at 3. NERC maintains that the terminology “does not act like an exception” because the language “does not absolve an entity from implementing methods to achieve the security objective for applicable systems.” *Id.*

responsible entities beyond those under the technical feasibility exception process. MISO suggests that the proposed changes to the NERC CIP Standards to accommodate virtualization will allow entities “the ability to build their infrastructure in a manner that reduces the need for [exceptions].”⁵⁷ NERC points to the stability of the technical feasibility exceptions in recent years and states that it does not anticipate the trend significantly shifting with the change to per system capability.⁵⁸ In contrast, EEI indicates the use of new exceptions is necessary because some emerging technologies will not be able to meet CIP requirements.⁵⁹ Using the example of protective relays, EEI avers that “[a]s standards evolve to mandate [advanced cybersecurity] capabilities, entities will increasingly need [an] exceptions process” to accommodate equipment limitations.⁶⁰

23. MISO proposes that NERC establish and maintain “a centralized repository of common, industry-wide exceptions” for monitoring new system capability exceptions other than through CIP compliance activities (i.e., audits) by cataloging Cyber Assets that have historically been unable to comply with CIP Requirements, documenting accepted mitigation strategies and compensating controls; and facilitating knowledge sharing.⁶¹

⁵⁷ MISO Comments at 4.

⁵⁸ NERC Comments at 4-5.

⁵⁹ EEI Comments at 5.

⁶⁰ *Id.*

⁶¹ MISO Comments at 4-5.

MISO claims the proposed repository would minimize redundant technical feasibility exception submissions; promote consistency and transparency in the application and review of exceptions; and enable the retirement of exceptions as capabilities evolve or new solutions are identified.⁶²

24. MISO additionally proposes that NERC develop a System Capability Exception Program (SCEP), which responsible entities can implement internally with the support of new and existing guidance documents. MISO suggests that NERC could develop implementation guidance to support such a program.⁶³ MISO asserts that the SCEP would need to include program expectations (e.g., scope of exceptions), required program elements (e.g., compensating controls), and management tools.

25. However, other commenters indicate that new system capability exceptions can be sufficiently monitored through traditional CIP Reliability Standards compliance activities. EEI and MRO NSRF assert that NERC can use existing compliance mechanisms, such as audits, spot-checks, evidence reporting, and data gathering through NERC's evidence request tool to monitor implementation.⁶⁴ NERC states that Regional Entities could use the Align tool to collect information on devices that do not have the

⁶² *Id.* at 5.

⁶³ *Id.* at 6.

⁶⁴ EEI Comments at 6-7; MRO NSRF Comments at 3. *See also* BPA Comments at 4.

capability to implement CIP requirements in the context of audit preparation, self-certifications, and development of Inherent Risk Assessments.⁶⁵

26. EEI and MRO NSRF recommend that, if the Commission retains the current technical feasibility exception process, the process be streamlined by eliminating the requirement that responsible entities seek re-approval when adding assets to an existing technical feasibility exception because the mitigation measures and risk rationale would remain unchanged, while enabling timely upgrades and preserving security.⁶⁶ PGE recommends adopting the per system capability language and developing a streamlined process that would require responsible entities to provide data on the number of, and reasoning for, self-identified exceptions to the ERO Enterprise for visibility with no pre-approval requirement. PGE asserts that its proposed streamlined approach would avoid delays in the implementation of virtualization and eliminate both: (1) the need to modify the CIP Reliability Standards through the standard development process; and (2) the re-approval requirement for technical feasibility exceptions.⁶⁷

⁶⁵ NERC Comments at 6.

⁶⁶ Both EEI and MRO NSRF provide the same example: when installing a new physical access control systems door controller panel in a newly established physical security perimeter, the same technical feasibility exceptions conditions and mitigations apply. EEI Comments at 7; MRO NSRF Comments at 4.

⁶⁷ PGE Comments at 3-4.

3. Commission Determination

27. We are persuaded by commenters that an exception process is still needed for existing and emerging technologies. Indeed, some existing technologies are unable to meet certain CIP Requirements and would be out of compliance with no mitigation opportunity without an exception process.⁶⁸ Additionally, we recognize BPA's concern that eliminating an exception for legacy equipment may pose a risk to reliability because implementing a specific security control on a particular system could affect its interoperability with other systems needed to ensure reliability.⁶⁹

28. Further, we believe that the exception process merits streamlining. As noted by commenters, the current technical feasibility exception process requires responsible entities to seek approval or re-approval of exceptions from the ERO that can delay implementation of security measures that strengthen reliability.⁷⁰ Accordingly, with our approval of the package of 11 proposed virtualization Reliability Standards, NERC's proposed per system capability exception will replace the technical feasibility exception process.

29. However, we are not persuaded by the explanation of NERC and other commenters that the per system capability language adequately addresses the concerns raised in the NOPR regarding the fundamental needs for oversight, consistency, and

⁶⁸ EEI Comments at 5; MRO NSRF Comments at 1.

⁶⁹ BPA Comments at 3.

⁷⁰ EEI Comments at 4; MRO NSRF Comments at 4.

alternative mitigation in a CIP exceptions program.⁷¹ These concepts stem from the Commission's initial approval of the version 1 CIP Reliability Standards in Order No. 706, in which the Commission explained that the technical feasibility exceptions "must be governed by a clear set of criteria."⁷²

30. NERC proposed the use of the phrase per system capability after recognizing the significant administrative burden the technical feasibility exception process places on responsible entities and the Regional Entities.⁷³ While NERC's proposed per system capability exception language does reduce the administrative burden placed on responsible entities and Regional Entities, we find that currently it lacks clearly defined parameters in which responsible entities can invoke a per system capability exception. We determine that the lack of clearly defined parameters for invoking a per system capability exception denies the Commission, the ERO Enterprise, and responsible entities the certainty needed to oversee, administer, and participate in the per system capability exception program, respectively.

31. We are not persuaded by arguments that the Commission should rely solely on NERC's Compliance Monitoring and Enforcement Program engagements, such as compliance audits and spot-checks of responsible entities, to provide adequate oversight of the use of the per system capability language. Moreover, at the outset of the

⁷¹ NOPR, 192 FERC ¶ 61,228 at PP 19-21, 25.

⁷² Order No. 706, 122 FERC ¶ 61,040 at P 209.

⁷³ See NERC Petition at 29.

self-implementing exception program, there is no track record on the circumstances in which responsible entities will invoke per system capability exceptions or parameters for acceptable mitigation measures implemented by responsible entities as an alternative to strict compliance with the CIP Requirements where a per system capability exception will be invoked. We are not assuaged by the statements of NERC and other commenters that the per system capability language will simply carry on the legacy exceptions from the technical feasibility exception program,⁷⁴ as the proposed CIP Standards add per system capability language to six additional CIP Standards that previously lacked exception language.⁷⁵ Moreover, while NERC asserts that per system capability necessarily encompasses alternative mitigation actions that achieve the underlying objective of a CIP Requirement,⁷⁶ an express obligation for alternative mitigation does not appear in the CIP Standards or other NERC documents (e.g., the NERC Glossary or the NERC Rules of Procedure) other than NERC's petition and NOPR comments.

32. In light of these uncertainties surrounding the self-implementing exception process, we determine that greater oversight is needed than proposed by NERC.

Exclusive reliance on audits and other compliance tools will not necessarily ensure timely feedback on basic information such as how many exceptions are being invoked and for

⁷⁴ NERC Comments at 4-5.

⁷⁵ See NOPR, 192 FERC ¶ 61,228 at P 15. See also EEI Comments at 5 ("Some existing and emerging technologies cannot fully meet certain CIP requirements due to inherent design limitations.").

⁷⁶ NERC Comments at 4.

what CIP Requirements, and the alternative mitigation measures implemented. Further, documentation of the exception process is needed to eliminate potential confusion and better assure consistent usage among responsible entities relying on the per system capability exception and across the Regional Entities when conducting audits and other compliance activities.

33. Consequently, we direct NERC to develop a program for the per system capability exceptions to satisfy the fundamental needs for oversight, consistency, and alternative mitigation. We decline to adopt any specific proposal offered by commenters. Rather, we allow NERC the latitude to develop a program provided that it includes the following three elements: (1) a clear set of criteria that promote consistency and ensure that responsible entities understand the parameters for invoking the per system capability exception, documentation requirements,⁷⁷ and the obligation to implement alternative mitigation; (2) mandatory reporting requirements to the ERO Enterprise (i.e., the relevant Regional Entity, NERC, or both) for responsible entities that invoke the per system capability language; and (3) submission of an annual report to the Commission that includes anonymized, aggregated data that indicates how entities are utilizing the exception language. We discuss each of these elements below.

34. First, NERC must develop a clear set of criteria that promote consistency and ensure that responsible entities understand the parameters for invoking the per system

⁷⁷ The documentation requirements in this element may be more extensive than the mandatory reporting requirements to the ERO in the second element.

capability exception, documentation requirements, and the obligation to implement alternative mitigation. As mentioned earlier, while NERC discusses these elements in its petition and comments in this docket, there is no NERC document that provides responsible entities, Regional Entities, and the Commission a comprehensive understanding of the expectations of the per system capability process. We believe that clear guidance is vital to ensure (1) that responsible entities properly identify, document and mitigate per system capability exceptions and (2) consistency across Regional Entities when conducting audits and other compliance activities.

35. NERC has the discretion to choose an appropriate format to develop the required criteria, e.g., changes to the NERC Rules of Procedure, development of new or modified guidance documents, or modifications to the CIP Reliability Standards. We also direct NERC to ensure the per system capability exception program with the above criteria is available in time for the early adoption of the 11 proposed CIP Reliability Standards by responsible entities that choose to comply early.⁷⁸ This approach will ensure that the program is in place by the time responsible entities are self-implementing per system capability exceptions.

36. Second, the ERO Enterprise must develop mandatory reporting requirements through a request for data—through Align or another reporting mechanism—on basic information from entities using the per system capability exceptions, including the relevant CIP Reliability Standard and Requirement, an explanation of the need for the

⁷⁸ NERC Petition at 59-60.

exception, description of alternative mitigation, and any other fields of information that NERC determines are useful for monitoring exceptions. To be clear, while we direct the ERO to collect data on the exceptions, we do not require an approval process akin to the technical feasibility exception program. Moreover, as discussed earlier, legacy technical feasibility exceptions have been steady for a number of years and are well understood.⁷⁹ Therefore, NERC at its discretion may craft an appropriate less detailed data collection for legacy exceptions, while collecting more detailed information for newly invoked exceptions. This approach could provide the necessary insight into the volume and circumstances of new per system capability exceptions while reducing the burden with regard to legacy technical feasibility exceptions.

37. Third, NERC must submit an annual report to the Commission that provides adequate data and analysis on responsible entity usage of the per system capability exception for the Commission to fulfill its oversight role. Similar to reporting on technical feasibility exceptions directed in Order No. 706, NERC's annual report should provide an anonymized, aggregated, wide-area analysis.⁸⁰ The report must include at a minimum the following data:

⁷⁹ See NERC Comments at 4. See also NERC, *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 5 (filed Sept 26, 2025) (“The data . . . indicates that the number of registered entities that are engaging in the TFE program remains stable from prior reporting years.”).

⁸⁰ Order No. 706, 122 FERC ¶ 61,040 at PP 220-221.

- The total number of registered entities with active per system capability exceptions, the total number of reported per system capability exceptions that are still in effect (nationally and by region), and a comparison of these numbers over the previous reporting period;
- Categorization of active per system capability exceptions by applicable Requirements covered;
- Generalized discussion indicating the types of assets and/or systems for which new per system capability exceptions are claimed; and
- Discussion on types of mitigation measures employed.

The report should include any other information or analysis that NERC believes will assist the Commission in understanding the usage and efficacy of the per system capability exception program.

38. The annual report should be filed with the Commission 12 months after compliance with the 11 virtualization Reliability Standards becomes mandatory. Initial annual reports will provide the Commission and NERC visibility into the exception process and help the Commission conduct oversight to ensure that the new process is appropriately implemented. We are open to revisiting the frequency of the reports to the Commission after the initial three reporting cycles, if it is shown that the per system capability exception process is adequately executed and supporting Bulk-Power System security.

C. NERC Glossary Definitions

1. NOPR

39. In the NOPR, the Commission proposed to approve NERC's petition as supplemented, including the package of four proposed new definitions and 18 modified definitions in the NERC Glossary, as just, reasonable, not unduly discriminatory or preferential, and in the public interest. The Commission stated that the proposed new and modified definitions should provide a clear and consistent understanding of the terms across all Reliability Standards.⁸¹

2. Comments

40. Commenters generally support approval of NERC's package of 11 Reliability Standards without mentioning the four proposed new definitions and 18 modified definitions in the NERC Glossary.⁸² GE Vernova states that modernizing the definitions "will enable utilities to adopt virtualized designs."⁸³

3. Commission Determination

41. Pursuant to section 215(d)(2) of the FPA, we approve the proposed four new definitions and 18 modified definitions in the NERC Glossary. We find that the proposed

⁸¹ NOPR, 192 FERC ¶ 61,228 at P 17.

⁸² BPA Comments at 1; EEI Comments at 3; PGE Comments at 1 (supporting the entirety of EEI Comments).

⁸³ GE Vernova Comments at 1. The rest of GE Vernova's comments recommend that the final rule explicitly address issues associated with cloud deployment models, which are outside of the scope of this proceeding and thus not considered.

new and modified definitions will establish a consistent understanding of the meaning of those terms across Reliability Standards. Additionally, we find that the package of proposed new and revised definitions and proposed Reliability Standards will allow responsible entities the opportunity to adopt virtualization, improving the reliability of the Bulk-Power System by providing significant cyber security benefits and flexibility in responding to cyber threats.

III. Information Collection Statement

42. The Commission bases its paperwork burden estimates on the additional paperwork burden presented by the revisions to Reliability Standards that the Commission has approved. The approved revisions focus on security objectives rather than specific controls for system security management to accommodate virtualized environments. The Reliability Standards approved by this final rule are objective-based and allow registered entities to choose compliance approaches best tailored to their systems. The Reliability Standards approved by this final rule will 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.

43. The Reliability Standards approved by this final rule do not require responsible entities to submit any filings with either the Commission or NERC as the ERO.

Responsible entities, however, will be required to maintain documentation adequate to demonstrate compliance with the Reliability Standards approved by this final rule.

Commission and NERC staff conduct periodic audits of registered entities, and auditors

rely on the entity's documentation in determining compliance with Reliability Standards. While registered 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 Measures provided in the Reliability Standards approved by this final rule.

44. 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 in Reliability Standard CIP-002-7. However, as stated in the NERC petition, the revisions in Reliability Standard CIP-002-7 are minor, mostly aligning the standard with updates to the NERC Glossary.⁸⁴ Therefore, we do not envision an increased paperwork burden specifically pertaining to any modifications in 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 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:

⁸⁴ NERC Petition at 38.

Total Changes Approved in Docket RM24-8-000⁸⁵						
	Number of Respondents (1)	Annual Number of Responses per Respondent (2)	Total Number of Responses (1)*(2)=(3)	Average Burden & Cost Per Response ⁸⁶ (4)	Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)	Cost per Respondent (\$) (5)÷(1)
Conforming to modifications proposed under Reliability Standard CIP-002-7	1673	1	1673	The Commission does not anticipate any material information collection costs associated with CIP-002-7.	The Commission does not anticipate any material information collection costs associated	The Commission does not anticipate any material information collection costs associated

⁸⁵ The paperwork burden estimate includes costs associated with the initial development of a policy to address the requirements.

⁸⁶ 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) \div 3 = \85.26 .

The figure is rounded to \$85.00 for use in calculating wage figures in this final rule.

Total Changes Approved in Docket RM24-8-000⁸⁵						
	Number of Respondents (1)	Annual Number of Responses per Respondent (2)	Total Number of Responses (1)*(2)=(3)	Average Burden & Cost Per Response ⁸⁶ (4)	Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)	Cost per Respondent (\$) (5)÷(1)
					with CIP-002-7.	with CIP-002-7.
Update compliance related documentation of one 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, CIP-009-7.1, CIP-010-5, CIP-011-4.1, and CIP-013-3	400 (per standard)	1	400 (per standard)	57.7 hrs. (Burden per Response per Respondent); \$4,905 (Cost per Response per Respondent)	23,080 hrs. (Burden per Response across all Respondents); \$1,961,800 (Cost per Response across all Respondents)	\$4,905 (Cost per Response per Respondent)
Total burden			4,000	577 hrs.	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; 23,080 hours for each CIP Standard.

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

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

Action: Revision to FERC-725B information collection.

OMB Control No.: 1902-0248.

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

Frequency of Responses: On occasion.

Necessity of the Information: This final rule approves the requested modifications to Reliability Standards pertaining to critical infrastructure protection. As discussed above, the Commission approves proposed 11 virtualization Reliability Standards pursuant to section 215(d)(2) of the FPA because it allows responsible entities the opportunity to adopt virtualization, improving the reliability of the Bulk-Power System by providing significant cyber security benefits and flexibility in responding to cyber threats.

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

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

47. For submitting comments concerning the collection(s) of information and the associated burden estimate(s), please send your comments to the Commission, and to the Office of Management and Budget, Office of Information and Regulatory Affairs, Washington, DC 20503 [Attention: Desk Officer for the Federal Energy Regulatory Commission, phone: (202) 395-4638, fax: (202) 395-7285]. For security reasons, comments to the Office of Management and Budget should be submitted by e-mail to: oir_submission@omb.eop.gov. Comments submitted to the Office of Management and Budget should include Docket Number RM24-8-000 and OMB Control Number 1902-0248.

IV. Environmental Analysis

48. 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.⁸⁷ 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.⁸⁸ The action approved herein falls within this categorical exclusion in the Commission's regulations.

⁸⁷ *Reguls. Implementing the Nat'l Env't Pol'y Act*, Order No. 486, 52 FR 47897 (Dec. 17, 1987), FERC Stats. & Regs. Preambles 1986-1990 ¶ 30,783 (1987) (cross-referenced at 41 FERC ¶ 61,284).

⁸⁸ 18 CFR 380.4(a)(2)(ii).

V. Regulatory Flexibility Act

49. The Regulatory Flexibility Act of 1980 (RFA)⁸⁹ generally requires a description and analysis of final 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.⁹⁰ 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 hour sales).⁹¹

50. 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 NERC Compliance Registry, we have selected a combination of 288 Generator Owners (GO) and Generator Operators (GOP) as applicable 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).

⁸⁹ 5 U.S.C. 601-612.

⁹⁰ 13 CFR 121.101.

⁹¹ 13 CFR 121.201, Subsector 221 (Utilities).

51. 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, and the impact the regulation has on larger competitors.”⁹²

52. Moreover, this final rule approves Reliability Standards that permit voluntary actions by registered entities for the purpose of accommodating virtualized environments. The Reliability Standards approved in this final rule do not mandate or require action by any registered entity other than updating compliance documentation for processes related to the approved Reliability Standards. As a result, we certify that the Reliability Standards approved in this final rule will not have a significant economic impact on a substantial number of small entities. Accordingly, no regulatory flexibility analysis is required.

VI. Document Availability

53. 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>).

54. 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

⁹² 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>.

eLibrary, type the docket number excluding the last three digits of this document in the docket number field.

55. User assistance is available for eLibrary and the Commission's website during normal business hours from FERC Online Support at 202-502-6652 (toll free at 1-866-208-3676) or email at ferconlinesupport@ferc.gov, or the Public Reference Room at (202) 502-8371, TTY (202) 502-8659. E-mail the Public Reference Room at public.referenceroom@ferc.gov.

VII. Regulatory Planning and Review

56. Executive Orders 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. The Office of Information and Regulatory Affairs (OIRA) has determined this regulatory action is not a "significant regulatory action," under section 3(f) of Executive Order 12866, as amended.

Accordingly, OIRA has not reviewed this regulatory action for compliance with the analytical requirements of Executive Order 12866.

VIII. Effective Date and Congressional Notification

57. This final rule is effective **[INSERT DATE 60 DAYS FROM PUBLICATION IN FEDERAL REGISTER FOR NON-MAJOR RULES]**. The Commission has determined, with the concurrence of the Administrator of the Office of Information and

Regulatory Affairs of the Office of Management and Budget, that this rule is not a “major rule” as defined in section 351 of the Small Business Regulatory Enforcement Fairness Act of 1996.

By the Commission.

(S E A L)

Debbie-Anne A. Reese,
Secretary.