6717-01-P

**DEPARTMENT OF ENERGY**

**Federal Energy Regulatory Commission**

**18 CFR Part 40**

**[Docket No. RM25-8-000]**

**Critical Infrastructure Protection Reliability Standard CIP-003-11 – Cyber Security – Security Management Controls**

**AGENCY**: Federal Energy Regulatory Commission.

**ACTION**: Notice of proposed rulemaking.

**SUMMARY**: The Federal Energy Regulatory Commission (Commission) proposes to approve Critical Infrastructure Protection (CIP) Reliability Standard: CIP-003-11 (Cyber Security – Security Management Controls). The North American Electric Reliability Corporation, the Commission-certified electric reliability organization, submitted the proposed Reliability Standard modifications to mitigate risks posed by a coordinated cyberattack on low impact facilities; the aggregate impact of which could be much greater.

**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, NE, 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**:

Jacob Waxman (Technical Information)

Office of Electric Reliability

Federal Energy Regulatory Commission

888 First Street, NE

Washington, DC 20426

(202) 502-6879

Jacob.Waxman@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

**SUPPLEMENTARY INFORMATION:**

1. Pursuant to section 215(d)(2) of the Federal Power Act (FPA),[1] we propose to approve proposed Reliability Standard CIP-003-11 (Cyber Security – Security Management Controls), submitted by the North American Electric Reliability Corporation (NERC), as just, reasonable, not unduly discriminatory or preferential, and in the public interest. We also propose to approve the associated violation risk factors, violation severity levels, implementation plans, and effective dates for the proposed Reliability Standard, as well as to approve the retirement of currently effective Reliability Standard CIP-003-9.[2]

2. Proposed Reliability Standard CIP-003-11 specifies security management controls that establish responsibility and accountability to protect low impact bulk electric system (BES) Cyber Systems against compromise that could lead to misoperation or instability in the bulk electric system.[3] Reliability Standard CIP-003-11, amongst other obligations, requires entities with assets containing low impact BES Cyber Systems to document and maintain plans that include controls specified in Attachment 1 of the Standard. NERC states that the modifications in proposed Reliability Standard CIP-003-11 would mitigate the risks posed by a coordinated attack utilizing distributed low impact BES Cyber Systems by adding controls to authenticate remote users, protecting the authentication

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

[2] We are issuing a NOPR concurrently in Docket No. RM24-8-000. In that NOPR, we are proposing to approve proposed Reliability Standard CIP-003-10, 192 FERC ¶ 61,228. Here, we are proposing to approve proposed Reliability Standard CIP-003-11 and have it supersede Reliability Standard CIP-003-10.

[3] NERC Petition at 1.

information in transit, and detecting malicious communications to or between assets containing low impact BES Cyber Systems with external routable connectivity.[4]

3. We seek comments on all aspects of proposed Reliability Standard CIP-003-11 and our proposal to approve the Standard. As discussed later, we also seek comments on the continuing evolution of threats of compromise to low impact BES Cyber Systems. Related, we seek comment on whether it is worthwhile to direct NERC to perform a study or develop a whitepaper on evolving threats as they relate to the potential exploitation of low impact BES Cyber Systems.

## I. Background

### A. Section 215 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.[5] Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[6] Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[7] and subsequently certified NERC.[8]

---

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

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

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

[7] *Rules Concerning Certification of the Elec. Reliability Org.; & Procs. for the Establishment, Approval, & Enf't of Elec. Reliability Standards*, Order No. 672, 71 FR 8662 (Feb. 17, 2006), 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 71 FR 19814 (Apr. 18, 2006), 114 FERC ¶ 61,328 (2006); *see also* 18 CFR 39.4(b).

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

### B. Low Impact BES Cyber Systems

5. The CIP Reliability Standards apply a "tiered" approach with different obligations depending on whether a BES Cyber System[9] is classified as high, medium, or low impact.[10] The purpose of categorizing BES Cyber Systems is to apply cybersecurity requirements consistently, efficiently, and commensurate with the adverse impact that a loss, compromise, or misuse of those systems could have on the reliable operation of the Bulk-Power System.

6. Most individual BES Cyber Systems within the bulk electric system are categorized as low impact.[11] Individual low impact BES Cyber Systems have less of an impact on bulk electric system reliability than medium or high impact BES Cyber Systems and thus, have fewer CIP Reliability Standard requirements. Nevertheless, low impact BES Cyber Systems may still introduce reliability risks of a higher impact when distributed low impact BES Cyber Systems are subjected to a coordinated cyber-attack.

---

[9] BES Cyber Systems are defined as "one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks." A BES Cyber Asset is defined as "[a] Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed degraded or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System." NERC, *Glossary of Terms Used in NERC Reliability Standards* 49 (Feb. 26, 2025) (NERC Glossary), https://www.nerc.com/pa/Stand/Glossary of Terms/Glossary_of_Terms.pdf.

[10] Reliability Standard CIP-002-5.1a (BES Cyber System Categorization) delineates three categories of BES Cyber Systems: high, medium, and low, determined by a BES Cyber System's potential impact on Bulk-Power System reliability.

[11] *See, e.g.,* NERC, *Low Impact Criteria Review Report* 5 (Oct. 2022) (Low Impact Criteria Review Report), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC_LICRT_White_Paper_clean.pdf#search=low%20impact%20criteria%20review%20report.

## II. NERC Petition[12]

7. On December 20, 2024, NERC submitted proposed Reliability Standard CIP-003-11 for Commission approval. NERC explains that, in response to the SolarWinds Orion platform attack, and at the direction of the NERC Board of Trustees, NERC staff assembled a team of cybersecurity experts and compliance experts called the Low Impact Criteria Review Team (LICRT) that developed a report that discussed the potential threats and risks posed by a coordinated attack on low impact BES Cyber Systems.[13] NERC's proposed modifications made in Reliability Standard CIP-003-11 reflect many of the recommendations from the LICRT.[14]

8. NERC states that the proposed Reliability Standard would enhance reliability by mitigating the risk posed by a coordinated attack utilizing distributed low impact BES Cyber Systems.[15] NERC explains that, to address the threat of a coordinated attack on dispersed low impact BES Cyber Systems, the proposed Standard adds controls to: (1) authenticate remote users, (2) protect the authentication information in transit, and (3) detect malicious communications to or between assets containing low impact BES Cyber Systems with external routable connectivity.[16]

---

[12] The proposed Reliability Standard is not attached to this NOPR. The proposed Reliability Standard is available on the Commission's eLibrary document retrieval system in Docket No. RM25-8-000 and on the NERC website, www.nerc.com.

[13] NERC Petition at 8.

[14] *See id.* at 1-2, 9.

[15] *Id*. at 11.

[16] *Id*.

9. The above enhancements are reflected primarily in modifications to Requirement R1 and Attachment 1 of proposed Reliability Standard CIP-003-11. Specifically, NERC proposed to remove Requirement R1 Part 1.2.6 on vendor electronic remote access security controls.[17] NERC explains that this change reflects the proposed deletion of Attachment 1, Section 6 (vendor electronic remote access and security controls), which was combined into Attachment 1, Section 3 (electronic access controls).[18] NERC also states that the proposed changes remove the word "remote" from the phrase "electronic remote access" as the section would now include *all* electronic access.[19]

10. NERC explains that proposed Attachment 1, Section 3.1.2 would expand the scope of Reliability Standard CIP-003 to include all communications, rather than only vendor specific communications.[20] According to NERC, this revision would help entities mitigate the risk posed by malicious communications to or from BES Cyber Systems, while allowing entities the flexibility as to where the control is implemented based on their architecture.[21] Further, NERC notes that proposed Attachment 1, Section 3.1.3 would mitigate the risk of unauthenticated access to networks on which low impact BES Cyber Systems reside; specifically, it would require entities to implement controls to authenticate users prior to permitting access to networks containing low impact BES

---

[17] *Id*. at 12.

[18] *Id*. at 12-13.

[19] *Id*. at 15.

[20] *Id*. at 16.

[21] *Id*.

Cyber Systems or Shared Cyber Infrastructure that supports a low impact BES Cyber System.[22] In addition, NERC explains that proposed Attachment 1, Section 3.1.4 would require responsible entities to protect their user authentication information while in transit between a remote user's Cyber Asset and either the asset containing the low impact BES Cyber Systems or the entity's authentication system.[23]

11. NERC's proposed implementation plan states that the proposed Standard would become effective on the first day of the first calendar quarter that is 36 months after the effective date of the Commission's order approving the proposed Reliability Standard.[24] NERC explains that its proposed implementation plan reflects the time needed for entities to: (1) revise their cyber security policy, plan, and procedures; (2) hire and train new staff to implement the new cyber security controls; (3) reconfigure system, network, or security architectures; and (4) purchase, procure, and install new technologies.[25]

## III. Discussion

12. Pursuant to section 215(d)(2) of the FPA, we propose to approve proposed Reliability Standard CIP-003-11 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. We also propose to approve the associated violation risk factors, violation severity levels, implementation plans, and effective dates

---

[22] *Id*. (stating that each user would thus be authenticated before they gain access to the network containing low impact BES Cyber systems).

[23] *Id*. at 18 (noting that this protection would mitigate the risk of user authentication information being captured).

[24] *Id*. at 20.

[25] *Id*. at 21.

of Reliability Standard CIP-003-11, as well as to approve the retirement of currently effective Reliability Standard CIP-003-9.[26]

13. We believe that the proposed Reliability Standard represents an improvement over the currently mandatory and effective CIP Reliability Standards. The Low Impact Criteria Review Report identified several risks to low impact BES Cyber Systems that proposed CIP-003-11 addresses by introducing new security controls. The proposed Standard improves upon previous versions of CIP-003 by requiring responsible entities, for each asset containing low impact BES Cyber Systems, to detect malicious traffic, authenticate all users, and protect authentication data from unauthenticated access. We seek comment on all aspects of the proposed Reliability Standard and solicit comments regarding another matter discussed immediately below.

14. As discussed above, NERC developed the proposed modifications to Reliability Standard CIP-003-11 based on the recommendations of the Low Impact Criteria Review Report. Since 2022, however, there have been evolving threats that could potentially compromise low impact BES Cyber Systems and serve as a launch point to compromise other external BES Cyber Systems, including high and medium impact BES Cyber Systems.

15. In 2023 and 2024, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) reported that Volt Typhoon, an advanced persistent threat group linked to China,[27] maintained *unauthorized access* to the

---

[26] *See supra* note 2 (explaining that approval of Reliability Standard CIP-003-11 would also supersede CIP-003-10, pending before the Commission); *see also* NERC Petition at 22 (requesting retirement of "proposed Reliability Standard CIP-003-10, or the version of Reliability Standard CIP-003 then in effect").

[27] *See* DHS CISA, *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection* (June 2023),

operational technology network of a small public power utility.[28] In the continental United States, Volt Typhoon has exploited weak security controls, existing remote administration tools, and VPN connections.[29] These cyber-attackers leveraged the trust of less protected systems to move laterally and pivot, compromising externally connected, higher criticality targets.[30] Although Volt Typhoon is a more recent example, cyber attackers have used malware in the past to cause power outages.[31] For instance, according to CISA, the attack methodology seen in the CrashOverride malware attack could be adapted to impact U.S. critical infrastructure.[32] Under the proposed Standard, low impact BES Cyber Systems are only required to detect, not monitor, detect, and mitigate (together as a bundle of complimentary security controls) potential or actual

---

https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF; *see also* DHS CISA, *Nation State Threats*, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors#:~:text=APT%20actors%20are%20well%2Dresourced,network/system%20disruption%20or%20destruction (stating that advanced persistent threat groups engage in sophisticated malicious cyber activity aimed at prolonged network/system intrusion).

[28] *See* DRAGOS, *Hunting Active Threats in Littleton's Grid with the Dragos Platform and OT Watch* (Feb. 2025), https://www.dragos.com/wp-content/uploads/2025/03/Dragos_Littleton_Electric_Water_CaseStudy.pdf.

[29] *See id*.; *see also* DARKREADING, *Volt Typhoon Strikes Massachusetts Power Utility* (Mar. 12, 2025), https://www.darkreading.com/cyberattacks-data-breaches/volt-typhoon-strikes-massachusetts-power-utility.

[30] *See e.g.,* Joint CISA Advisory, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure* 13-14 (Feb. 7, 2024), https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf.

[31] *See e.g.,* DHS CISA, *Alert: TA17-163A CrashOverride Malware*, (July 20, 2021), https://www.cisa.gov/news-events/alerts/2017/06/12/crashoverride-malware.

[32] *See id.*

security events.[33] Thus, under the proposed Standard, an entity does not have to respond to or mitigate the risk of compromise to its low impact BES Cyber Systems. Further, in the proposed Standard, an entity is not required to authorize and restrict electronic access to any other Cyber Asset that is on the same network as the low impact BES Cyber System,[34] thereby putting the low impact BES Cyber System at a greater risk of compromise.[35] As such, we seek to understand opportunities to strengthen the controls of low impact BES Cyber Systems while also addressing the continuing evolution of cybersecurity threats such as Volt Typhoon.

16. In light of the above discussion, we seek comment on the continuing evolution of threat of compromise to low impact BES Cyber Systems posed by Volt Typhoon and similar cyberattacks that initially impact low impact BES Cyber Systems and then move laterally and pivot to higher impact BES Cyber Systems to effectuate a broader campaign. We seek comment from NERC, electric industry stakeholders, and other interested persons regarding the potential risk of the cyber threat discussed above, as well as electric industry stakeholders' activities to mitigate the described cyber threat.[36] We also seek comment on whether it is worthwhile to direct NERC to perform a study or develop a whitepaper, (essentially updating the Low Impact Criteria Review Report), on

---

[33] *See* NERC Petition at 1-4, 9, 11.

[34] *See id*., Ex. A-1 at 19-20.

[35] For high and medium impact BES Cyber Systems, the CIP Reliability Standards require that *all* electronic access to a network in which the BES Cyber System is connected be controlled (i.e., authorized and restricted). *See* Reliability Standard CIP-005-7, Requirement R1, Parts 1.2 and 1.3.

[36] Commenters should not include Critical Energy/Electric Infrastructure Information (CEII) in their submissions.

evolving threats as they relate to the potential exploitation of low impact BES Cyber Systems.

## IV. Information Collection Statement

17. The FERC-725B information collection requirements are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995. OMB's regulations require approval of certain information collection requirements imposed by agency rules. Upon approval of a collection of information, OMB will assign an OMB control number and expiration date. Respondents subject to the filing requirements will not be penalized for failing to respond to these collections of information unless the collections of information display a valid OMB control number. The Commission solicits comments on the need for this information, whether the information will have practical utility, the accuracy of the burden estimates, ways to enhance the quality, utility, and clarity of the information to be collected or retained, and any suggested methods for minimizing respondents' burden, including the use of automated information techniques.

18. The Commission bases its paperwork burden estimates on the additional paperwork burden presented by the proposed Reliability Standard CIP-003-11 as this is a modification to an existing Reliability Standard. Reliability Standards are objective-based and allow entities to choose compliance approaches best tailored to their systems. The NERC Compliance Registry, as of June 2025, identifies approximately 1,673 unique U.S. entities that are subject to mandatory compliance with CIP Reliability Standards, each of which will face an increased paperwork burden under proposed Reliability Standard CIP-003-11. Based on these assumptions, we estimate the following reporting burden:

| Total Changes Proposed by the NOPR in Docket No. RM25-8-000[37] | | | | | | |
|---|---|---|---|---|---|---|
| | **Number of Respondents (1)** | **Annual Number of Responses per Respondent (2)** | **Total Number of Responses (1)*(2)=(3)** | **Average Burden & Cost Per Response[38] (4)** | **Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)** | **Cost per Respondent ($) (5)÷(1)** |
| Create one or more documented process(es) (R2) | 1,673 | 1 | 1,673 | 1 hr.; $97 | 1,673 hrs.; $162,281 | $97 |
| R2, Attachment 1, Section 2, Physical Security Controls | 1,673 | 1 | 1,673 | 2 hrs.; $194 | 3346 hrs.; $324,562 | $194 |
| R2, Attachment 1, Section 3, Electronic Access Controls | 1,673 | 1 | 1,673 | 1 hr.; $97 | 1673 hrs.; $162,281 | $97 |

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

[38] This burden applies in Year 1 to Year 3.

The hourly cost for wages is based in part on the average of the occupational categories from the Bureau of Labor Statistics website (http://www.bls.gov/oes/current/naics2_22.htm) plus benefits:

Legal (Occupation Code: 23-0000): $162.66

Electrical Engineer (Occupation Code: 17-2071): $79.31

Office and Administrative Support (Occupation Code: 43-0000): $48.59

($162.66 + $79.31 + $48.59) ÷ 3 = $96.85

The figure is rounded to $97.00 for use in calculating wage figures in this NOPR.

| | | | | | | |
|---|---|---|---|---|---|---|
| R2, Attachment 1, Section 3.1 | 1,673 | 1 | 1,673 | 5 hrs.; $485 | 8,365 hrs.; $811,405 | $485 |
| R2, Attachment 1, Section 3.1.1 | 1,673 | 1 | 1,673 | 2 hrs.; $194 | 3346 hr.; $324,562 | $194 |
| R2, Attachment 1, Section 3.1.2 | 1,673 | 1 | 1,673 | 20 hrs.; $1,940 | 33,460 hrs.; $3,245,620 | $1,940 |
| R2, Attachment 1, Section 3.1.3 | 1,673 | 1 | 1,673 | 60 hrs.; $5,820 | 100,380 hrs.; $9,736,860 | $5,820 |
| R2, Attachment 1, Section 3.1.4 | 1,673 | 1 | 1,673 | 60 hrs.; $5,820 | 100,380 hrs.; $9,736,860 | $5,820 |
| R2, Attachment 1, Section 3.1.5 | 1,673 | 1 | 1,673 | 1 hr.; $97 | 1,673 hrs.; $162,281 | $97 |

| | | | | | | |
|---|---|---|---|---|---|---|
| R2, Attachment 1, Section 3.1.6 | 1,673 | 1 | 1,673 | 1 hr.; $97 | 1,673 hr.; $162,281 | $97 |
| R2, Attachment 1, Section 3.2 | 1,673 | 1 | 1,673 | 1 hr.; $97 | 1,673 hrs.; $162,281 | $97 |
| Total burden for FERC-725B(5) under CIP-003-11 | | | 1,673 | | 257,642 hrs.; $24,991,274 | $14,938 |

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

- Year 1-3 total: 1,673 responses; 257,642 hours
- The annual cost burden for each Year 1 to 3 is $8,330,425.

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 NOPR proposes to approve the requested modifications to the proposed Standard on critical infrastructure protection. As discussed

above, the Commission proposes to approve proposed CIP-003-11 pursuant to section 215(d)(2) of the FPA because it improves upon the currently-effective Standard.

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

20. 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) 502-6468].

21. 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 OMB should be submitted by e-mail to: oira_submission@omb.eop.gov. Comments submitted to OMB should include Docket Number RM25-8-000 and OMB Control Number 1902-0248.

## V. Environmental Analysis

22. 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.[39] The Commission has categorically excluded certain actions from this requirement as not having a significant effect on the human

[39] *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).

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

## VI. Regulatory Flexibility Act Certification

23. The Regulatory Flexibility Act of 1980 (RFA)[41] 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.[42] 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).[43]

24. Proposed Reliability Standard CIP-003-11 is expected to impose an additional burden on 1,673 U.S. entities[44] (reliability coordinators, generator operators, generator owners, interchange coordinators or authorities, transmission operators, balancing authorities, transmission owners, and certain distribution providers).

---

[40] 18 CFR 380.4(a)(2)(ii).

[41] 5 U.S.C. 601-612.

[42] 13 CFR 121.101.

[43] 13 CFR 121.201, Subsector 221 (Utilities).

[44] Public utilities may fall under one of several different categories, each with a size threshold based on the company's number of employees, including affiliates, the parent company, and subsidiaries. For the analysis in this NOPR, we are using a 500 employee threshold for each affected entity to conduct a comprehensive analysis.

Of the 1,673 affected entities discussed above, we estimate that 406 entities are small entities and, therefore, will be affected by the proposed modifications to CIP-003-11. We estimate that each of the 406 small entities to whom the proposed modifications of CIP-003-11 applies will incur one-time costs of approximately $19,000 per entity to implement this Standard, in addition to the ongoing paperwork burden reflected in the Information Collection Statement (a total of $14,938 per entity over Years 1-3), giving a total one-time cost of $33,938 per entity. We do not consider the estimated one-time costs for these 406 small entities to have a significant economic impact.

25. We view this as a minimal economic impact for each entity. Accordingly, we certify that proposed Reliability Standard CIP-003-11 will not have a significant economic impact on a substantial number of small entities. Thus, no regulatory flexibility analysis is required.

## VII. Comment Procedures

26. 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. RM25-8-000, 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.

27. 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.

28. 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.

## VIII. Document Availability

29. 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).

30. 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.

31. 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.

## IX. Regulatory Planning and Review

32. 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.

By the Commission.

Issued: September 18, 2025.

**Carlos D. Clay,**

*Deputy Secretary.*

[FR Doc. 2025-18396 Filed: 9/22/2025 8:45 am; Publication Date: 9/23/2025]