BILLING CODE 6717-01-P
DEPARTMENT OF ENERGY
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM18-20-000]

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

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Federal Energy Regulatory Commission (Commission) proposes to approve 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 the proposed Reliability Standard for Commission approval in response to a Commission directive. In addition, the Commission proposes to direct that NERC develop certain modifications to Reliability Standard CIP-012-1 to require protections regarding the availability of communication links and data communicated between bulk electric system control centers and, further, to clarify the types of data that must be protected.

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. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format.
- Mail/Hand Delivery: Those unable to file electronically may mail or hand-deliver comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE, Washington, DC 20426.

Instructions: For detailed instructions on submitting comments and additional information on the rulemaking process, see the Comment Procedures Section of this document.

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:

1. Pursuant to section 215(d)(2) of the Federal Power Act (FPA),[1] the Commission proposes to approve 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 the proposed Reliability Standard for Commission approval in response to a Commission directive in Order No. 822.[2] Specifically, pursuant to section 215(d)(5) of the FPA, the Commission directed that NERC develop modifications to require responsible entities to 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)."[3]

2. Proposed Reliability Standard CIP-012-1 is intended to augment the currently-effective Critical Infrastructure Protection (CIP) Reliability Standards to mitigate cybersecurity risks associated with communications between bulk electric system Control Centers.[4] Specifically, proposed Reliability Standard CIP-012-1 supports situational

---

[1] 16 U.S.C. 824o(d)(2) (2012).

[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).

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

[4] 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." Glossary of Terms Used in NERC Reliability Standards (NERC Glossary),

(continued…)

awareness and reliable bulk electric system operations 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.[5] Accordingly, the Commission proposes to approve proposed Reliability Standard CIP-012-1 based on a determination that the standard is largely responsive to the Commission's directive in Order No. 822 and improves the cybersecurity posture of applicable entities.

3. However, we are concerned that there still may be certain cyber security risks associated with the protection of communications links and sensitive bulk electric system data communicated between bulk electric system Control Centers that are not adequately addressed in NERC's proposal. First, proposed 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.[6] As discussed below, at this time, we are not persuaded by NERC's explanation that certain currently-effective CIP Reliability Standards address the issue of availability.

---

http://www.nerc.com/files/glossary_of_terms.pdf. The acronym BES refers to the bulk electric system.

[5] 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).

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

Second, proposed 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 proposed Reliability Standard or the NERC Glossary. Clarification of the types of covered data is warranted.

4. To address these issues, pursuant to section 215(d)(5) of the FPA, the Commission proposes to direct that NERC develop modifications to the CIP Reliability Standards to: (1) require protections regarding the availability of communication links and data communicated between bulk electric system Control Centers; and (2) clearly identify the types of data that must be protected.

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.[7] Pursuant to section 215 of the FPA, the

[7] 16 U.S.C. 824o(e).

Commission established a process to select and certify an ERO,[8] and subsequently certified NERC.[9]

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.[10] Specifically, the Commission directed NERC to, among other things, develop modifications to the CIP Reliability Standards to require responsible entities to 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)."[11] 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

[8] *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).

[9] *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).

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

[11] *Id.* P 53.

system reliability by . . . helping to maintain situational awareness and support reliable operations through timely and accurate communication between Control Centers."[12]

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."[13] The Commission also recognized that the data managed by responsible entities has different attributes that may require different information protection controls, and the Commission stated that NERC should consider the different attributes of bulk electric system data as it assesses appropriate information protection controls. The Commission concluded that NERC "should have flexibility in the manner in which it addresses the Commission's directive."[14]

8. In Order No. 822, the Commission found to be reasonable the following principles outlined in NERC's comments in that Commission proceeding regarding protections for communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers:

---

[12] *Id.* P 54 (citing NERC Comments at 20).

[13] *Id.* P 54.

[14] *Id.* P 55.

> (1) should not have an adverse effect on reliability, including the recognition of instances where the introduction of latency could have negative results; (2) should account for the risk levels of assets and information being protected, and require protections that are commensurate with the risks presented; and (3) should be results-based in order to provide flexibility to account for the range of technologies and entities involved in bulk electric system communications.[15]

In addition, the Commission cautioned that "not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection."[16] Therefore, the Commission determined that NERC should develop controls that reflect the risk being addressed in a reasonable manner.

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

9. 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.[17] NERC states that the purpose of the proposed Reliability Standard 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.

---

[15] *Id*.

[16] *Id*. P 56.

[17] Proposed Reliability Standard CIP-012-1 is not attached to this notice of proposed rulemaking (NOPR). The proposed Reliability Standards are available on the Commission's eLibrary document retrieval system in Docket No. RM18-20-000 and on the NERC website, www.nerc.com.

10. NERC explains that, although the Commission directed modifications to Reliability Standard CIP-006-6, the standard drafting team determined to address the Commission's communications directive by developing a new Reliability Standard. According to NERC, the differences in the scope and applicability between the existing requirements of Reliability Standard CIP-006-1 and the Commission's directive necessitated the development of a new Reliability Standard. Specifically, NERC notes that while Reliability Standard CIP-006-6, Requirement R1, Part 1.10 mandates protections for nonprogrammable communication components outside a Physical Security Perimeter (PSP) but inside the same Electronic Security Perimeter (ESP) for certain Cyber Assets, proposed Reliability Standard CIP-012-1 "requires protections for communications between Control Centers that transmit certain data regardless of the location of Cyber Assets inside or outside a PSP or ESP."[18] In addition, NERC explains that unlike Reliability Standard CIP-006-6, which applies to high and medium impact BES Cyber Assets at Control Centers, proposed Reliability Standard CIP-012-1 applies to assets associated with communications between certain Control Centers.

11. NERC states that proposed 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

[18] NERC Petition at 9.

Control Centers."[19] 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.[20]

12. NERC posits that, consistent with the Commission's directive in Order No. 822, the risks posed by different types of BES Control Centers and the associated data communicated between the Control Centers were considered by the standard drafting team to determine its appropriate scope and applicability.[21] With regard to functional entities and facilities, NERC states that proposed Reliability Standard CIP-012-1 applies to balancing authorities, generator operators, reliability coordinators, transmission operators and transmission owners that own or operate a Control Center. NERC explains that proposed Reliability Standard CIP-012-1 applies to all Control Centers, with one exemption discussed below, "regardless of the impact level of BES Cyber Systems located at or associated with those control centers."[22] In that regard, NERC explains that the standard drafting team determined that the sensitivity of data communicated between Control Centers "is not necessarily dependent on the impact level of the BES Cyber

[19] *Id.* at 10.

[20] *Id.* at 3.

[21] *Id.*

[22] *Id.* at 10.

Systems located at or associated with the Control Centers."[23] NERC states that the standard drafting team, instead, focused on the types of Real-time data a Control Center will communicate and whether the compromise of that data would pose a high risk to bulk electric system reliability.

13. As noted above, the types of data within the scope of proposed Reliability Standard CIP-012-1 consists 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. However, NERC points out that proposed Reliability Standard CIP-012-1 exempts Control Centers "that transmit[] to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource of transmission station or substation co-located with the transmitting Control Center."[24] NERC explains that proposed 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."[25] According to NERC, while Operational Planning Analysis data provides information for next-day operations, "entities adjust their operating actions during the current day based on the data from Real-time Assessments

[23] *Id.*

[24] *Id.* at 11.

[25] *Id.* at 12.

and Real-time monitoring."[26] NERC contends that if there is a risk that Operational Planning Analysis data has been compromised, the responsible entity has the opportunity to verify the data prior to any impact on Real-time operations. Therefore, NERC concludes that while "an Operational Planning Analysis factors into how an entity operates, there is less of a risk that an entity would act on compromised data from an Operational Planning Analysis given it will base its operating actions on Real-time inputs."[27]

14. NERC also indicates that data at rest and oral communications fall outside the scope of proposed 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, 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 proposed 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."[28] NERC notes that Reliability Standard COM-001-3 requires reliability coordinators, balancing authorities, and transmission operators to have alternative interpersonal communication capability, which could be used if there is a suspected compromise of oral communication on one channel.

---

[26] *Id*.

[27] *Id*. at 13.

[28] *Id*. at 14.

II. Discussion

15. Pursuant to section 215(d)(2) of the FPA, the Commission proposes to approve proposed Reliability Standard CIP-012-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. The proposed Reliability Standard will enhance existing protections for bulk electric system reliability by augmenting the currently-effective CIP Reliability Standards to mitigate cybersecurity risks associated with communications between bulk electric system Control Centers. Specifically, consistent with the Commission's directive in Order No. 822, proposed 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 and Real-time monitoring data transmitted between bulk electric system Control Centers.

16. While the Commission proposes to approve Reliability Standard CIP-012-1, certain cyber security risks associated with communications between bulk electric system Control Centers may not be fully addressed even with the implementation of the proposed Reliability Standard. As discussed below, the Commission is concerned that a significant cyber security risk associated with the protection of communications links and sensitive bulk electric system data communicated between bulk electric system Control Centers may persist because: (1) the CIP Reliability Standards do not address the availability of communication links and data communicated between bulk electric system Control Centers; and (2) proposed 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.

17. To address these gaps, the Commission seeks comment on proposals to direct NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP Reliability Standards to: (1) require protections regarding the availability of communication links and data communicated between bulk electric system Control Centers; and (2) clearly identify the types of data that must be protected.

18. 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

Order No. 822

19. In Order No. 822, the Commission directed that NERC "should identify the scope of sensitive bulk electric system data that must be protected and specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted or at rest."[29] In addition, the Commission clarified that "the directed modification should encompass communication links and data for intra-Control Center and inter-Control Center communications."[30]

---

[29] Order No. 822, 154 FERC ¶ 61,037 at P 56.

[30] *Id.* P 58.

20. Specifically, the Commission explained that bulk electric system Control Centers must be capable of exchanging and storing sensitive bulk electric system data from interconnected entities in order for responsible entities to adequately perform their reliability functions. The Commission determined "that additional measures to protect both the integrity and *availability* of sensitive bulk electric system data are warranted."[31] The Commission explained that protecting the availability of sensitive bulk electric system data involves ensuring that the data required for bulk electric system operations is available when needed. The Commission responded to concerns that the risks posed by bulk electric system communication networks do not justify the cost of implementing controls by explaining that communications between Control Centers are fundamental to reliable bulk electric system operations. The Commission, however, also recognized that "not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection."[32] The Commission therefore determined that it expected NERC to develop controls that reflect the associated risk and that can be implemented in a reasonable manner.

NERC Petition

21. NERC states that proposed Reliability Standard CIP-012-1, Requirement R1 mandates that:

---

[31] *Id.* P 54 (emphasis added).

[32] *Id.* P 56.

> each Responsible Entity develop a plan to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between and applicable Control Centers.[33]

NERC acknowledges that Order No. 822 directed that "NERC should develop measures to protect the confidentiality, integrity, and availability of sensitive [bulk electric system] data."[34] NERC states, however, that while proposed Reliability Standard CIP-012-1 requires protections for the confidentiality (i.e., unauthorized disclosure) and integrity (i.e., unauthorized modification) of Real-time Assessment and Real-time monitoring data, the availability of that data is addressed in currently-effective Reliability Standards.

22. Specifically, NERC maintains that Reliability Standard IRO-002-5 "requires redundant and diversely routed data exchange infrastructure within the Reliability Coordinator's primary Control Center in order to exchange Real-time data used in Real-time monitoring and Real-time Assessments with Balancing Authorities, Transmission Operators, and other entities the Reliability Coordinator deems necessary."[35] Similarly, NERC states that Reliability Standard TOP-001-4 "requires Balancing Authorities and Transmission Operators to have redundant and diversely routed data exchange infrastructure to exchange Real-time data."[36] According to NERC, the "redundancy of

---

[33] Petition at 15-16.

[34] *Id.* at 17.

[35] *Id.* at 18.

[36] *Id.*

data exchange infrastructure helps to ensure the availability of critical Real-time data for Control Centers."[37] Further, NERC notes that Reliability Standards IRO-010-2 and TOP-003-3 require reliability coordinators, transmission operators, and balancing authorities to use a mutually agreeable security protocol for exchange of Real-time data. NERC contends that, by agreeing on security protocols, entities communicate directly with the appropriate entities rather than having to translate different protocols, which helps to ensure the availability of Real-time data.

Discussion

23. We are not persuaded by the explanation in NERC's petition that currently-effective CIP Reliability Standard requirements address the availability directive in Order No. 822. Sensitive bulk electric system data generally includes monitoring, operational, and system planning data. Ensuring timely and reliable access to and use of this information is essential to the reliable operation of the bulk electric system. As the Commission noted 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."[38] In particular, the Commission stated that additional protections to address the availability of sensitive bulk electric system data are warranted.[39]

---

[37] *Id.*

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

[39] *Id.*

24. We are not persuaded that the currently-effective Reliability Standards cited in NERC's petition require responsible entities to protect the availability of sensitive bulk electric system data in a manner consistent with the directives in Order No. 822. For instance, Reliability Standards IRO-002-5 and TOP-001-4 require responsible entities to have redundant and diversely routed data exchange infrastructure *within* the Control Center environment, but do not pertain to communications *between* individual Control Centers, which was the subject of the Commission's directive in Order No. 822. 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. 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 improve availability.

25. Bonneville Power Administration (BPA) and CenterPoint Energy Houston Electric addressed this distinction during the standards development process when they responded to the standard drafting team's assertion that the availability directive is adequately addressed by currently-effective CIP Reliability Standards. BPA explained that "[w]hile the requirements of TOP-001-4 and IRO-002-5 (redundant and diverse routing of data) can be used to achieve increased Availability, it can also be achieved through other equally effective methods . . . [and] [t]herefore, 'availability' is not adequately addressed

by TOP-001-4 and IRO-002-5 and limits entities' options to address availability by other methods more appropriate to their systems."[40] CenterPoint stated that, "TOP-001-4 and IRO-002-5 do not ensure availability or communication of data between inter-entity and intra-entity Control Centers, but only the redundancy of infrastructure internal to the requesting entity's primary Control Center."[41]

26. Not addressing the availability of covered communication links and data could lead to unreliable operations resulting from the inability to communicate data between Control Centers. While NERC contends that currently-effective CIP Reliability Standards adequately protect the availability of sensitive bulk electric system data, there is no obligation on responsible entities to affirmatively protect the availability of such data. Moreover, while the Commission in Order No. 822 allowed NERC flexibility in what data is protected and how, NERC has not addressed the directive to protect the availability of sensitive bulk electric system data.

27. Accordingly, pursuant to section 215(d)(5) of the FPA, the Commission proposes to 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. We seek comment on this proposal.

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

Order No. 822

[40] NERC Petition at page 273 of pdf.

[41] *Id.* at page 274 of pdf.

28. In Order No. 822, the Commission stated that NERC "should identify the scope of sensitive bulk electric system data that must be protected and specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted or at rest."[42] In addition, the Commission clarified that "the directed modification should encompass communication links and data for intra-Control Center and inter-Control Center communications."[43]

NERC Petition

29. NERC states that proposed Reliability Standard CIP-012-1 applies to Real-time Assessment and Real-time monitoring data due to the critical nature of the information. NERC explains that:

> Reliability Coordinators and Transmission Operators must perform Real-time Assessments every 30 minutes to assess the conditions on the system and determine whether there are any actual or potential exceedances of System Operating Limits or Interconnection Reliability Operating Limits.[44]

In addition, NERC states that reliability coordinators, balancing authorities, and transmission operators must perform Real-time monitoring. NERC contends that since responsible entities "operate and monitor the [bulk electric system] according to this Real-time information, it is of critical importance that it is accurate."[45]

---

[42] Order No. 822, 154 FERC ¶ 61,037 at P 56.

[43] *Id.* P 58.

[44] NERC Petition at 12.

[45] *Id.*

Discussion

30. Proposed Reliability Standard CIP-012-1 requires the protection of Real-time Assessment and Real-time monitoring data. While Real-time Assessment is broadly defined by NERC, Real-time monitoring data is not defined. Moreover, the proposed Reliability Standard does not specifically indicate the types of data to be protected. We are concerned that without further clarity, Reliability Standard CIP-012-1 may be implemented and enforced in an inconsistent manner.

31. In the Technical Rationale document appended to NERC's petition, NERC explained in more detail (relative to the language of the proposed Reliability Standard's requirements) what data should be protected under proposed Reliability Standard CIP-012-1:

> The SDT recognized the FERC reference to additional Reliability Standards and the responsibilities to protect the applicable data in accordance with NERC Reliability Standards TOP-003 and IRO-010. The SDT used these references to drive the identification of sensitive BES data and chose to base the CIP-012-1 requirements on the Real-time data specification elements in these standards. This approach provides consistent scoping of identified data, and does not require each entity to devise its own list or inventory of this data. Many entities are required to provide this data under agreements executed with their [reliability coordinator (RC)], [balancing authority (BA)] or [transmission operator (TOP)]. Data requiring protection in CIP-012-1 consists of a subset of data that is identified by the RC, BA, and TOP in the TOP-003 and IRO-010 data specification standards,

> limited to Real-time Assessment data and Real-time monitoring data.[46]

The references to Reliability Standards TOP-003 and IRO-010 in the Technical Rationale document are not found in proposed Reliability Standard CIP-012-1. Instead Requirement R1 of proposed Reliability Standard CIP-012-1 only uses the terms "Real-time Assessment and Real-time monitoring data." In addition, as the Technical Rational indicates at the outset: "This Technical Rationale and Justification for CIP-012-1 is not a Reliability Standard and should not be considered mandatory and enforceable."[47]

32. Not clearly defining the types of data that must be protected under the proposed Reliability Standard could result in uneven compliance and enforcement. The term "Real-time Assessment" is broadly defined in the NERC Glossary of Terms, and the term "Real-time monitoring" is not defined at all. These terms, alone, may not be understood or enforced in a consistent manner. This concern arose during the standard drafting process in comments regarding an earlier version of the proposed Reliability Standard, which was later modified.[48] Still relevant, however, are concerns raised regarding the potential ambiguities associated with enforcement of the scope of data that must be

---

[46] NERC Petition, Exhibit F (Technical Rationale) at 1-2; *see also* Exhibit E (Draft Implementation Guidance) at 5 (providing similar context as to what data should be protected).

[47] NERC Petition, Exhibit F at iv; *see also* Exhibit E at 3 (indicating that the draft Implementation Guidance document only provides examples in achieving compliance).

[48] An early version of Requirement R1 of proposed Reliability Standard CIP-012-1 identified the scope of the data to be protected as "data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring."

protected. In particular, while NERC identifies Reliability Standards IRO-002-5, Requirements R5 and R6, and TOP-001-4, Requirements R10 and R11 in discussing the parameters of Real-time monitoring data, the information outlined in the identified requirements is not included in the language of proposed Reliability Standard CIP-012-1 itself and, therefore, implementation and compliance concerns may arise.[49]

33. The compliance obligations imposed under proposed Reliability Standard CIP-012-1 should be clear in order for responsible entities to effectively and reasonably implement the required protections. The lack of clarity regarding the scope of Real-time monitoring data is inconsistent with principles outlined by the Commission in Order No. 672.[50] In particular, the lack of clarity may result in: (1) a failure to establish a clear and unambiguous requirement regarding the protection of Real-time monitoring data;[51] and (2) a failure to identify clear and objective criterion to facilitate consistent and non-preferential enforcement since responsible entities will not have a clear understanding of the Real-time monitoring data to be protected.[52] Since the controls required under Reliability Standard CIP-012-1 are plan-based, the scope of data to be protected should be clear and unambiguous so that responsible entities will accurately identify vulnerabilities or risks requiring mitigation.

---

[49] *See* NERC Petition at page 505 of pdf.

[50] Order No. 672, 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328.

[51] *Id.* PP 322, 325.

[52] *Id.* P 327.

34. Therefore, pursuant to section 215(d)(5) of the FPA, the Commission proposes to direct that NERC develop modifications to the CIP Reliability Standards to clearly identify the types of data that must be protected. We seek comment on this proposal. In particular, we seek comment on the specific information covered by the term "Real-time monitoring" and whether a NERC Glossary definition would assist with implementation and compliance.

III. Information Collection Statement

35. The FERC-725B information collection requirements contained in this notice of proposed rulemaking are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.[53] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[54] 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 these collections of information unless the collections of information display a valid OMB control number. The Commission solicits comments on the Commission's 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

[53] 44 U.S.C. 3507(d) (2012).

[54] 5 CFR 1320.11.

any suggested methods for minimizing respondents' burden, including the use of automated information techniques.

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

37. The NERC Compliance Registry, as of December 2017, identifies approximately 1,250 unique U.S. entities that are subject to mandatory compliance with Reliability Standards. Of this total, we estimate that 714 entities will face an increased paperwork burden under proposed Reliability Standard CIP-012-1. Based on these assumptions, we estimate the following reporting burden:

Annual Changes Proposed by the NOPR in Docket No. RM18-20-000

	No. of Respondents (1)	No. of Responses[55] per Respondent (2)	Total No. of Responses (1)X(2)=(3)	Avg. Burden Hrs. & Cost Per Response[56] (4)	Total Annual Burden Hours & Total Annual Cost (3)X(4)=5
Implementation of Documented Plan(s) (Requirement R1)[57]	714	1	714	128 hrs.; $10,496	91,392 hrs.; $7,494,144
Document Identification of Security Protection (Requirement R1.1)[57]	714	1	714	40 hrs.; $3,280	28,560 hrs.; $2,341,920

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

[56] The loaded hourly wage figure (includes benefits) is based on the average of the occupational categories for 2017 found on the Bureau of Labor Statistics website (http://www.bls.gov/oes/current/naics2_22.htm):

Information Security Analysts (Occupation Code: 15-1122): $42.84

Computer and Mathematical (Occupation Code: 15-0000): $44.02

Legal (Occupation Code: 23-0000): $143.68

Computer and Information Systems Managers (Occupation Code: 11-3021): $96.51

These various occupational categories' wage figures are averaged and weighted equally as follows: ($42.84/hour + $44.02/hour + $143.68/hour + $96.51/hour) ÷ 4 = $81.76/hour. The resulting wage figure is rounded to $82.00/hour for use in calculating wage figures in the NOPR in Docket No. RM18-20-000.

[57] This is a one-time reporting requirement.

Identification of Security Protection Application (if owned by same Responsible Entity) (Requirement R1.2)[57]	714	1	714	20 hrs.; $1,640	14,280 hrs.; $1,170,960
Identification of Security Protection Application (if not owned by same Responsible Entity) (Requirement R1.3)[57]	714	1	714	160 hrs.; $13,120	14,240 hrs.; $9,367,680
Maintaining Compliance (ongoing)	714	1	714	83 hrs.; $6,806	59,262 hrs.; $4,859,484
Total (one-time)			2,856		148,472 hrs.; $12,174,704
Total (ongoing)			714		59,262 hrs.; $4,859,484
TOTAL			3,570		207,734 hrs.; $17,034,188

38. The one-time burden for the FERC-725B information collection will be averaged over three years:

- 148,472 hours ÷ 3 = 49,491 hours/year over three years
- The number of one-time responses for the FERC-725B information collection is also averaged over three years: 2,856 responses ÷ 3 = 952 responses/year

39. The responses and burden for one-time and ongoing burden for Years 1-3 will total respectively as follows:

- Year 1: 1,666 responses [952 responses (one-time) + 714 responses (ongoing)]; 108,753 hours [49,491 hours (one-time) + 59,262 hours (ongoing)]
- Year 2: 1,666 responses [952 responses (one-time) + 714 responses (ongoing)]; 108,753 hours [49,491 hours (one-time) + 59,262 hours (ongoing)]
- Year 3: 1,666 responses [952 responses (one-time) + 714 responses (ongoing)]; 108,753 hours [49,491 hours (one-time) + 59,262 hours (ongoing)]

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

Action: Proposed 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 notice of proposed rulemaking proposes to approve the requested modifications to Reliability Standards pertaining to critical infrastructure protection. As discussed above, the Commission proposes to approve 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.

41. 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].

42. 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, 725 17th Street NW, 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 RM18-20-000 and FERC-725B (OMB Control No. 1902-0248).

IV. Environmental Analysis

43. 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.[58] 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

[58] *Regulations Implementing the National Environmental Policy Act of 1969*, Order No. 486, FERC Stats. & Regs. ¶ 30,783 (1987) (cross-referenced at 41 FERC ¶ 61,284).

not substantially change the effect of the regulations being amended.[59] The actions proposed herein fall within this categorical exclusion in the Commission's regulations.

V. Regulatory Flexibility Act Analysis

44. The Regulatory Flexibility Act of 1980 (RFA) generally requires a description and analysis of proposed rules that will have significant economic impact on a substantial number of small entities.[60] The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.[61] 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).[62]

45. Proposed Reliability Standard CIP-012-1 is expected to impose an additional burden on 714 entities[63] (reliability coordinators, generator operators, generator owners, interchange coordinators or authorities, transmission operators, balancing authorities, and transmission owners).

---

[59] 18 CFR 380.4(a)(2)(ii).

[60] 5 U.S.C. 601-12 (2012).

[61] 13 CFR 121.101.

[62] 13 CFR 121.201, Subsection 221.

[63] 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 due to each affected entity falling within the role of Electric Bulk Power Transmission and Control (NAISC Code: 221121).

46. Of the 714 affected entities discussed above, we estimate that approximately 82% percent of the affected entities are small entities. We estimate that each of the 585 small entities to whom the proposed modifications to Reliability Standard CIP-012-1 apply will incur one-time costs of approximately $17,051 per entity to implement the proposed Reliability Standards, as well as the ongoing paperwork burden reflected in the Information Collection Statement (approximately $6,806 per year per entity). We do not consider the estimated costs for these 585 small entities to be a significant economic impact. Accordingly, we propose to certify that proposed Reliability Standard CIP-012-1 will not have a significant economic impact on a substantial number of small entities.

VI. Comment Procedures

47. 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. RM18-20-000, and must include the commenter's name, the organization they represent, if applicable, and address.

48. The Commission encourages comments to be filed electronically via the eFiling link on the Commission's web site at http://www.ferc.gov. The Commission accepts most standard word processing formats. Documents created electronically using word processing software should 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.

49. Commenters that are not able to file comments electronically must send an original of their comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE, Washington, DC 20426.

50. 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.

VII. Document Availability

51. 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.

52. 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.

53. 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 direction of the Commission.

Issued: April 18, 2019

Nathaniel J. Davis, Sr.,
Deputy Secretary.

[FR Doc. 2019-08236 Filed: 4/23/2019 8:45 am; Publication Date: 4/24/2019]