Proposed Rules

Federal Register
Vol. 82, No. 206
Thursday, October 26, 2017

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

18 CFR Part 40

[Docket No. RM17–11–000]

Revised Critical Infrastructure Protection Reliability Standard CIP–003–7—Cyber Security—Security Management Controls

AGENCY: Federal Energy Regulatory Commission, DOE.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Federal Energy Regulatory Commission (Commission) proposes to approve Critical Infrastructure Protection (CIP) Reliability Standard CIP–003–7 (Cyber Security—Security Management Controls), submitted by the North American Electric Reliability Corporation (NERC). Proposed Reliability Standard CIP–003–7 improves upon the current Commission-approved CIP Reliability Standards by clarifying the obligations pertaining to electronic access control for low impact BES Cyber Systems; adopting mandatory security controls for transient electronic devices (*e.g.,* thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems) used at low impact BES Cyber Systems; and requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems. In addition, the Commission proposes to direct NERC to develop certain modifications to the NERC Reliability Standards to provide clear, objective criteria for electronic access controls for low impact BES Cyber Systems; and address the need to mitigate the risk of malicious code that could result from third-party transient electronic devices.

DATES: Comments are due December 26, 2017.

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: Matthew Dale (Technical Information), Office of Electric Reliability, Federal Energy Regulatory Commission, 888 First Street NE., Washington, DC 20426, (202) 502–6826, *matthew.dale@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 of the Federal Power Act (FPA),[1] the Commission proposes to approve Critical Infrastructure Protection (CIP) Reliability Standard CIP–003–7 (Cyber Security—Security Management Controls). The North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), submitted proposed Reliability Standard CIP–003–7 in response to directives in Order No. 822.[2] The Commission also proposes to approve the associated violation risk factors and violation severity levels, implementation plan and effective dates proposed by NERC. In addition, the Commission proposes to approve the modified definitions of Transient Cyber Asset and Removable Media as well as the retirement of the definitions for Low Impact External Routable Connectivity (LERC) and Low Impact Electronic Access Point (LEAP) in the NERC Glossary of Terms Used in NERC Reliability Standards (NERC Glossary). Further, the Commission proposes to approve the retirement of Reliability Standard CIP–003–6.

2. Proposed Reliability Standard CIP–003–7 is designed to mitigate the cybersecurity risks to bulk electric system facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable as a result of a cybersecurity incident, would affect the reliable operation of the bulk electric system.[3] As discussed below, the Commission proposes to determine that proposed Reliability Standard CIP–003–7 is just, reasonable, not unduly discriminatory or preferential, and in the public interest and addresses the directives in Order No. 822 by: 1. Clarifying the obligations pertaining to electronic access control for low impact BES Cyber Systems;[4] and 2. adopting mandatory security controls for transient electronic devices (*e.g.,* thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems) used at low impact BES Cyber Systems. In addition, by requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances for low impact BES Cyber Systems, the proposed Reliability Standard aligns the treatment of low impact BES Cyber Systems with that of high and medium impact BES Cyber Systems, which currently include a requirement for declaring and responding to CIP Exceptional Circumstances. Accordingly, we propose to approve proposed Reliability Standard CIP–003–7 because the proposed modifications improve the base-line cybersecurity posture of responsible entities compared to the current Commission-approved CIP Reliability Standards.

3. In addition, pursuant to FPA section 215(d)(5), the Commission proposes to direct NERC to develop certain modifications to the CIP Reliability Standards. As discussed below, while proposed Reliability Standard CIP–003–7 improves electronic access control for low impact BES Cyber Systems and enhances security controls for transient electronic

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

[2] *Revised Critical Infrastructure Protection Reliability Standards,* Order No. 822, 154 FERC ¶ 61,037, *reh'g denied,* Order No. 822–A, 156 FERC ¶ 61,052 (2016).

[3] *See* NERC Petition at 2.

[4] NERC defines ''BES Cyber System'' as one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

devices used at low impact BES Cyber Systems, we propose to direct that NERC modify Reliability Standard CIP–003–7 to: 1. Provide clear, objective criteria for electronic access controls for low impact BES Cyber Systems; and 2. address the need to mitigate the risk of malicious code that could result from third-party transient electronic devices. We believe that modifications addressing these two concerns will address potential gaps and improve the cyber security posture of responsible entities that must comply with the CIP standards.

I. Background

A. Section 215 and Mandatory Reliability Standards

4. 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.[5] Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[6] and subsequently certified NERC.[7]

B. Order No. 822

5. The Commission approved the ''Version 1'' CIP standards in January 2008, and subsequently acted on revised versions of the CIP standards.[8] On January 21, 2016, in Order No. 822, the Commission approved seven CIP Reliability Standards: CIP–003–6 (Security Management Controls), CIP–004–6 (Personnel and Training), CIP–006–6 (Physical Security of BES Cyber Systems), CIP–007–6 (Systems Security Management), CIP–009–6 (Recovery Plans for BES Cyber Systems), CIP–010–2 (Configuration Change Management and Vulnerability Assessments), and CIP–011–2 (Information Protection). The Commission determined that the Reliability Standards under consideration at that time were an improvement over the prior iteration of the CIP Reliability Standards and addressed the directives in Order No. 791 by, among other things, addressing in an equally effective and efficient manner the need for a NERC Glossary definition for the term ''communication networks'' and providing controls to address the risks posed by transient electronic devices (*e.g.,* thumb drives and laptop computers) used at high and medium impact BES Cyber Systems.[9]

6. In addition, in Order No. 822, pursuant to section 215(d)(5) of the FPA, the Commission directed NERC, *inter alia,* to: 1. Develop modifications to the LERC definition to eliminate ambiguity surrounding the term ''direct'' as it is used in the LERC definition; and 2. develop modifications to the CIP Reliability Standards to provide mandatory protection for transient electronic devices used at low impact BES Cyber Systems.[10]

C. NERC Petition

7. On March 3, 2017, NERC submitted a petition seeking approval of Reliability Standard CIP–003–7 and the associated violation risk factors and violation severity levels, implementation plan and effective dates. NERC states that proposed Reliability Standard CIP–003–7 satisfies the criteria set forth in Order No. 672 that the Commission applies when reviewing a proposed Reliability Standard.[11] NERC also sought approval of revisions to NERC Glossary definitions for the terms Removable Media and Transient Cyber Asset, as well as the retirement of the NERC Glossary definitions of LERC and LEAP. In addition, NERC proposed the retirement of Commission-approved Reliability Standard CIP–003–6.

8. NERC states that proposed Reliability Standard CIP–003–7 improves upon the existing protections that apply to low impact BES Cyber Systems. NERC avers that the proposed modifications address the Commission's directives from Order No. 822 by: 1. Clarifying electronic access control requirements applicable to low impact BES Cyber Systems; and 2. adding requirements for the protection of transient electronic devices used for low impact BES Cyber Systems. In addition, while not required by Order No. 822, NERC proposes a CIP Exceptional Circumstances policy for low impact BES Cyber Systems.

9. In response to the Commission's directive to develop modifications to eliminate ambiguity surrounding the term ''direct'' as it is used in the LERC definition, NERC proposes to: 1. Retire the terms LERC and LEAP from the NERC Glossary; and 2. modify Section 3 of Attachment 1 to proposed Reliability Standard CIP–003–7 ''to more clearly delineate the circumstances under which Responsible Entities must establish access controls for low impact BES Cyber Systems.'' [12] NERC states that the proposed revisions are designed to simplify the electronic access control requirements associated with low impact BES Cyber Systems in order to avoid ambiguities associated with the term ''direct.'' NERC explains that it recognized the ''added layer of unnecessary complexity'' introduced by distinguishing between ''direct'' and ''indirect'' access within the LERC definition and asserts that the proposed revisions will ''help ensure that Responsible Entities implement the required security controls effectively.'' [13]

10. With regard to the Commission's directive to develop modifications to the CIP Reliability Standards to provide mandatory protection for transient electronic devices used at low impact BES Cyber Systems, NERC proposes to add a new section to Attachment 1 to proposed Reliability Standard CIP–003–7 to require responsible entities to include controls in their cyber security plans to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems that could result from the use of ''Transient Cyber Assets or Removable Media.'' Specifically, proposed Section 5 of Attachment 1 lists controls to be applied to Transient Cyber Assets and Removable Media that NERC contends ''will provide enhanced protections against the propagation of malware from transient devices.'' [14]

11. NERC also proposes a modification that was not directed by the Commission in Order No. 822. Namely, NERC proposes revisions in Requirement R1 of proposed Reliability Standard CIP–003–7 to require responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems.[15] NERC

[5] 16 U.S.C. 824o(e) (2012).

[6] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards,* Order No. 672, FERC Stats. & Regs. ¶ 31,204, *order on reh'g,* Order No. 672–A, FERC Stats. & Regs. ¶ 31,212 (2006).

[7] *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).

[8] *Mandatory Reliability Standards for Critical Infrastructure Protection,* Order No. 706, 122 FERC ¶ 61,040, *order on reh'g,* Order No. 706–A, 123 FERC ¶ 61,174 (2008), *order on clarification,* Order No. 706–B, 126 FERC ¶ 61,229 (2009), *order on clarification,* Order No. 706–C, 127 FERC ¶ 61,273 (2009).

[9] Order No. 822, 154 FERC ¶ 61,037 at P 17; *see also Version 5 Critical Infrastructure Protection Reliability Standards,* Order No. 791, 78 FR 72755 (Dec. 3, 2013), 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g,* Order No. 791–A, 146 FERC ¶ 61,188 (2014).

[10] Order No. 822, 154 FERC ¶ 61,037 at P 18.

[11] *See* NERC Petition at 2 (citing Order No. 672, FERC Stats. & Regs. ¶ 31,204 at PP 262, 321–337); *id.* at Exhibit D (Order No. 672 Criteria).

[12] *Id.* at 16.

[13] *Id.* at 16.

[14] *Id.* at 26–27.

[15] A CIP Exceptional Circumstance is defined in the NERC Glossary as a situation that involves or threatens to involve one or more of the following,

states that a number of requirements in the existing CIP Reliability Standards specify that responsible entities do not have to implement or continue implementing these requirements during a CIP Exceptional Circumstance in order to avoid hindering the entities' ability to timely and effectively respond to the CIP Exceptional Circumstance. NERC explains that since the proposed requirements relating to transient electronic devices used at low impact BES Cyber Systems include an exception for CIP Exceptional Circumstances, NERC is proposing to add a requirement for responsible entities to have a CIP Exceptional Circumstances policy that applies to low impact BES Cyber Systems, as it already requires for high and medium impact BES Cyber Systems.[16]

12. NERC requests that proposed Reliability Standard CIP–003–7 and the revised definitions of Transient Cyber Asset and Removable Media become effective the first day of the first calendar quarter that is eighteen months after the effective date of the Commission's order approving the proposed Reliability Standard.

II. Discussion

13. Pursuant to section 215(d)(2) of the FPA, we propose to approve Reliability Standard CIP–003–7 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. Proposed Reliability Standard CIP–003–7 largely addresses the Commission's directives in Order No. 822 and is an improvement over the current Commission-approved CIP Reliability Standards. Specifically, the modifications to Section 3 of Attachment 1 to Reliability Standard CIP–003–7 clarify the obligations pertaining to electronic access control for low impact BES Cyber Systems. In addition, the modifications to Attachment 1 to Reliability Standard CIP–003–7 require mandatory security controls for transient electronic devices used at low impact BES Cyber Systems. We also propose to approve the new provision in Reliability Standard CIP–003–7, Requirement R1 requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems. While Order No. 822 did not direct NERC to expand the scope of the CIP Exceptional Circumstances policy, the revision aligns the treatment of low impact BES Cyber Systems with that of high and medium impact BES Cyber Systems if and when a CIP Exceptional Circumstance occurs.

14. We also propose to approve the revisions to the NERC Glossary definitions of Transient Cyber Asset and Removable Media, as well as the retirement of the NERC Glossary definitions for LERC and LEAP since the proposed modifications to Reliability Standard CIP–003–7 obviate the need for the two terms. We further propose to approve the violation risk factor and violation severity level assignments associated with proposed Reliability Standard CIP–003–7 as well as NERC's proposed implementation plan and effective dates.

15. In addition, as discussed below, pursuant to section 215(d)(5) of the FPA, the Commission proposes to direct NERC to develop certain modifications to the CIP Reliability Standards. While proposed Reliability Standard CIP–003–7 improves electronic access control for low impact BES Cyber Systems and enhances security controls for transient electronic devices used at low impact BES Cyber Systems, we propose to direct that NERC modify Reliability Standard CIP–003–7 to: 1. Provide clear, objective criteria for electronic access controls for low impact BES Cyber Systems; and 2. address the need to mitigate the risk of malicious code that could result from third-party transient electronic devices.

16. Below, we discuss the following issues: A. Electronic access controls for low impact BES Cyber Systems; B. protection of transient electronic devices; C. proposed retirement and modification of definitions; D. NERC's proposed implementation plan and effective dates; and E. proposed violation severity level and violation risk factor assignments.

A. Electronic Access Controls for Low Impact BES Cyber Systems Order No. 822

17. In Order No. 822, the Commission directed NERC to modify the LERC definition to eliminate ambiguity surrounding the term ''direct'' as it is used in the LERC definition.[17] The Commission explained that the directive was intended to codify the clarification provided in NERC's NOPR comments, in which NERC referenced a statement in the Guidelines and Technical Basis section of Reliability Standard CIP–003–6 that electronic access controls must be applied to low impact BES Cyber Systems unless responsible entities implement a ''complete security break'' between the external host (cyber asset) and any cyber asset(s) that may be used to pass communications to the low impact BES Cyber System.[18] The Commission observed that ''a suitable means to address our concern is to modify the [LERC] definition consistent with the commentary in the Guidelines and Technical Basis section of CIP–003–6.'' [19]

18. In addition, the Commission explained that the directive was also intended to eliminate a loophole that would have allowed transitive connections to out-of-scope cyber assets (*e.g.,* serial devices) to go unprotected under the LERC definition.[20]

NERC Petition

19. In its Petition, NERC proposes to: 1. Retire the terms LERC and LEAP from the NERC Glossary; and 2. modify Section 3 of Attachment 1 to Reliability Standard CIP–003–7 ''to more clearly delineate the circumstances under which Responsible Entities must establish access controls for low impact BES Cyber Systems.'' [21] NERC states that the proposed revisions are designed to simplify the electronic access control requirements associated with low impact BES Cyber Systems in order to avoid ambiguities associated with the term ''direct.'' NERC states further that it recognized the ''added layer of unnecessary complexity'' introduced by distinguishing between ''direct'' and ''indirect'' access within the LERC definition and asserts that the proposed revisions will ''help ensure that Responsible Entities implement the required security controls effectively.'' [22]

20. NERC states that proposed Reliability Standard CIP–003–7 would require responsible entities to implement electronic access controls for any communication, direct or indirect (*i.e.,* communications through an intermediary device where no direct connection is present), between a low

or similar, conditions that impact safety or bulk electric system reliability: A risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability. Glossary of Terms Used in NERC Reliability Standards (August 1, 2017), *http://www.nerc.com/files/glossary_of_terms.pdf.*

[16] NERC Petition at 31–32.

[17] Order No. 822, 154 FERC ¶ 61,037 at P 73.

[18] *Id.* (citing NERC NOPR Comments at 31).

[19] *Id.*

[20] *Id.* (''NERC's clarification on this issue resolves many of the concerns raised by EnergySec, APS, and SPP RE regarding the proposed definition, as a complete security break would not appear to permit transitive connections through one or more out of scope cyber assets to go unprotected under the definition, and would appear to require the assets to maintain 'separate conversations' as suggested by SPP RE.'').

[21] NERC Petition at 16.

[22] *Id.*

impact BES Cyber System and an outside Cyber Asset that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System. NERC asserts that the proposed revisions to Section 3 of Attachment 1 to proposed Reliability Standard CIP–003–7 improve the clarity of the electronic access requirements and focus responsible entities ''on the security objective of controlling electronic access to permit only necessary inbound and outbound electronic access to low impact BES Cyber Systems.'' [23]

21. NERC explains that Section 3.1 of Attachment 1 to proposed Reliability Standard CIP–003–7 is composed of three basic elements: 1. Identifying routable protocol communications from outside the asset containing the low impact BES Cyber System; 2. determining necessary inbound and outbound electronic access; and 3. implementing electronic access controls to permit only necessary inbound and outbound electronic access to the low impact BES Cyber System.

22. With regard to the first element, NERC states that Section 3.1 of Attachment 1 defines the circumstances where communications require electronic access controls. The three characteristics are:

1. The communication is between the low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber System(s);

2. the communication uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

3. the communication is not used for time-sensitive protection or control functions between intelligent electronic devices.

NERC states further that each of the three characteristics were included in the original LERC definition.[24]

23. NERC asserts that the first characteristic helps to properly focus the electronic access controls in light of ''the wide array of low impact BES Cyber Systems and the risk-based approach to protecting different types of BES Cyber Systems.'' [25] NERC explains that, whether a ''Responsible Entity uses a logical border as a demarcation point or some other understanding of what is inside or outside the asset, [the responsible entity] would have to provide a reasonable justification for its determination.'' [26] On the second characteristic, NERC states that routable communications present increased risks to the security of BES Cyber Systems and require additional protections. Therefore, communications with a low impact BES Cyber System involving routable connections require protections to address the risk of uncontrolled communications. With regard to the third characteristic, NERC explains that the exclusion of communications for time-sensitive protection and control functions is intended to avoid precluding the functionality of time-sensitive reliability enhancing functions. NERC states, however, that an entity invoking this exclusion may have to demonstrate that applying electronic access controls would introduce latency that would negatively impact functionality.[27]

24. According to NERC, the second characteristic of Section 3.1 of Attachment 1 provides that responsible entities may permit only necessary inbound and outbound electronic access to low impact BES Cyber Systems as determined by the responsible entity. NERC explains that Section 3.1 does not specify a bright line as to what constitutes ''necessary inbound and outbound access'' due to ''the wide array of assets containing low impact BES Cyber Systems and the myriad of reasons a Responsible Entity may need to allow electronic access to and from a low impact BES Cyber Systems.'' [28] NERC maintains that responsible entities ''have the flexibility to identify the necessary electronic access to meet their business and operational needs.'' [29]

25. NERC explains that ''a Responsible Entity must document the necessity of its inbound and outbound electronic access permissions and provide justification of the need for such access'' in order to demonstrate compliance with Section 3.1 of Attachment 1.[30] NERC states that absent a documented, reasonable justification, the ERO may find that the responsible entity was not in compliance with Section 3.1. NERC asserts that the purpose of the phrase ''as determined by the Responsible Entity'' in Section 3.1 is to indicate that the determination whether electronic access is necessary is to be made in the first instance by the responsible entity based on the facts and circumstances of each case. NERC states further that that the phrase ''as determined by the Responsible Entity'' does not limit the ERO's ability to engage in effective compliance oversight. Specifically, NERC contends that the ERO has the authority to review the documented justification for permitting electronic access and to determine whether it represents a reasonable exercise of discretion in light of the overall reliability objective.[31]

26. In support of its position, NERC cites the draft Reliability Standard Audit Worksheet (RSAW) for proposed Reliability Standard CIP–003–7, which provides the following language in the Note to Auditor section for Requirement R2:

> The entity must document its determination as to what is necessary inbound and outbound electronic access and provide justification of the business need for such access. Once this determination has been made and documented, the audit team's professional judgment cannot override the determination made by the Responsible Entity.[32]

NERC also provides a list of Commission-approved CIP Reliability Standards where the phrase ''as determined by the Responsible Entity'' or similar language is used. NERC states that in all circumstances where the phrase ''as determined by the Responsible Entity'' or similar language is used, ''the ERO has the authority to evaluate the reasonableness of the Responsible Entity's determination when assessing compliance to ensure it is consistent with the reliability objective of the requirement. To interpret this language otherwise would be inconsistent with NERC's statutory obligation to engage in meaningful compliance oversight . . .'' [33]

Commission Proposal

27. The Commission proposes to approve Reliability Standard CIP–003–7 because, as discussed above, the proposed Reliability Standard largely addresses the directives in Order No. 822 and is an improvement over the current Commission-approved CIP Reliability Standards. However, NERC's proposed revisions to Reliability Standard CIP–003–7 regarding the LERC

[23] *Id.* at 17.

[24] *Id.* at 18.

[25] *Id.* at 19.

[26] *Id.*

[27] *Id.* at 20.

[28] *Id.* at 21–22.

[29] *Id.* at 22.

[30] *Id.*

[31] *Id.* at 22–23.

[32] *Id.* at 22, n.42.

[33] *Id.* at 23–24. NERC also indicates, *id* at n.42, that Footnote 1 of the draft RSAW states that ''[w]hile the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in the RSAW, to determine compliance with the Reliability Standard.'' Draft RSAW, *http://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/RSAW_CIP-003-7(i)_v2_Clean_01202017.pdf.*

directive and electronic access controls for low impact BES Cyber Systems raise certain issues. In Order No. 822, the Commission directed NERC to develop modifications to the LERC definition to eliminate ambiguity surrounding the term ''direct'' as it is used in the definition. The directive was based on the concern that responsible entities could avoid adopting adequate electronic access protections for low impact BES Cyber Systems by simply installing a device, such as a laptop or protocol converter, in front of the BES Cyber System to ''break'' the direct routable connection. As the Commission noted in Order No. 822, the desired clarification could have been made by including the security concepts from the Guidelines and Technical Basis section of Reliability Standard CIP–003–6 in the definition.[34] Instead, NERC's proposal comprehensively revises a responsible entity's obligations under Requirement R2 through the revisions to Attachment 1 by deleting the term LERC and giving responsible entities significantly more deference in determining how they construct the electronic access protections for low impact BES Cyber Systems.

28. We are concerned that the proposed revisions may not provide adequate electronic access controls for low impact BES Cyber Systems. Specifically, proposed Reliability Standard CIP–003–7 does not provide clear, objective criteria or measures to assess compliance by independently confirming that the access control strategy adopted by a responsible entity would reasonably meet the security objective of permitting only ''necessary inbound and outbound electronic access'' to its low impact BES Cyber Systems.

29. Section 3.1 of Attachment 1 to proposed Reliability Standard CIP–003–7 does not appear to contain clear criteria or objective measures to determine whether the electronic access control strategy chosen by the responsible entity would be effective for a given low impact BES Cyber System to permit only necessary inbound and outbound connections. In order to ensure an objective and consistently-applied requirement, the electronic access control plan required in Attachment 1 should require the responsible entity to articulate its access control strategy for a particular set of low impact BES Cyber Systems and provide a technical rationale rooted in security principles explaining how that strategy will reasonably restrict electronic access. Attachment 1 should also outline basic security principles in order to provide clear, objective criteria or measures to assist in assessing compliance. Without such a requirement, auditors will not necessarily have adequate information to assess the reasonableness of the responsible entity's decision with respect to how the responsible entity identified necessary communications or restricted electronic access to specific low impact BES Cyber Systems. And absent such information, it is possible that an auditor could assess a violation where an entity adequately protected its low impact BES Cyber Systems or fail to recognize a situation where additional protections are necessary to meet the security objective of the standard.

30. As the Commission stated in Order No. 672, there ''should be a clear criterion or measure of whether an entity is in compliance with a proposed Reliability Standard. It should contain or be accompanied by an objective measure of compliance so that it can be enforced and so that enforcement can be applied in a consistent and non-preferential manner.'' [35] The Commission reiterated this point in Order No. 791, stating that ''the absence of objective criteria to evaluate the controls chosen by responsible entities for Low Impact assets introduces an unacceptable level of ambiguity and potential inconsistency into the compliance process, and creates an unnecessary gap in reliability.'' [36] The Commission also observed that ''ambiguity will make it difficult for registered entities to develop, and NERC and the regions to objectively evaluate, the effectiveness of procedures developed to implement'' the Reliability Standard.[37]

31. As a possible model, the electronic access control requirements that are applied to medium and high impact BES Cyber systems provide a number of criteria that can be used to assess the sufficiency of a responsible entity's electronic access control strategy. For medium and high impact BES Cyber Systems, auditors use the following criteria to review whether the access control strategy is reasonable: 1. Whether the electronic access was granted through an authorized and monitored electronic access point (Reliability Standard CIP–005–5, Requirement R1); 2. whether the electronic access granted to individuals/devices was evaluated based on need (Reliability Standard CIP–005–5, Requirement R1.3); 3. whether the entity has mechanisms to enforce authentication of users with electronic access (Reliability Standard CIP–007–6, Requirement R5); and 4. whether the responsible entity routinely uses strong passwords and manages password changes (Reliability Standard CIP–007–6, Requirement R5). Absent similar criteria in the low impact electronic access control plan that are appropriately tailored to the risks posed by low impact BES Cyber Systems, responsible entities may adopt electronic access controls that do not meet the overarching security objective of restricting inbound and outbound electronic access.

32. Therefore, pursuant to section 215(d)(5) of the FPA, we propose to direct NERC to develop modifications to Reliability Standard CIP–003–7 to provide clear, objective criteria for electronic access controls for low impact BES Cyber Systems consistent with the above discussion. The Commission seeks comment on this proposal.

B. Protection of Transient Electronic Devices

Order No. 822

33. In Order No. 822, the Commission directed NERC to develop modifications to provide mandatory protection for transient electronic devices used at low impact BES Cyber Systems based on the risk posed to bulk electric system reliability. The Commission stated that such modifications ''will provide an important enhancement to the security posture of the bulk electric system by reinforcing the defense-in-depth nature of the CIP Reliability Standards at *all* impact levels.'' [38] The Commission also stated that the proposed modifications should be designed to effectively address the risks posed by transient electronic devices used at low impact BES Cyber Systems ''in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards.'' [39]

NERC Petition

34. In its Petition, NERC proposes to add a new section to Attachment 1 to proposed Reliability Standard CIP–003–7 to require responsible entities to include controls in their cyber security plans to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems through the

[34] *See* Order No. 822, 154 FERC ¶ 61,037 at P 73.

[35] *Rules Concerning Certification of the Electric Reliability Organization and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards,* Order No. 672, FERC Stats. & Regs. ¶ 31,204, at P 327 (2006).

[36] Order No. 791, 145 FERC ¶ 61,160 at P 108.

[37] *Id.*

[38] Order No. 822, 154 FERC ¶ 61,037 at P 32 (emphasis in original).

[39] *Id.*

use of ''Transient Cyber Assets or Removable Media.'' Specifically, proposed Section 5 of Attachment 1 lists controls to be applied to Transient Cyber Assets and Removable Media that NERC states ''will provide enhanced protections against the propagation of malware from transient devices.'' [40]

35. NERC states that the language in proposed Section 5 to Attachment 1 parallels the language in Attachment 1 to Reliability Standard CIP–010–2, which addresses mitigation of the risks of the introduction of malicious code to high and medium impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. NERC states further that, as in Reliability Standard CIP–010–2, proposed Section 5 distinguishes between Transient Cyber Assets managed by a responsible entity and those managed by a third-party; the distinction arising because of a responsible entity's lack of control over Transient Cyber Assets managed by a third-party. NERC explains that the proposed controls for Removable Media do not distinguish between the responsible entity-managed assets and third-party managed assets due to the functionality of Removable Media. NERC provides the example of a thumb drive that can be scanned prior to use regardless of which party manages the asset.[41]

36. NERC explains that proposed Section 5 of Attachment 1 requires responsible entities to meet the security objectives ''by implementing the controls that the Responsible Entity determines necessary to meet its affirmative obligation to mitigate the risks of the introduction of malicious code.'' [42] NERC states that the approach reflected in Section 5 provides the flexibility to implement the controls that best suit the needs and characteristics of a responsible entity's organization. NERC explains further that ''the Responsible Entity must demonstrate that its selected controls were designed to meet the security objective to mitigate the risk of the introduction of malicious code.'' [43]

37. NERC outlines certain distinctions between proposed Section 5 of Attachment 1 to proposed Reliability Standard CIP–003–7 and Attachment 1 to Reliability Standard CIP–010–2. Specifically, NERC states that proposed Section 5 does not include requirements relating to authorization or software vulnerabilities, as are contained in Attachment 1 to Reliability Standard CIP–010–2. NERC explains that this difference is consistent with the risk-based approach of the CIP Reliability Standards and ''the underlying principle of concentrating limited industry resources on protecting those BES Cyber Systems with greater risk to the BES.'' NERC states that Section 5 focuses on the risk associated with the introduction of malicious code.[44]

38. In addition, NERC states that proposed Section 5 to Attachment 1 does not include language requiring a responsible entity to determine whether additional mitigation actions are necessary where a third party manages a Transient Cyber Asset, nor does it include language requiring a responsible entity to implement additional mitigation actions in such situations. NERC states that it nonetheless expects ''that if another party's processes and practices for protecting its Transient Cyber Assets do not provide reasonable assurance that they are designed to effectively meet the security objective of mitigating the introduction of malicious code, the Responsible Entity must take additional steps to meet the stated objective.'' [45] NERC explains that if a third party's practices and policies do not provide reasonable assurance that the Transient Cyber Assets would be protected from malicious code, ''simply reviewing those policies and procedures without taking other steps to mitigate the risks of introduction of malicious code may not constitute compliance.'' [46]

Commission Proposal

39. NERC's proposed modifications in Reliability Standard CIP–003–7, Requirement R2, Attachment 1, Section 5 that include malware detection and prevention controls for responsible entity-managed Transient Cyber Assets and Removable Media should improve the cybersecurity posture of responsibility entities compared to currently-effective Reliability Standard CIP–003–6. The revisions in Section 5.2, however, do not address one aspect of the reliability gap identified in Order No. 822 regarding low impact BES Cyber Systems. Specifically, as noted above, proposed Reliability Standard CIP–003–7 does not explicitly require mitigation of the introduction of malicious code from third-party managed Transient Cyber Assets, even if the responsible entity determines that the third-party's policies and procedures are inadequate.[47] While the proposed Reliability Standard does not explicitly require mitigation of the introduction of malicious code from third-party managed Transient Cyber Assets, NERC states that the failure to mitigate this risk ''may not constitute compliance.'' [48] NERC's statement suggests that, with regard to low impact BES Cyber Systems, the proposed requirement lacks an obligation for a responsible entity to correct any deficiencies that are discovered during a review of third-party Transient Cyber Asset management practices. Indeed, the parallel provision for high and medium impact BES Cyber Systems specifies that ''Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.'' [49] Yet, such language obligating mitigation action is not proposed for low impact BES Cyber Assets.

40. The proposed Reliability Standard may, therefore, contain a reliability gap where a responsible entity contracts with a third-party but fails to mitigate potential deficiencies discovered in the third-party's malicious code detection and prevention practices prior to a Transient Cyber Asset being connected to a low impact BES Cyber System. That is because the proposed Reliability Standard does not contain: 1. A requirement for the responsible entity to mitigate any malicious code found during the third-party review(s); or 2. a requirement that the responsible entity take reasonable steps to mitigate the risks of third party malicious code on their systems, if an arrangement cannot be made for the third-party to do so. Without these obligations, we are concerned that responsible entities could, without compliance consequences, simply accept the risk of deficient third-party transient electronic device management practices.[50] Moreover, the requirement to ''review'' methods used by third-parties to detect and prevent malware may fail to convey the necessary next steps that a responsible entity should take.[51]

[40] *Id.* at 26–27.

[41] *Id.* at 28.

[42] *Id.*

[43] *Id.* at 29.

[44] NERC Petition at 29.

[45] *Id.* at 29–30.

[46] *Id.* at 30.

[47] *See* NERC Petition at 29–30.

[48] *Id.* at 30.

[49] Reliability Standard CIP–010–2 (Cyber Security—Configuration Change Management and Vulnerability Assessments), Requirement R4, Attachment 1, Section 2.3. In contrast, the obligations to ''review'' methods used by third-parties to detect and prevent malware are similar for lower, medium and high impact BES Cyber Assets. *Cf.* CIP–010–2, Attachment 1, Sections 2.1 and 2.2; and proposed CIP–010–3, Attachment 1, Section 3.2.

[50] *See* Order No. 706, 122 FERC ¶ 61,040 at P 150 (rejecting the concept of acceptance of risk in the CIP Reliability Standards).

[51] *See* Order No. 791, 145 FERC ¶ 61,160 at P 108.

41. Therefore, pursuant to section 215(d)(5) of the FPA, we propose to direct that NERC develop modifications to proposed Reliability Standard CIP–003–7 to address the need to mitigate the risk of malicious code that could result from third-party Transient Cyber Assets consistent with the above discussion. The Commission seeks comment on this proposal.

C. Proposed NERC Glossary Definitions

42. Proposed Reliability Standard CIP–003–7 includes two revised definitions for inclusion in the NERC Glossary. Specifically, NERC proposes to revise the definitions of Transient Cyber Asset and Removable Media in order to accommodate the use of the terms at all impact levels. NERC explains that the original definitions include references to concepts or requirements associated only with high and medium impact BES Cyber Systems and the definitions were modified to avoid confusion because protections for Transient Electronic Devices will now be extended to low impact BES Cyber Systems.[52]

43. In addition, NERC proposes to retire the definitions of LERC and LEAP. NERC states that the proposed retirement of the NERC Glossary terms LERC and LEAP accords with the proposed modifications to Section 3 of Attachment 1 to proposed Reliability Standard CIP–003–7 and is intended to simplify the electronic access control requirements for low impact BES Cyber Systems by avoiding the ambiguities associated with the term ''direct.'' NERC explains further that it ''recognized that distinguishing between 'direct' and 'indirect' electronic access within the LERC definition added a layer of unnecessary complexity.'' [53]

44. We propose to approve the revised definitions of Transient Cyber Asset and Removable Media, as well as the retirement of the definitions of LERC and LEAP.

D. Implementation Plan and Effective Dates

45. NERC requests an effective date for proposed Reliability Standard CIP–003–7 and the revised definitions of Transient Cyber Asset and Removable Media on the first day of the first calendar quarter that is eighteen months after the effective date of the Commission's order approving the proposed Reliability Standard. NERC explains that the proposed implementation plan does not alter the previously-approved compliance dates for Reliability Standard CIP–003–6 other than the compliance date for Reliability Standard CIP–003–6, Requirement R2, Attachment 1, Sections 2 and 3, which would be replaced with the effective date for proposed Reliability Standard CIP–003–7. NERC also proposes that the retirement of Reliability Standard CIP–003–6 and the associated definitions become effective on the effective date of proposed Reliability Standard CIP–003–7.[54]

46. We propose to approve NERC's implementation plan for proposed Reliability Standard CIP–003–7, as described above.

E. Violation Risk Factor/Violation Severity Level Assignments

47. NERC requests approval of two violation risk factors and violation severity levels assigned to proposed Reliability Standard CIP–003–7. Specifically, NERC requests approval of violation risk factor and violation severity level assignments associated with Requirements R1 and R2 of Reliability Standard CIP–003–7.[55] We propose to accept these violation risk factors and violation severity levels.

III. Information Collection Statement

48. The FERC–725B information collection requirements contained in this proposed rule are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.[56] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[57] 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 any suggested methods for minimizing respondents' burden, including the use of automated information techniques.

49. The Commission bases its paperwork burden estimates on the changes in paperwork burden presented by the proposed revision to CIP Reliability Standard CIP–003–7 as compared to the current Commission-approved Reliability Standard CIP–003–6. The Commission has already addressed the burden of implementing Reliability Standard CIP–003–6.[58] As discussed above, the immediate rulemaking addresses three areas of modification to the CIP Reliability Standards: 1. Clarifying the obligations pertaining to electronic access control for low impact BES Cyber Systems; 2. adopting mandatory security controls for transient electronic devices (*e.g.,* thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems) used at low impact BES Cyber Systems; and 3. requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems.

50. The NERC Compliance Registry, as of September 2017, identifies approximately 1,320 U.S. entities that are subject to mandatory compliance with Reliability Standards. Of this total, we estimate that 1,100 entities will face an increased paperwork burden under proposed Reliability Standard CIP 003–7, estimating that a majority of these entities will have one or more low impact BES Cyber Systems. Based on these assumptions, we estimate the following reporting burden:

[52] NERC Petition at 30.

[53] *Id.* at 16.

[54] *Id.,* Exhibit C (Implementation Plan).

[55] *Id.,* Exhibit F (Analysis of Violation Risk Factors and Violation Severity Levels).

[56] 44 U.S.C. 3507(d) (2012).

[57] 5 CFR 1320.11 (2017).

[58] *See* Order No. 822, 154 FERC ¶ 61,037 at PP 84–88.

RM17–11–000 NOPR

[Mandatory Reliability Standards for Critical Infrastructure Protection Reliability Standards]

	Number of respondents (1)	Annual number of responses per respondent (2)	Total number of responses (1) * (2) = (3)	Average burden & cost per response [59] (4)	Total annual burden hours & total annual cost (3) * (4) = (5)	Cost per respondent ($) (5) ÷ (1)
Create low impact TCA assets plan (one-time) [60] ...	1,100	1	1,100	20 hrs.; $1,680	6,875 hrs.; $1,848,000 ...	$1,680
Updates and reviews of low impact TCA assets (ongoing) [61].	1,100	[62] 300	330,000	1.5 hrs. [63]; $126	495,000 hrs.; $41,580,000.	37,800
Update/modify documentation to remove LERC and LEAP (one-time) [60].	1,100	1	1,100	20 hrs.; $1,680	6,875 hrs.; $1,848,000 ...	1,680
Update paperwork for access control implementation in Section 2 [64] and Section 3 [65] (ongoing) [61].	1,100	1	1,100	20 hrs.; $1,680	6,875 hrs.; $1,848,000 ...	1,680
Total (one-time) [60]	.....	.....	2,200	.....	13,750 hrs.; $3,696,000	.....
Total (ongoing) [61]	.....	.....	331,100	.....	501,875 hrs.; $43,428,000.	.....

51. The following shows the annual cost burden for each group, based on the burden hours in the table above:

- Year 1: $3,696,000.
- Years 2 and 3: $43,428,000.
- The paperwork burden estimate includes costs associated with the initial development of a policy to address requirements relating to: 1. Clarifying the obligations pertaining to electronic access control for low impact BES Cyber Systems; 2. adopting mandatory security controls for transient electronic devices (*e.g.,* thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems) used at low impact BES Cyber Systems; and 3. requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems. Further, the estimate reflects the assumption that costs incurred in year 1 will pertain to policy development, while costs in years 2 and 3 will reflect the burden associated with maintaining logs and other records to demonstrate ongoing compliance.

52. *Title:* Mandatory Reliability Standards, Revised Critical Infrastructure Protection Reliability Standards

Action: Proposed Collection FERC–725B.

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 proposed rule 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 revised CIP Reliability Standard CIP–003–7 pursuant to section 215(d)(2) of the FPA because it improves upon the currently-effective suite of cyber security CIP Reliability Standards.

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

53. 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, email: *DataClearance@ferc.gov,* phone: (202) 502–8663, fax: (202) 273–0873].

54. For submitting comments concerning the collection(s) of information and the associated burden estimate(s), please send your comments to the Commission, and to the Office of Management and Budget, Office of Information and Regulatory Affairs, Washington, DC 20503 [Attention: Desk Officer for the Federal Energy Regulatory Commission, phone: (202) 395–4638, fax: (202) 395–7285]. For security reasons, comments to OMB should be submitted by email to: *oira_submission@omb.eop.gov.* Comments submitted to OMB should include Docket Number RM17–11–000 and OMB Control Number 1902–0248.

IV. Regulatory Flexibility Act Analysis

55. 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.[66] The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.[67] 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).[68] Proposed Reliability Standard CIP–003–7 is expected to impose an additional burden on 1,100 entities [69] (reliability coordinators, generator operators, generator owners, interchange coordinators or authorities, transmission operators, balancing authorities,

[59] The loaded hourly wage figure (includes benefits) is based on the average of three occupational categories for 2016 found on the Bureau of Labor Statistics Web site (*http://www.bls.gov/oes/current/naics2_22.htm):*

Legal (Occupation Code: 23–0000): $143.68.

Electrical Engineer (Occupation Code: 17–2071): $68.12.

Office and Administrative Support (Occupation Code: 43–0000): $40.89 ($143.68 + $68.12 + $40.89) ÷ 3 = $84.23. The figure is rounded to $84.00 for use in calculating wage figures in this NOPR.

[60] This one-time burden applies in Year One only.

[61] This ongoing burden applies in Year 2 and beyond.

[62] We estimate that each entity will perform 25 updates per month. 25 updates *12 months = 300 updates (*i.e.* responses) per year.

[63] The 1.5 hours of burden per response is comprised of three sub-categories:

Updates to managed low TCA assets: 15 minutes (0.25 hours) per response.

Updates to unmanaged low TCA assets: 60 minutes (1 hour) per response.

Reviews of low TCA applicable controls: 15 minutes (0.25 hours) per response.

[64] Physical Security Controls.

[65] Electronic Access Controls.

[66] 5 U.S.C. 601–12 (2012).

[67] 13 CFR 121.101 (2017).

[68] SBA Final Rule on ''Small Business Size Standards: Utilities,'' 78 FR 77343 (Dec. 23, 2013).

[69] Public utilities may fall under one of several different categories, each with a size threshold based on the company's number of employees, including affiliates, the parent company, and subsidiaries. For the analysis in this NOPR, we are using a 500 employee threshold due to each affected entity falling within the role of Electric Bulk Power Transmission and Control (NAISC Code: 221121).

transmission owners, and certain distribution providers).

56. Of the 1,100 affected entities discussed above, we estimate that approximately 857 or 78 percent [70] of the affected entities are small. As discussed above, proposed Reliability Standard CIP–003–7 enhances reliability by providing criteria against which NERC and the Commission can evaluate the sufficiency of an entity's electronic access controls for low impact BES Cyber systems, as well as improved security controls for transient electronic devices (*e.g.,* thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems). We estimate that each of the 857 small entities to whom the proposed modifications to Reliability Standard CIP–003–7 applies will incur one-time costs of approximately $3,360 per entity to implement this standard, as well as the ongoing paperwork burden reflected in the Information Collection Statement (approximately $39,480 per year per entity). We do not consider the estimated costs for these 857 small entities to be a significant economic impact.

57. Based on the above analysis, we propose to certify that the proposed Reliability Standard will not have a significant economic impact on a substantial number of small entities.

V. Environmental Analysis

58. 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.[71] 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.[72] The actions proposed herein fall within this categorical exclusion in the Commission's regulations.

VI. Comment Procedures

59. 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 December 26, 2017. Comments must refer to Docket No. RM17–11–000, and must include the commenter's name, the organization they represent, if applicable, and address.

60. 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.

61. 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.

62. 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

63. 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.

64. 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.

65. User assistance is available for eLibrary and the Commission's Web site during normal business hours from the Commission's Online Support at 202–502–6652 (toll free at 1–866–208–3676) or email at *ferconlinesupport@ferc.gov,* or the Public Reference Room at (202) 502–8371, TTY (202) 502–8659. Email the Public Reference Room at *public.referenceroom@ferc.gov.*

By direction of the Commission.

Issued October 19, 2017.

Nathaniel J. Davis, Sr.,

Deputy Secretary.

[FR Doc. 2017–23287 Filed 10–25–17; 8:45 am]

BILLING CODE 6717–01–P

[70] 77.95 percent.

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

[72] 18 CFR 380.4(a)(2)(ii) (2017).

DEPARTMENT OF THE TREASURY

Internal Revenue Service

26 CFR Part 1

[REG–134247–16]

RIN 1545–BN73

Revision of Regulations Under Chapter 3 Regarding Withholding of Tax on Certain U.S. Source Income Paid to Foreign Persons; Correction

AGENCY: Internal Revenue Service (IRS), Treasury.

ACTION: Notice of proposed rulemaking; correction.

SUMMARY: This document corrects a correction to a notice of proposed rulemaking (REG–134247–16) that was published in the **Federal Register** on Friday, September 15, 2017. The notice of proposed rulemaking, published on January 6, 2017, under section 1441 of the Internal Revenue Code of 1986 (Code), relates to withholding of tax on certain U.S. source income paid to foreign persons and requirements for certain claims for refund or credit of income tax made by foreign persons.

DATES: The correction published on September 15, 2017 (82 FR 43314), is corrected as of October 26, 2017 and is applicable beginning January 6, 2017.

FOR FURTHER INFORMATION CONTACT: Kamela Nelan at (202) 317- 6942 (not a toll-free number).

SUPPLEMENTARY INFORMATION:

Background

The notice of proposed rulemaking (REG–134247–16) that is the subject of this correction is under section 1441 of the Code.

Need for Correction

As published, the notice of proposed rulemaking (REG–134247–16) contains an error which may prove to be misleading and needs to be corrected.

Correction of Publication

Accordingly, the notice of proposed rulemaking published at 82 FR 43314, September 15, 2017, is corrected as follows:

On page 43314, in the third column, under the heading ''Correction of Publication'', in the fourth line, the