170 FERC ¶ 61,031
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM18-20-000; ORDER NO. 866]

Critical Infrastructure Protection Reliability Standard CIP-012-1 – Cyber Security – Communications between Control Centers

(Issued January 23, 2020)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule.

SUMMARY: The Federal Energy Regulatory Commission (Commission) approves Reliability Standard CIP-012-1 (Cyber Security – Communications between Control Centers). The North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization, submitted Reliability Standard CIP-012-1 for Commission approval in response to a Commission directive. In addition, the Commission directs NERC to develop modifications to the CIP Reliability Standards to require protections regarding the availability of communication links and data communicated between bulk electric system Control Centers.

DATES: This rule will become effective **[INSERT DATE 60 days after publication in the FEDERAL REGISTER].**

FOR FURTHER INFORMATION CONTACT:

Vincent Le (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6204
vincent.le@ferc.gov

Kevin Ryan (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6840
kevin.ryan@ferc.gov

SUPPLEMENTARY INFORMATION:

170 FERC ¶ 61,031
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Neil Chatterjee, Chairman;
Richard Glick and Bernard L. McNamee.

Critical Infrastructure Protection Reliability Standard CIP-012-1 – Cyber Security – Communications between Control Centers

Docket No. RM18-20-000

ORDER NO. 866

FINAL RULE

(Issued January 23, 2020)

1. Pursuant to section 215(d)(2) of the Federal Power Act (FPA),[1] the Commission approves Reliability Standard CIP-012-1 (Cyber Security – Communications between Control Centers). The North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), submitted Reliability Standard CIP-012-1 for Commission approval in response to a Commission directive in Order No. 822.[2] In Order No. 822, the Commission directed NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the Reliability Standards to require responsible entities to implement controls to protect, at a minimum,

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

[2] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, at P 53, *order denying reh'g*, Order No. 822-A, 156 FERC ¶ 61,052 (2016).

communications links and sensitive bulk electric system data communicated between bulk electric system Control Centers "in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)."[3]

2. Consistent with the directive in Order No. 822, Reliability Standard CIP-012-1 improves upon the currently-effective Critical Infrastructure Protection (CIP) Reliability Standards to mitigate cyber security risks associated with communications between bulk electric system Control Centers. Specifically, Reliability Standard CIP-012-1 supports situational awareness and reliable bulk electric system operations by requiring responsible entities to protect the confidentiality and integrity of Real-time Assessment[4] and Real-time monitoring data transmitted between bulk electric system Control Centers. Accordingly, the Commission approves Reliability Standard CIP-012-1 because it is largely responsive to the Commission's directive in Order No. 822 and improves the cyber security posture of responsible entities. We also approve the associated violation risk factors and violation severity levels, implementation plan, and effective date.

[3] 16 U.S.C. 824o(d)(5); Order No. 822, 154 FERC ¶ 61,037 at P 53.

[4] The NERC Glossary defines Real-time Assessment as, "An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to: load, generation output levels, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase angle and equipment limitations. (Real-time Assessment may be provided through internal systems or through third-party services.)" NERC Glossary of Terms Used in NERC Reliability Standards (July 3, 2018).

3. In addition, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to the CIP Reliability Standards to require protections regarding the *availability* of communication links and data communicated between bulk electric system Control Centers. As discussed in the Notice of Proposed Rulemaking (NOPR), Reliability Standard CIP-012-1 does not require protections regarding the availability of communication links and data communicated between bulk electric system Control Centers, as directed in Order No. 822.[5] In the NOPR, the Commission indicated that it did not agree with NERC's assertion that currently-effective Reliability Standards address availability, and we are not persuaded by NOPR comments raising the same argument. Instead, pursuant to section 215(d)(5) of the FPA, we determine that the absence of a requirement that specifically pertains to the availability of communication links and data communicated between bulk electric system Control Centers represents a reliability gap in the CIP Reliability Standards that should be addressed by NERC.

4. The Commission, in the NOPR, also proposed to direct NERC to identify clearly the types of data that must be protected under Reliability Standard CIP-012-1. The NOPR expressed concern that Reliability Standard CIP-012-1 does not adequately identify the types of data covered by its requirements, due to, among other things, the fact that the term "Real-time monitoring" is not defined in the Reliability Standard or the NERC Glossary. After considering the NOPR comments, however, we determine not to

[5] *See Critical Infrastructure Protection Reliability Standard CIP-012-1 – Cyber Security – Communication between Control Centers*, Notice of Proposed Rulemaking, 167 FERC ¶ 61,055, at P 54 (2019) (NOPR).

direct the proposed modification based on the explanation of the types of data that must be protected set forth in the NOPR comments.

I. Background

A. Section 215 and Mandatory Reliability Standards

5. Section 215 of the FPA requires a Commission-certified ERO to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval. 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]

B. Order No. 822

6. In Order No. 822, the Commission approved seven modified CIP Reliability Standards and directed NERC to develop additional modifications to the CIP Reliability Standards.[9] Specifically, the Commission directed that NERC, among other things, develop modifications to the CIP Reliability Standards to require that responsible entities

[6] 16 U.S.C. 824o(e).

[7] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006).

[8] *North American Electric 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).

[9] Order No. 822, 154 FERC ¶ 61,037 at PP 1, 3.

implement controls to protect, at a minimum, communications links and sensitive bulk electric system data communicated between bulk electric system Control Centers "in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)."[10] The Commission observed that NERC, as well as other commenters in that proceeding, "recognize that inter-Control Center communications play a critical role in maintaining bulk electric system reliability by . . . helping to maintain situational awareness and support reliable operations through timely and accurate communication between Control Centers."[11]

7. The Commission explained that Control Centers associated with responsible entities, including reliability coordinators, balancing authorities, and transmission operators, must be capable of receiving and storing a variety of bulk electric system data from their interconnected entities in order to adequately perform their reliability functions. The Commission, therefore, determined that "additional measures to protect both the integrity and availability of sensitive bulk electric system data are warranted."[12] The Commission cautioned, however, that "not all communication network components and data pose the same risk to bulk electric system reliability and may not require the

[10] *Id.* P 53.

[11] *Id.* P 54.

[12] *Id*.

same level of protection."[13] Therefore, the Commission determined that NERC should develop controls that reflect the risk being addressed in a reasonable manner.

C. NERC Petition and Reliability Standard CIP-012-1

8. On September 18, 2018, NERC submitted for Commission approval proposed Reliability Standard CIP-012-1 and the associated violation risk factors and violation severity levels, implementation plan, and effective date.[14] NERC states that the purpose of Reliability Standard CIP-012-1 is to help maintain situational awareness and reliable bulk electric system operations by protecting the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.

9. NERC states that Reliability Standard CIP-012-1 "requires Responsible Entities to develop and implement a plan to address the risks posed by unauthorized disclosure (confidentiality) and unauthorized modification (integrity) of Real-time Assessment and Real-time monitoring data while being transmitted between applicable Control Centers."[15] According to NERC, the required plan must include the following: (1) identification of security protections; (2) identification of where the protections are applied; and (3) identification of the responsibilities of each entity in case a Control Center is owned or operated by different responsible entities.[16]

---

[13] *Id.* P 56.

[14] Reliability Standard CIP-012-1 is not attached to this Final Rule. The Reliability Standard is available on the Commission's eLibrary document retrieval system in Docket No. RM18-20-000 and on the NERC website, www.nerc.com.

[15] NERC Petition at 10.

[16] *Id.* at 3.

10. As noted above, the types of data within the scope of Reliability Standard CIP-012-1 consist of Real-time Assessment and Real-time monitoring data exchanged between Control Centers. NERC states that it is critical that this information is accurate since responsible entities operate and monitor the bulk electric system based on this Real-time information. NERC explains that Reliability Standard CIP-012-1 "excludes other data typically transferred between Control Centers, such as Operational Planning Analysis data, that is not used by the Reliability Coordinator, Balancing Authority, and Transmission Operator in Real-time."[17]

11. NERC also indicates that data at rest and oral communications fall outside the scope of Reliability Standard CIP-012-1. Regarding data at rest, NERC states that the standard drafting team determined that since data at rest resides within BES Cyber Systems,[18] it is already protected by the controls mandated by Reliability Standards CIP-003-6 through CIP-011-2. According to NERC, oral communications are out of scope of Reliability Standard CIP-012-1 "because operators have the ability to terminate the call and initiate a new one via trusted means if they suspect a problem with, or compromise of, the communication channel."[19] NERC notes that Reliability Standard COM-001-3 requires reliability coordinators, balancing authorities, and transmission

[17] *Id.* at 12.

[18] BES Cyber System is defined as "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." NERC Glossary. The acronym BES refers to the bulk electric system.

[19] NERC Petition at 14.

operators to have alternative interpersonal communication capability, which could be used if there is a suspected compromise of oral communication on one channel.

D. Notice of Proposed Rulemaking

12. On April 18, 2019, the Commission issued a NOPR proposing to approve Reliability Standard CIP-012-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest.[20] The NOPR stated that Reliability Standard CIP-012-1 is largely responsive to the Commission's directive in Order No. 822 and improves the cyber security posture of the bulk electric system by requiring responsible entities to protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between bulk electric system Control Centers, which supports situational awareness and reliable bulk electric system operations.

13. While proposing to approve Reliability Standard CIP-012-1, the Commission also proposed to direct NERC to develop modifications to the CIP Reliability Standards to address potential reliability gaps. First, the NOPR stated that Reliability Standard CIP-012-1 does not require protections regarding the availability of communication links and data communicated between bulk electric system Control Centers as directed in Order No. 822. The NOPR explained that the Commission was not persuaded by NERC's explanation that certain currently-effective Reliability Standards address the issue of availability. Second, the NOPR raised a concern that Reliability Standard CIP-012-1 does not adequately identify the types of data covered by its requirements,

[20] NOPR, 167 FERC ¶ 61,055 at P 1.

due to, among other things, the fact that Real-time monitoring is not defined in the proposed Reliability Standard or the NERC Glossary.[21]

14. In response to the NOPR, eight entities submitted comments. A list of commenters appears in Appendix A. The discussion below addresses the proposals in the NOPR as well as the NOPR comments.

II. Discussion

15. Pursuant to section 215(d)(2) of the FPA, the Commission approves Reliability Standard CIP-012-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. Reliability Standard CIP-012-1 largely addresses the Commission's directive in Order No. 822 because it will enhance existing protections for bulk electric system reliability by augmenting the currently-effective CIP Reliability Standards to mitigate cyber security risks associated with communications between bulk electric system Control Centers. Reliability Standard CIP-012-1 achieves this by requiring responsible entities to protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between bulk electric system Control Centers, thereby supporting situational awareness and reliable bulk electric system operations.

16. While the Commission approves Reliability Standard CIP-012-1, we also determine that the reliability risks identified in Order No. 822 will not be fully addressed with the implementation of the Reliability Standard. As discussed below, a significant cyber security risk associated with the protection of communications links and sensitive bulk

[21] *Id.* P 16.

electric system data communicated between bulk electric system Control Centers remains because Reliability Standard CIP-012-1 does not address the availability of communication links and data communicated between bulk electric system Control Centers. To address this gap, the Commission directs NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP Reliability Standards to require protections regarding the availability of communication links and data communicated between bulk electric system Control Centers.

17. Below, we discuss the following issues: (A) availability of bulk electric system communication links and data; and (B) scope of bulk electric system data that must be protected.

A. Availability of Bulk Electric System Communication Links and Data

1. NOPR

18. The NOPR stated that Reliability Standard CIP-012-1 does not address the availability component of the Commission's directive in Order No. 822. The NOPR identified this as a gap because ensuring timely and reliable access to and use of data is essential to the reliable operation of the bulk electric system. The NOPR indicated that the existing Reliability Standards cited in NERC's petition do not require responsible entities to protect the availability of sensitive bulk electric system data in a manner consistent with Order No. 822.[22] In particular, the NOPR stated that the cited Reliability

[22] *Id.* P 24.

Standards either do not apply to communications between individual Control Centers or, while their effect may be to support availability, the Reliability Standards do not create an obligation to protect availability.[23]

2. Comments

19. NERC, Trade Associations, Tri-State and IRC do not support a directive that addresses the availability of communication links and data communicated between bulk electric system Control Centers. Reclamation, Appelbaum, and Liu express support for the directive, while Bonneville offers qualified support.

20. Comments opposing the proposed directive largely reiterate the petition's assertion that currently-effective Reliability Standards adequately protect the availability of communication links and data communicated between bulk electric system Control Centers. For example, NERC contends that "[w]hile IRO-002-5 and TOP-001-4 cover infrastructure within Control Centers, not between Control Centers, the requirements help protect the availability of data to be exchanged between Control Centers … [because] the data exchange infrastructure in scope of these requirements facilitates sending and receiving data between Control Centers."[24] NERC explains that if "an applicable entity lost capability of some of this data exchange infrastructure, the applicable entity could continue to send and receive data between Control Centers because of the redundant data exchange infrastructure within its Control Center.[25] In addition, NERC states that

[23] *Id.*

[24] NERC Comments at 5.

[25] *Id.*; *see also* Trade Associations Comments at 6-8, Tri-state Comments at 3.

Reliability Standards IRO-010-2 and TOP-003-3 require applicable entities to use a mutually agreeable security protocol between Control Centers. NERC explains that this supports availability by helping to ensure that conflicting protocols do not impede receipt of data between Control Centers.

21. NERC also contends that Reliability Standard EOP-008-2 helps support the availability of communication links between Control Centers by requiring reliability coordinators to have backup Control Center facilities, or backup Control Center functionality for balancing authorities and transmission operators, in addition to their primary Control Centers. NERC explains that "[t]hese backup facilities supply redundancy of some communication links and data exchange infrastructure and capabilities at the backup Control Center."[26] NERC further explains that entities with geographically diverse primary and backup Control Centers may have communication links that are physically separate from one another. NERC concludes that although "geographic diversity alone will not always provide redundancy of communication links, having backup Control Centers with different paths to communicate with other Control Centers helps support availability of communication links."[27]

22. In addition, comments opposing the directive maintain that it is premature to require protections for the availability of the communication links and data at issue. NERC states that it recognizes that "there may be additional controls that could help

[26] NERC Comments at 7; *see also* Trade Associations Comments at 9-10.

[27] NERC Comments at 7.

address" risks to the availability of data and communication links and commits to "study the risks to availability of data and communication links between Control Centers and the current controls that support availability."[28] Trade Associations, similarly, "encourage[s] the Commission to consider directing NERC to study the issue [of telecommunications security] to identify specific availability vulnerabilities and potential mitigation methods."[29]

23. IRC, while not supporting the proposed directive, "acknowledges that [the Commission] could require additional actions by responsible entities to *promote* the availability of [bulk electric system] communication links to the extent possible through contracts with telecommunications providers."[30] IRC recommends a best efforts approach similar to how supply chain risks are addressed under Reliability Standard CIP-013-1. Specifically, IRC suggests that "NERC could adopt a standard that would require responsible entities, when negotiating these service contacts, to take reasonable steps or use best efforts to maximize the availability of communication links."[31]

24. Reclamation, in support of the Commission proposal, states that the availability of communication networks should encompass links between Control Centers owned by the same entity as well as Control Centers owned by different entities. Reclamation maintains that the requirements for electronic communications be parallel to the

[28] *Id.* at 8-9.

[29] Trade Associations Comments at 12.

[30] IRC Comments at 3 (emphasis in original).

[31] *Id.*

following requirements for oral communication contained in Reliability Standard COM-001-3: (1) have electronic communication capability; (2) designate alternative electronic communication capability in the event of a failure of the primary communication capability; (3) test the alternate method of electronic communication; (4) notify the entity on the other end of the communication path if a failure is detected; and (5) establish mutually agreeable action to restore the electronic communication capability.

25. As an initial matter, Bonneville recommends delaying approval of Reliability Standard CIP-012-1 until NERC conducts a pilot project to study the most effective way to encrypt data while ensuring the data is available to responsible entities. However, if the Commission approves the Reliability Standard, Bonneville "agrees with the Commission's proposal to address the availability of communication links and data communicated between Control Centers."[32] Bonneville explains that maintaining the availability of the communication links includes addressing both redundancy and recovery. Therefore, Bonneville recommends that, if Reliability Standard CIP-012-1 is approved, "the Commission order NERC to adopt modifications requiring Responsible Entities to have incident recovery plans/continuity of operation plans addressing planning for recovery time, capability, and capacity."[33] Similarly, Appelbaum supports the proposed directive and contends that "a requirement for a continuing operations plan for

[32] Bonneville Comments at 5.

[33] *Id.* at 6.

loss of critical data resulting for the loss of Control Center functionality should be directed."[34]

3. Commission Determination

26. We determine that modifications to the CIP Reliability Standards to address the availability of communication links and data communicated between bulk electric system control centers will enhance bulk electric system reliability. As the Commission stated in Order No. 822, bulk electric system Control Centers "must be capable of receiving and storing a variety of sensitive bulk electric system data from interconnected entities."[35] We are not persuaded by the contention in the petition and comments that currently-effective Reliability Standards adequately address the directive in Order No. 822 regarding availability. Instead, we determine that the Reliability Standards cited by NERC either do not apply to communications between Control Centers or do not create an obligation to protect the availability of data between Control Centers. Accordingly, the directed modifications to the CIP Reliability Standards are not duplicative of existing Reliability Standards.

27. As the Commission explained in the NOPR, the existing Reliability Standards cited by NERC are not responsive to the availability directive in Order No. 822.[36] Reliability Standards IRO-002-5 and TOP-001-4 require responsible entities to have

[34] Appelbaum Comments at 7.

[35] Order No. 822, 154 FERC ¶ 61,037 at P 54.

[36] NOPR, 167 FERC ¶ 61,055 at P 24.

redundant and diversely routed data exchange infrastructure *within* the Control Center environment, but they do not address communications *between* individual Control Centers, which was the subject of the Commission's directive in Order No. 822.[37] While it is true that the infrastructure associated with communications within Control Centers may be useful to data exchange between Control Centers, nothing in the cited Reliability Standards creates an obligation to maintain data availability between Control Centers. Similarly, Reliability Standards IRO-010-2 and TOP-003-3 require responsible entities to have mutually agreeable security protocols for exchange of Real-time data, which may have the effect of contributing to greater availability; however, these requirements do not create an obligation, as directed in Order No. 822, to protect the availability of those communication capabilities and associated data by applying appropriate security controls.

28. As the NOPR explained, creating an obligation to protect availability, while affording flexibility in terms of what data is protected and how, is distinct from relying on currently-effective Reliability Standards whose effect may be to support availability.[38] The comments do not offer a new or persuasive reason to alter this view. For example, the Trade Associations repeat the line of reasoning in the NERC petition by "encourag[ing] the Commission to focus holistically on the broad requirements contained with [the] IRO and

[37] NOPR, 167 FERC ¶ 61,055 at P 24; NERC Comments at 5 ("IRO-002-5 and TOP-011-4 cover infrastructure within Control Centers, not between Control Centers").

[38] NOPR, 167 FERC ¶ 61,055 at P 24; NERC Comments at 6-7 (stating that alarms, recovery plans, and the ability to disable data encryption also support data availability).

TOP standards, which focus on the performance requirements necessary to support Real-time monitoring and Real-time Assessments."[39] In this circumstance, we disagree with that approach because, as the Commission observed in Order No. 822, "NERC and other commenters recognize that inter-Control Center communications play a critical role in maintaining bulk electric system reliability by, among other things, helping to maintain situational awareness and reliable bulk electric system operations through timely and accurate communication between Control Center."[40] Thus, the holistic view urged by Trade Associations does not address the gap recognized by the Commission in Order No. 822.

29. The contention in NERC's comments that Reliability Standard EOP-008-2 could also help maintain the availability of communication links between bulk electric system Control Centers, rests on the same reasoning that the ancillary benefits of an existing Reliability Standard addresses the reliability gap identified by the Commission and concomitant availability directive in Order No. 822. While we agree that a requirement to maintain a backup Control Center arguably provides a level of redundancy for a responsible entity's overall operations, it does not require redundant and diversely routed communication paths between either the primary and backup Control Centers or third-party Control Centers.

[39] Trade Associations Comments at 8.

[40] Order No. 822, 154 FERC ¶ 61,037 at P 54.

30. In addition, we do not agree that it is premature to require protections for the availability of the communication links and data communicated between bulk electric system Control Centers. While NERC and Trade Associations advocate further study of the risks associated with availability, we conclude that the risks associated with losing the availability of either data or communication links between bulk electric system Control Centers is supported by the existing record and warrants a directive to modify the CIP Reliability Standards.[41]

31. We address several related issues raised in the comments. Commenters raise a concern that directing NERC to address requirements for certain aspects of availability, in particular redundancy and diverse routing, could have significant impacts on responsible entities using third-party telecommunications providers. Specifically, Trade Associations notes that responsible entities "may not have sufficient control over the design of these networks to ensure that such requirements are met."[42] Without control over these networks, commenters suggest that the only options for addressing availability would be to construct costly private networks or implement less secure internet-based connections.[43]

[41] *See* Appelbaum Comments at 7, Bonneville Comments at 5, IRC Comments at 3, Dr. Liu Comments at 1, Reclamation Comments at 1.

[42] Trade Associations Comments at 12.

[43] *See*, *e.g.*, *id.*, Tri-State Comments at 2.

32. We are not persuaded by these arguments. Rather, as IRC correctly notes in its discussion of the challenges raised in securing third-party telecommunications networks, while the Commission lacks jurisdiction over telecommunication service providers that may own and operate the communication links between bulk electric system Control Centers, the Commission has the authority to require responsible entities to take actions to promote the availability of communication links through service contracts with network providers.[44] For example, entities could enter into service contracts with telecommunication service providers that include an agreed-upon quality of service commitment to maintain the availability of the data exchange capability to minimize the availability risk. Such arrangements would mirror the approach in Reliability Standard CIP-013-1 (Cyber Security – Supply Chain Risk Management), which also involved non-jurisdictional entities.[45] NERC should likewise consider allowing responsible entities to contract with telecommunication service providers to minimize the risk of loss of availability of communication links and data communicated between bulk electric system Control Centers in cases where communications between Control Centers are managed by a third party.

[44] IRC Comments at 3.

[45] The currently-approved supply chain risk management Reliability Standard exempts communication networks and data links between discrete Electronic Security Perimeters. *See* NERC Reliability Standard CIP-013-1, Applicability Section 4.2.3.2.

33. We agree with Reclamation's comment that protections for the availability of communication links and data communicated between bulk electric system Control Centers should encompass both entity-owned and third-party owned Control Centers. The intent of the Commission's directive is for NERC to address the risks associated with the availability of communication links and data communicated between all bulk electric system Control Centers, which will require coordination between neighboring responsible entities.

34. We reject Bonneville's recommendation that the Commission delay approval of Reliability Standard CIP-012-1 to allow for a pilot project on encryption. The record in this proceeding does not support a delay, and Bonneville's request conflicts with the implementation plan proposed by NERC.[46] Moreover, the standard drafting team addressed the Commission's finding on this issue in Order No. 822. In Order No. 822, the Commission stated "that any lag in communication speed resulting from implementation of protections should only be measurable on the order of milliseconds and, therefore, will not adversely impact Control Center communications … [but that] technical issues should be considered by the standard drafting team … e.g., by making certain aspects of the revised CIP Standards eligible for Technical Feasibility Exceptions."[47] In response, NERC stated that the standard drafting team "developed an objective-based rather than prescriptive requirement … [that] will allow Responsible

[46] *See* NERC Petition at Exhibit B.

[47] Order No. 822, 154 FERC ¶ 61,037 at P 62.

Entities flexibility in mitigating the risks posed … in a manner suited to each of their respective operational environments."[48] Accordingly, we determine not to delay approval of Reliability Standard CIP-012-1.

35. We agree with Bonneville and Appelbaum that maintaining the availability of communication networks and data should include provisions for incident recovery and continuity of operations in a responsible entity's compliance plan. We recognize that the redundancy of communication links cannot always be guaranteed; responsible entities should therefore plan for both recovery of compromised communication links and use of backup communication capability should it be needed for redundancy (i.e., satellite or other alternate backup communications).

36. Accordingly, pursuant to section 215(d)(5) of the FPA, we direct that NERC develop modifications to the CIP Reliability Standards to require protections regarding the availability of communication links and data communicated between bulk electric system Control Centers, as discussed above.

B. Scope of Bulk Electric System Data that Must Be Protected

1. NOPR

37. The NOPR observed that Reliability Standard CIP-012-1 requires the protection of Real-time Assessment and Real-time monitoring data. The Commission explained that that while Real-time Assessment is defined in the NERC Glossary, Real-time monitoring data is not defined. Accordingly, the NOPR expressed concern that Reliability Standard

[48] NERC Petition, Exhibit D (Consideration of Issues and Directives) at 7.

CIP-012-1 does not clearly indicate the types of data to be protected. To address this, the Commission proposed to direct that NERC develop modifications to the CIP Reliability Standards to clearly identify the types of data that must be protected, including whether a NERC Glossary definition of Real-time monitoring would assist with implementation and compliance.

2. Comments

38. Appelbaum and Reclamation support the development of one or more definitions. Specifically, Reclamation recommends that the Commission direct NERC to develop definitions for the terms: (1) Real-time monitoring data; (2) Real-time data; (3) BES Data; (4) Operational Data; (5) System Planning Data; (6) availability and (7) Real-time monitoring. Appelbaum supports requiring a definition of Real-time monitoring given its importance to triggering alarms that system operators respond to and because it is an input to automatic dispatch.

39. NERC and other commenters maintain that a directive is unnecessary because the terms Real-time Assessment and Real-time monitoring are clear. NERC states that the "language used in proposed Reliability Standard CIP-012-1, 'Real-time Assessment and Real-time monitoring data,' is sufficient to identify the data as described in TOP-003-3 and IRO-010-2."[49] Specifically, NERC explains that since the IRO and TOP Reliability Standards are the only currently-effective Reliability Standards that use the phrase Real-

[49] NERC Comments at 10.

time monitoring and the term Real-time Assessment, "[c]ompliance with these standards defines the data that is used in Real-time monitoring and Real-time Assessments."[50] NERC concludes that by "using this language that is only referenced in the IRO and TOP Reliability Standards families, proposed CIP-012-1 brings the data identified pursuant to TOP-003-3 and IRO-010-2 into scope."[51]

40. Trade Associations and IRC concur with NERC that the scope of data subject to the requirements of proposed Reliability Standard CIP-012-1 is adequately clear. According to Trade Associations, responsible Entities and NERC understand that the types of data covered in CIP-012-1 is the data specified for Real-time Assessment and Real-time monitoring under TOP-003 and IRO-010. Similarly, IRC notes that "all responsible entities must already know the universe of data needed for Real-time Assessment and Real-time monitoring activities in order to comply with NERC Reliability Standards TOP-003-3 and IRO-010-2."[52] Regarding the concern raised in the NOPR that the term Real-time monitoring is not defined, IRC states that it "sees no reason that the term should be presumed to mean something different from what it means in other places where it is used in the NERC Reliability Standards."[53]

[50] *Id.*

[51] *Id.*

[52] IRC Comments at 4.

[53] *Id.*

41. While Bonneville does not take a position on the NOPR proposal, it notes a concern over "creating a compliance requirement to identify how different types of information are protected."[54] Bonneville states that, generally, the use of the same data exchange infrastructure will result in all data using that infrastructure receiving the same protection regardless of data type. Therefore, Bonneville avers that, if the Commission directs NERC to define the scope of data to be protected, then "a Responsible Entity should have the option to show that all data types are protected at the highest level using the same security protocols, without having to identify and show how specific types of data are protected."[55]

3. Commission Determination

42. In view of the comments, we determine not to adopt the NOPR proposal to direct modifications to define the scope of data covered by Reliability Standard CIP-012-1. NERC, Trade Associations and IRC agree that Reliability Standard CIP-012-1 requires the protection of Real-time Assessment and Real-time monitoring data identified under Reliability Standards TOP-003-3 and IRO-010-2. This point is also confirmed in the Technical Rationale document for Reliability Standard CIP-012-1.[56] We are persuaded that responsible entities must know the types of data needed for Real-time Assessment and Real-time monitoring activities in order to comply with Reliability Standards TOP-003-3 and IRO-010-2.

---

[54] Reclamation Comments at 6.

[55] *Id.*

[56] NERC Petition, Exhibit F (Technical Rationale) at 1-2.

43. With this understanding, we are satisfied that the data protected under Reliability Standard CIP-012-1 is the same data identified under Reliability Standards TOP-003-3 and IRO-010-2. We determine that this clarification addresses the concern in the NOPR that not defining the types of data that must be protected under Reliability Standard CIP-012-1 could result in uneven compliance and enforcement. In addition, we agree with Bonneville that responsible entities may show that all data types are protected at the highest level using the same security protocols, without having to identify and show how specific types of data are protected, so long as the security protocols are reasonable.

III. Information Collection Statement

44. The FERC-725B information collection requirements contained in this final rule are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.[57] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[58] Upon approval of a collection of information, OMB will assign an OMB control number and expiration date. Respondents subject to the filing requirements of this rule will not be penalized for failing to respond to the collection of information unless the collection of information displays a valid OMB control number.

[57] 44 U.S.C. 3507(d).

[58] 5 CFR 1320.

45. The Commission received no comments on the validity of the burden and cost estimates in the NOPR. The Commission is updating the burden estimates and labor costs contained in the NOPR. The Commission in this Final Rule corrected an error from the NOPR in the row "Identification of Security Protection Application (if not owned by same Responsible Entity) (Requirement R1.3)" where the total number of hours was understated by 100,000, and all calculations based upon this error.

46. The Commission is submitting these reporting and recordkeeping requirements to OMB for its review and approval under section 3507(d) of the PRA. Comments are solicited on the Commission's need for this information, whether the information will have practical utility, the accuracy of the provided burden estimate, ways to enhance the quality, utility, and clarity of the information to be collected, and any suggested methods for minimizing the respondent's burden, including the use of automated information techniques.

47. The Commission bases its paperwork burden estimates on the changes in paperwork burden presented by Reliability Standard CIP-012-1.

48. The NERC Compliance Registry, as of December 2019, identifies approximately 1,482 unique U.S. entities that are subject to mandatory compliance with Reliability Standards. Of this total, we estimate that 719 entities will face an increased paperwork burden under proposed Reliability Standard CIP-012-1. Based on these assumptions, we estimate the following reporting burden:

FERC-725B, Modifications Due to the Final Rule in Docket No. RM18-20-000					
	No. of Respondents (1)	**No. of Responses [59] per Respondent (2)**	**Total No. of Responses (1)X(2)=(3)**	**Avg. Burden Hrs. & Cost Per Response[60] (4)**	**Total Annual Burden Hours & Total Annual Cost (3)X(4)=5**
Implementation of Documented Plan(s) (Requirement R1)[61]	719	1	719	128 hrs.; $11,776	92,032 hrs.; $8,466,944
Document Identification of Security Protection (Requirement R1.1)[61]	719	1	719	40 hrs.; $3,680	28,560 hrs.; $2,645,920
Identification of Security Protection Application (if owned by same Responsible Entity) (Requirement R1.2)[61]	719	1	719	20 hrs.; $1,840	14,280 hrs.; $1,322,960
Identification of Security Protection Application (if not owned by same Responsible Entity) (Requirement R1.3)[61]	719	1	719	160 hrs.; $14,720	14,240 hrs.; $10,583,680

[59] We consider the filing of an application to be a "response."

Maintaining Compliance (ongoing, starting in Year 2)	719	1	719	83 hrs.; $7,636	59,677 hrs.; $5,490,284
Total (one-time, in Year 1)			2,876		250,212 hrs.; $23,019,504
Total (ongoing, starting in Year 2)			719		59,677 hrs.; $5,490,284

49. The one-time burden (in Year 1) for the FERC-725B information collection will be averaged over three years:

- 250,212 hours ÷ 3 = 83,404 hours/year over Years 1-3
- The number of one-time responses for the FERC-725B information collection is also averaged over Years 1-3: 2,876 responses ÷ 3 = 959 responses/year

---

[60] The hourly cost for wages plus benefits is based on the average of the occupational categories for 2018 found on the Bureau of Labor Statistics website (http://www.bls.gov/oes/current/naics2_22.htm):

Information Security Analysts (Occupation Code: 15-1122): $61.494

Computer and Mathematical (Occupation Code: 15-0000): $63.54

Legal (Occupation Code: 23-0000): $142.86

Computer and Information Systems Managers (Occupation Code: 11-3021): $98.81.

These various occupational categories' wage figures are averaged as follows: $61.494/hour + $63.54/hour + $142.86/hour + $98.81/hour) ÷ 4 = $91.70/hour. The resulting wage figure is rounded to $92.00/hour for use in calculating wage figures in the Final Rule in Docket No. RM18-20-000.

[61] This includes the record retention costs for the one-time and the on-going reporting documents.

50. The average annual number (for Years 1-3) of responses and burden for one-time and ongoing burden will total:

- 1,678 responses [959 responses (one-time) + 719 responses (ongoing)]
- 143,081 burden hours [83,404 hours (one-time) + 59,677 hours (ongoing)] hours (ongoing)]

51. Title: Mandatory Reliability Standards for Critical Infrastructure Protection [CIP] Reliability Standards.

Action: Revisions to FERC-725B information collection.

OMB Control No.: 1902-0248.

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

Frequency of Responses: One-time and Ongoing.

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 NERC's proposed Reliability Standard CIP-012-1 pursuant to section 215(d)(2) of the FPA because they improve upon the currently-effective suite of cyber security Reliability Standards.

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.

52. 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: Ellen Brown, Office of the Executive Director, e-mail: DataClearance@ferc.gov, phone: (202) 502-8663, fax: (202) 273-0873].

53. Please send comments concerning the collection of information and the associated burden estimate to the Commission, and to the Office of Management and Budget, Office of Information and Regulatory Affairs, 725 17th Street NW, Washington, DC 20503, Washington, DC 20503 [Attention: Desk Officer for the Federal Energy Regulatory Commission]. For security reasons, comments to OMB should be submitted by e-mail to: oira_submission@omb.eop.gov. Comments submitted to OMB should include FERC-725B (OMB Control No. 1902-0248).

IV. Environmental Analysis

54. 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.[62] 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.[63] The actions proposed herein fall within this categorical exclusion in the Commission's regulations.

V. Regulatory Flexibility Act Analysis

55. The Regulatory Flexibility Act of 1980 (RFA) generally requires a description and analysis of proposed and final rules that will have significant economic impact on a

[62] *Regulations Implementing the National Environmental Policy Act of 1969*, Order No. 486, FERC Stats. & Regs. ¶ 30,783 (1987).

[63] 18 CFR 380.4(a)(2)(ii).

substantial number of small entities.[64] The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.[65] The SBA revised its size standard for electric utilities (effective January 22, 2014) to a standard based on the number of employees, including affiliates (from the prior standard based on megawatt hour sales).[66]

56. Reliability Standard CIP-012-1 is expected to impose an additional burden on 719 entities[67] (reliability coordinators [RC], generator operators [GOP], generator owners [GO], transmission operators [TOP], balancing authorities [BA], and transmission owners [TO]).

57. Of the 719 affected entities discussed above, we estimate that approximately 82% percent of the affected entities are small entities. We estimate that each of the 590 small entities to whom the modifications to Reliability Standard CIP-012-1 apply will incur one-time, non-paperwork cost in Year 1 of approximately $17,051, plus

[64] 5 U.S.C. 601-12.

[65] 13 CFR 121.101.

[66] 13 CFR 121.201, Subsection 221.

[67] 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. These entities may be included in the SBA categories for: Hydroelectric Power Generation, Fossil Fuel Electric Power Generation, Nuclear Electric Power Generation, Solar Electric Power Generation, Wind Electric Power Generation Geothermal Electric Power Generation, Biomass Electric Power Generation, Other Electric Power Generation, Biomass Electric Power Generation, or Electric Bulk Power Transmission and Control. These categories have thresholds for small entities varying from 250-750 employees. For the analysis in this Final Rule, we are using a conservative threshold of 750 employees.

paperwork cost in Year 1 of $32,016, giving a total cost in Year 1 of $49,067. In Year 2 and Year 3, each entity will incur only the ongoing annual paperwork cost of $7,594. We do not consider the estimated costs for these 590 small entities to be a significant economic impact.

58. Accordingly, we certify that Reliability Standard CIP-012-1 will not have a significant economic impact on a substantial number of small entities.

VI. Effective Date and Congressional Notification

59. This Final Rule is effective **[insert date 60 days after publication in the Federal Register]**. The Commission has determined, with the concurrence of the Administrator of the Office of Information and Regulatory Affairs of OMB, that this rule is not a "major rule" as defined in section 351 of the Small Business Regulatory Enforcement Fairness Act of 1996. This Final Rule is being submitted to the Senate, House, and Government Accountability Office.

VII. Document Availability

60. 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) and in the Commission's Public Reference Room during normal business hours (8:30 a.m. to 5:00 p.m. Eastern time) at 888 First Street, NE, Room 2A, Washington, DC 20426.

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

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

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

Note: the following Appendix will not appear in the *Code of Federal Regulations*.

Appendix
Commenters

Abbreviation	Commenter
Appelbaum	Jonathan Appelbaum
Bonneville	Bonneville Power Administration
IRC	ISO/RTO Council
Dr. Liu	Dr. Chen-Ching Liu
NERC	North American Electric Reliability Corporation
Reclamation	Bureau of Reclamation
Trade Associations	American Public Power Association, Edison Electric Institute, National Rural Electric Cooperative Association
Tri-State	Tri-State Generation and Transmission Association, Inc.