6717-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

18 CFR Part 40

[Docket No. RM25-8-000]

Order No. 918; Critical Infrastructure Protection Reliability Standard CIP-003-11 - Cyber Security – Security Management Controls

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final action.

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

DATES: This action is effective [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

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
Felicia West (Legal Information)
Office of General Counsel
Federal Energy Regulatory Commission
888 First Street, NE

Washington, DC 20426
(202) 502-8948
Felicia.West@ferc.gov

SUPPLEMENTARY INFORMATION:

1. Pursuant to section 215(d)(2) of the Federal Power Act (FPA),[1] the Federal Energy Regulatory Commission (Commission) approves proposed Reliability Standard CIP-003-11, submitted by the North American Electric Reliability Corporation (NERC). We also approve the associated violation risk factors, violation severity levels, implementation plan, and effective date for the proposed Reliability Standard. In addition, we approve the retirement of the currently effective version of the proposed Reliability Standard upon the effective date of Reliability Standard CIP-003-11.[2] We approve proposed Reliability Standard CIP-003-11 because it improves the reliability of the bulk electric system (BES) by strengthening the cyber security protections for low impact BES Cyber Systems to reduce the risk of compromise.

2. Proposed CIP Reliability Standard CIP-003-11 specifies security management controls that establish responsibility and accountability to protect low impact BES Cyber Systems against compromise that could lead to misoperation or instability in the bulk electric system.[3] The proposed modifications to the Reliability Standard mitigate the risks posed by a coordinated attack utilizing distributed low impact BES Cyber Systems by adding controls to authenticate remote users, protecting authentication information in

---

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

[2] Concurrently in Docket No. RM24-8-000, we are issuing a final rule, in which we are approving, *inter alia*, the proposed Reliability Standard CIP-003-10. *Virtualization Reliability Standards*, 194 FERC ¶ 61,209 (2026). Here, we are approving the proposed Reliability Standard CIP-003-11, which will supersede Reliability Standard CIP-003-10. NERC explains that the proposed Reliability Standard CIP-003-11 incorporates and builds upon virtualization-related revisions in the proposed Reliability Standard CIP-003-10.

[3] NERC Petition at 1.

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

I. Background

A. Section 215 of the FPA and Mandatory Reliability Standards

3. 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.[4] Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[5] Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[6] and subsequently certified NERC.[7]

B. NERC Petition

4. On December 20, 2024, NERC submitted proposed Reliability Standard CIP-003-11 (Cyber Security – Security Management Controls) for Commission approval.[8] NERC stated that the purpose of proposed CIP Reliability Standard CIP-003-11 is to "specify consistent and sustainable security management controls that establish responsibility and

---

[4] 16 U.S.C. 824o(c).

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

[6] *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).

[7] *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).

[8] The proposed Reliability Standard is not attached to this final rule. 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.

accountability to protect BES Cyber Systems ("BCS") against compromise that could lead to misoperation or instability in the [BES]."[9] NERC explained that proposed CIP-003-11 is intended to "mitigate the risks posed by a coordinated attack utilizing distributed low impact BES Cyber Systems" by adding three specific categories of controls: "controls to authenticate remote users; protecting the authentication information in transit; and detecting malicious communications to or between assets containing low impact BES Cyber Systems with external routable connectivity."[10] In addition to seeking Commission approval of proposed Reliability Standard CIP-003-11, NERC requested that the Commission approve: (i) the associated implementation plan; (ii) the associated violation risk factors and violation severity levels; (iii) and the retirement of the proposed Reliability Standard CIP-003-10 or the version of Reliability Standard CIP-003 then in effect.[11]

C. Notice of Proposed Rulemaking

5. On September 18, 2025, the Commission issued a Notice of Proposed Rulemaking (NOPR) proposing to approve Reliability Standard CIP-003-11.[12] The Commission noted that under the tiered structure of the CIP Reliability Standards, most BES Cyber Systems are categorized as low impact and therefore are subject to fewer cybersecurity

---

[9] NERC Petition at 1.

[10] *Id.* at 1-2. *See also id.* at 8-9 (citing NERC, *Low Impact Criteria Review Report*, at v and 15 (Oct. 2022) (Low Impact Criteria Review Report), https://www.nerc.com/globalassets/our-work/reports/white-papers/nerc_licrt_white_paper_clean.pdf.

[11] *Id.* at 2.

[12] *Critical Infrastructure Protection Reliability Standard CIP-003-11 – Cyber Sec. – Sec. Mgmt. Controls*, 192 FERC ¶ 61,227 (2025) (NOPR).

requirements than medium and high impact systems.[13] However, the Commission emphasized that "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."[14]

6. In the NOPR, the Commission sought comments on the continuing threats of compromise to low impact BES Cyber Systems and on whether it would be 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.[15] The Commission received comments from the following: NERC, the Trade Associations, Mr. Tammer Haddad, and Mr. Michael Ravnitzky.[16]

II. Discussion

A. Proposed Reliability Standard CIP-003-11

1. Comments

7. NERC and the Trade Associations support the Commission's proposal to approve Reliability Standard CIP-003-11 without modification. NERC states that proposed Reliability Standard CIP-003-11 "would enhance reliability by mitigating the risk posed by a coordinated attack using distributed low impact BES Cyber Systems."[17] NERC

---

[13] *Id.* PP 5-6.

[14] *Id.* P 6.

[15] *Id.* P 16.

[16] The Trade Associations include: American Public Power Association, Edison Electric Institute, Electric Power Supply Association, Large Public Power Council, National Rural Electric Cooperative Association, and Transmission Access Policy Study Group.

[17] NERC Comments at 2. *See also* Trade Associations Comments at 1.

reiterates that by adding controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications to, from, or between assets containing low impact BES Cyber Systems with external routable connectivity, the BES Cyber Systems are more protected from the threat of a coordinated attack on dispersed low impact systems. NERC "strongly encourages the Commission to move forward . . . expeditiously" so that the reliability benefits of the proposed Standard "may be realized as soon as possible."[18]

8. The Trade Associations state that the proposed modifications "appropriately implements" the Low Impact Criteria Review Report's recommendations, including requirements to permit only necessary access, authenticate users, protect credentials in transit, detect malicious communications, and control vendor access.[19] In their view, proposed Reliability Standard CIP-003-11 "will improve the baseline cybersecurity requirements to mitigate against threats of a coordinated attack" for low impact BES Cyber Systems and complements the protections already included in Reliability Standard CIP-005 and related Reliability Standards.[20]

9. Conversely, Mr. Haddad and Mr. Ravnitzky argue that the proposed Reliability Standard CIP-003-11 is incomplete and should not be approved without modification.[21] Mr. Haddad contends that the proposed Standard adopts a "detection-only approach" for low impact BES Cyber Systems that "creates unacceptable vulnerabilities that

---

[18] NERC Comments at 2-3.

[19] Trade Associations Comments at 5-6 (citing the Low Impact Criteria Review Report).

[20] *Id.* at 12.

[21] Mr. Haddad Comments at 1; Mr. Ravnitzky Comments at 5.

sophisticated threat actors are actively exploiting."[22] Mr. Haddad cites the Volt Typhoon and Colonial Pipeline incidents as evidence that detection without response enables adversaries to persist and pivot. He recommends remanding the proposed Standard to NERC with directions to add response requirements, establish collaborative defense mechanisms such as Regional Security Operations Centers, provide support for small utilities, and accelerate implementation.[23]

10. Mr. Ravnitzky similarly argues that approving CIP-003-11 without additional requirements "risks leaving exploitable gaps in the Bulk-Power System's defenses,"[24] particularly because "adversaries exploit weak, distributed targets to reach critical systems."[25] Mr. Ravnitzky further claims that "[t]he NOPR does not contain an explicit requirement addressing lateral-movement risk."[26] He recommends conditioning approval on adding mandatory response timelines, clarifying definitions, mandating network segmentation or compensating controls, requiring cryptographic baselines, and enhancing vendor access, telemetry, and validation obligations.[27]

---

[22] Mr. Haddad Comments at 1-2.

[23] *Id.* at 1-2, 4.

[24] Mr. Ravnitzky Comments at 5.

[25] *Id.* at 1.

[26] *Id.* at 2. "Lateral movement" is the set of techniques adversaries use *after gaining an initial foothold* in a network to move from one system, account, or network segment to another, with the goal of expanding access, escalating privileges, discovering critical assets, and positioning themselves for further actions (such as data theft, disruption, or impact). *See* MITRE ATT&CK, *Lateral Movement* (last updated Aug. 11, 2025), https://attack.mitre.org/tactics/TA0008/.

[27] Mr. Ravnitzky Comments at 1-3.

2. Commission Determination

11. We adopt the NOPR proposal and approve Reliability Standard CIP-003-11 as proposed by NERC. Based on the record in this proceeding, we find that Reliability Standard CIP-003-11 is just, reasonable, not unduly discriminatory or preferential, and in the public interest.[28] We also approve the associated violation risk factors, violation severity levels, implementation plan, and effective date for the proposed Reliability Standard. In addition, we approve the retirement of the currently effective version of the proposed Reliability Standard upon the effective date of Reliability Standard CIP-003-11.

12. We agree with NERC that Reliability Standard CIP-003-11 strengthens baseline cybersecurity protections for low impact BES Cyber Systems by addressing the risk of coordinated cyberattacks that exploit distributed, externally routable assets. We find that the new requirements to authenticate remote users, protect authentication information in transit, and detect malicious communications directly target the threat vectors identified in the Low Impact Criteria Review Report and represent a measured, risk-based enhancement to existing controls applicable to low impact BES Cyber Systems.[29] The expansion of detection requirements to include all traffic into or out of a low impact BES Cyber System, as opposed to just detecting malicious traffic in vendor-based electronic access, should mitigate the risk of malicious communications to or from a low impact BES Cyber System from going undetected.[30] Similarly, we agree with NERC that the new requirements to authenticate users and protect their authentication information

---

[28] *See* NOPR, 192 FERC ¶ 61,127 at P 12.

[29] *Id.* P 8; Low Impact Criteria Review Report at 15.

[30] NERC Petition at 16.

should mitigate the risk of unauthorized users gaining access to low impact BES Cyber Systems or compromising legitimate credentials to gain access.[31] Together, these controls should improve the cybersecurity posture of the BES by protecting against potential coordinated attacks on multiple low impact BES Cyber Systems or using a compromised low impact BES Cyber System to move laterally and pivot to a medium or high impact BES Cyber System.

13. We acknowledge concerns raised by individual commenters that Reliability Standard CIP-003-11 does not impose explicit response or remediation requirements,[32] except in the event of a system disruption.[33] However, we decline to condition the approval of Reliability Standard CIP-003-11 on the addition of response-specific requirements. We find that NERC reasonably determined, through the Reliability Standards development process, that Reliability Standard CIP-003-11 should focus on baseline access controls, and authentication and detection enhancements for low impact BES Cyber Systems, while continuing to evaluate response-related issues through ongoing initiatives.[34] In particular, we note that NERC's CIP Roadmap, discussed further below, recommends developing guidance for improved cybersecurity incident response plans and associated playbooks,[35] and we encourage NERC to address both

---

[31] *Id.* at 16-17.

[32] *See* Mr. Haddad Comments at 1-4; Mr. Ravnitzky Comments at 2-4.

[33] Proposed Reliability Standard CIP-003-11, Requirement R2 & Attach. 1, Sec. 4.

[34] *See* NERC Comments 4-8; *see also* NERC Petition at 6-7. *See infra* Section II.B (discussing NERC's proposed initiatives in its *Critical Infrastructure Protection Roadmap* (Jan. 2026) (CIP Roadmap), https://www.nerc.com/globalassets/our-work/reports/special-reports/nerc_cip_roadmap_01122026.pdf.

[35] CIP Roadmap at 9.

substantive response efforts and recommended timeline(s) for response as part of that effort. We also note that Reliability Standard CIP-003-11, Requirement R2 and Section 4 of Attachment 1 require entities to have Cyber Security Incident Response plans for low impact BES Cyber Systems, including identification, classification, and response to Cyber Security Incidents.[36]

B. Proposal for NERC Study

1. NOPR Proposal

14. In the NOPR, the Commission explained that NERC developed the proposed modifications to Reliability Standard CIP-003-11 based on the recommendations of the Low Impact Criteria Review Report. Noting cybersecurity threats that have emerged since the 2022 issuance of the Report, the Commission asked for comment on the merit of directing 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.[37]

2. Comments on Evolving Threats and an Additional Study

15. All commenters generally agree that coordinated attacks leveraging remote access to multiple low impact BES Cyber Systems present systemic reliability risks,[38] but differ in opinion as to whether the Commission should direct NERC to perform further study. NERC and the Trade Associations oppose a directive to require NERC to conduct a study—explaining that NERC already has multiple initiatives underway, including the Level 2 Alert on Cross-Border Remote Access and the CIP Roadmap, which is evaluating

---

[36] Proposed Reliability Standard CIP-003-11, Requirement R2 & Attach. 1, Sec. 4.

[37] NOPR, 192 FERC ¶ 61,127 at P 16.

[38] Mr. Haddad Comments at 2; NERC Comments at 3-4; Mr. Ravnitzky Comments at 2; Trade Associations Comments at 5-6.

emerging cybersecurity and physical risk across the industry.[39] NERC asserts that requiring a study would duplicate existing efforts and interfere with NERC's multi-year planning process.[40]

16. NERC emphasizes that it has already conducted a comprehensive assessment of evolving cyber risks through the issuance of the Level 2 Alert on Cross-Border Remote Access and the development of the CIP Roadmap approved as part of the NERC's 2025 Work Plan Priorities.[41] NERC further states that the CIP Roadmap will "evaluate standards against emerging cybersecurity and physical risks (e.g., network intrusion, new registrants, emerging cyber threats, cloud usage, artificial intelligence, or other new technologies)."[42] NERC explains that the results of the Level 2 Alert and CIP Roadmap will enable NERC and industry to prioritize risks and determine whether additional studies, guidance documents, or standards development projects are warranted.[43]

17. Similarly, Trade Associations claim that directing NERC to conduct an additional study would be inefficient and counterproductive given the ongoing industry efforts coordinated through NERC and its technical committees.[44] They note that industry participants are already engaged in multiple parallel initiatives addressing emerging cyber

---

[39] NERC Comments at 1-2, 8; Trade Associations Comments at 1-2, 10-12 (citing NERC, *2025 Work Plan Priorities* (Dec. 10, 2024), https://www.nerc.com/globalassets/who-we-are/2025-work-plan-priorities-approved-december-10-2024.pdf); *see also* CIP Roadmap.

[40] NERC Comments at 8.

[41] *Id.* at 4-5.

[42] *Id.* at 6-7.

[43] *Id.* at 8; Trade Associations Comments at 11-12.

[44] Trade Associations Comments at 11-12.

risks, including work on cloud security, artificial intelligence, internal network security monitoring, supply chain management and vendor incident response.[45]

18. However, Mr. Haddad and Mr. Ravnitzky raise issues concerning the adequacy of cybersecurity protections for low impact BES Cyber Systems, including the potential for pivoting from low-impact systems into medium and high impact systems or from non-BES Cyber Assets into low-impact systems.[46] Mr. Ravnitzky recommends that NERC be directed to publish an "adversary-centric whitepaper mapping plausible attack chains from low-impact compromises to system effects."[47] He recommends that the study include measurable performance indicators for detection and response and be coordinated with federal partners such as the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy (DOE).[48] He contends that anonymized key performance indicator reporting could be used so that industry and regulators can measure systemic programs and provide guidance for future rulemakings.[49]

19. Mr. Haddad expresses concern that threat assessments can become obsolete due to the rapid evolution of cyber environments and threats.[50] Mr. Haddad argues that "periodic re-evaluation of threat models must become standard practice, especially for sectors like energy where adversaries have demonstrated persistence and patience."[51]

---

[45] *Id.* at 11-13.

[46] Mr. Haddad Comments at 2, Mr. Ravnitzky Comments at 2.

[47] Mr. Ravnitzky Comments at 4.

[48] *Id.*

[49] *Id.*

[50] Mr. Haddad Comments, attach. at 6 (Literary Review).

[51] *Id.*

Beyond an additional study, Mr. Haddad recommends the Commission establish a federal task force for "small utility cybersecurity" including the Commission, DOE, CISA, and NERC, to develop and support the implementation of shared security services and capabilities for small utilities.[52]

3. Commission Determination

20. We decline to direct NERC to conduct an additional standalone study, or whitepaper, on evolving threats related to the potential exploitation of low impact BES Cyber Systems.

21. We are persuaded by NERC's explanation that it already has substantial and comprehensive efforts underway that are evaluating the risks to low impact BES Cyber Systems.[53] NERC explains that it will consider the "collective findings from the Level 2 Alert and the CIP Roadmap to determine the most serious cyber security and physical risks to the BPS" and that "future actions will likely include studies, if it is determined more information is needed."[54] NERC explains that the CIP Roadmap will inform NERC's CIP Reliability Standards priorities over the next few years.[55]

22. In fact, since the issuance of the NOPR and submission of comments, NERC publicly issued its CIP Roadmap.[56] We note that the CIP Roadmap identifies several focus areas that directly affect low impact BES Cyber Systems, including risks associated

---

[52] Mr. Haddad Comments at 5.

[53] NERC Comments at 7-8.

[54] *Id.* at 8.

[55] *Id.* at 6-7.

[56] *See supra* note 35.

with remote and third-party access, shared and cloud-managed infrastructure, lateral movement pathways, and the maturity of detection capabilities.[57] The CIP Roadmap emphasizes that low impact BES Cyber Systems may present increased system risk when leveraged as part of coordinated attacks and recommends that these risks be addressed through the prioritized, risk-based evolution of CIP Reliability Standards and supporting guidance, rather than isolated or duplicative studies.[58] While the CIP Roadmap does not establish fixed timelines for each recommendation, NERC asserts that it actively prioritizes these efforts based on risk significance, operational feasibility, and stakeholder input.[59]

23. Based on these considerations, we conclude that directing NERC to perform an additional study at this time is unnecessary. NERC's ongoing work under the CIP Roadmap, including the recommendations related to Reliability Standards development, provides an appropriate and efficient mechanism to address evolving threats to low impact BES Cyber Systems and related concerns.

24. We further encourage NERC to look at how it can achieve efficiencies in effort and time in the implementation of the recommendations outlined in the CIP Roadmap report. The recommendations, if implemented in a timely and efficient manner, present the opportunity to significantly advance the security of low impact BES Cyber Systems. We will continue to monitor NERC's progress and expect NERC to keep us informed of material findings from this work that may warrant future consideration.

---

[57] CIP Roadmap at 3, 6, 8.

[58] *Id.* at 5 (citing the Low Impact Criteria Review Report).

[59] *Id.* at 2-3; *see also* NERC Comments at 8.

25. Finally, we believe that our approval of Reliability Standard CIP-003-11 and NERC's ongoing initiatives will address some of these concerns raised by commenters, such as the risk of lateral movement.[60] In response to Mr. Haddad, we also decline to recommend a federal task force for "small utility cybersecurity," as it is out of scope for this rulemaking.

III. Information Collection Statement

26. The Commission bases its paperwork burden estimates on the additional paperwork burden presented by the revisions to Reliability Standard that the Commission has approved. The approved revisions focus on mitigation risks posed by a coordinated attack on low-impact facilities. The Reliability Standard approved by this final rule is objective-based and provides requirements to address ongoing threats to the low impact BES Cyber Systems.

The Reliability Standard approved by this final rule does 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 Standard 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 Standard includes compliance measures, which provide examples of the type of documentation an entity may want to develop and maintain to demonstrate compliance.

---

[60] *See supra* Section II.A.2 (explaining how Reliability Standard CIP-003-11 will strengthen protections for low impact BES Cyber Systems). *See supra* note 26; *see also* CIP Roadmap at 5, 8 (noting how multi-factor authentication can help mitigate the risk of lateral movement).

The reporting burden below is based on the compliance measurements provided in the Reliability Standard approved by this final rule. 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. Entities are allowed to choose their compliance approach to most efficiently meet the requirements of the Reliability Standards. All 1,673 entities would need to conform to modifications in Reliability Standard CIP-003-11. Therefore, these entities will have an increased paperwork burden. Based on these assumptions, the estimated reporting burden is as follows:

Total Changes Proposed by the NOPR in Docket No. RM25-8-000[61]						
	Number of Respondents (1)	**Annual Number of Responses per Respondent (2)**	**Total Number of Responses (1)*(2)=(3)**	**Average Burden & Cost Per Response**[62] **(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	1hr.; $97	1673 hrs.; $162,281	$97
R2, Attachment 1, Section 3.1	1,673	1	1,673	5 hrs.; $485	8,365 hrs.; $811,405	$485

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

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

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

27. 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 One to Three is $8,330,425.

28. Title: Mandatory Reliability Standards for Critical Infrastructure Protection (CIP).

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 Reliability Standard CIP-003-11. As discussed above, the Commission approves Reliability Standard CIP-003-11 pursuant to section 215(d)(2) of the Federal Power Act because it mitigates risks posed by a coordinated cyberattack on low-impact facilities, the aggregate impact of which could be much greater.

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 Federal Power Act.

29. 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].

30. 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: oira_submission@omb.eop.gov. Comments submitted to the Office of Management and Budget should include Docket No. RM25-8 and OMB Control Number 1902-0248.

IV. Environmental Analysis

31. 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.[63] 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.[64] The action proposed herein falls within this categorical exclusion in the Commission's regulations.

V. Regulatory Flexibility Act

32. The Regulatory Flexibility Act of 1980 (RFA)[65] 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.[66] 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).[67]

---

[63] *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).

[64] 18 CFR 380.4(a)(2)(ii).

[65] 5 U.S.C. 601-612.

[66] 13 CFR 121.101.

[67] *Id.* 121.201, Subsector 221 (Utilities).

33. The SBA sets the threshold for what constitutes a small business. Under SBA's size standards, balancing authorities, generator operators, generator owners, reliability coordinators, transmission operators, and 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 entities and its associates). 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."[68]

34. The Reliability Standard CIP-003-11 is expected to impose an additional burden on 1,673 U.S. entities[69] (reliability coordinators, generator operators, generator owners, transmission operators, balancing authorities, transmission owners, and certain distribution providers).

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

---

[68] 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.

[69] 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.

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.

35. The Reliability Standard approved in this final rule requires minimal action by registered entities subject to compliance. As a result, we certify that the Reliability Standard approved in this final rule will not have a significant economic impact on small entities.

VI. Document Availability

36. 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).

37. 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.

38. 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

39. 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

40. This final rule is effective [INSERT DATE 60 DAYS AFTER DATE OF 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 action is not a "major rule" as defined in section 351 of the Small Business Regulatory Enforcement Fairness Act of 1996.

By the Commission.

Issued: March 19, 2026.

Carlos D. Clay,
Deputy Secretary.

[FR Doc. 2026-05711 Filed: 3/23/2026 8:45 am; Publication Date: 3/24/2026]