154 FERC ¶ 61,037
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM15-14-000]

Revised Critical Infrastructure Protection Reliability Standards

(Issued January 21, 2016)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule.

SUMMARY: The Federal Energy Regulatory Commission (Commission) approves seven critical infrastructure protection (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 proposed Reliability Standards address the cyber security of the bulk electric system and improve upon the current Commission-approved CIP Reliability Standards. In addition, the Commission directs NERC to develop certain modifications to improve the CIP Reliability Standards.

DATES: This rule will become effective **[INSERT DATE 65 days after publication in the FEDERAL REGISTER].**

FOR FURTHER INFORMATION CONTACT:

Daniel Phillips (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6387
daniel.phillips@ferc.gov

Simon Slobodnik (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6707
simon.slobodnik@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:

154 FERC ¶ 61,037
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Norman C. Bay, Chairman;
Cheryl A. LaFleur, Tony Clark,
and Colette D. Honorable.

Revised Critical Infrastructure Protection Reliability Standards — Docket No. RM15-14-000

ORDER NO. 822

FINAL RULE

(Issued January 21, 2016)

1. Pursuant to section 215 of the Federal Power Act (FPA),[1] the Commission approves seven critical infrastructure protection (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) (proposed CIP Reliability Standards). The North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), submitted the seven proposed CIP Reliability Standards in response

[1] 16 U.S.C. 824o.

to Order No. 791.[2] The Commission also approves NERC's implementation plan and violation risk factor and violation severity level assignments. In addition, the Commission approves NERC's new or revised definitions for inclusion in the NERC Glossary of Terms Used in Reliability Standards (NERC Glossary), subject to modification. Further, the Commission approves the retirement of Reliability Standards CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, and CIP-011-1.

2. The proposed CIP Reliability Standards are 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-Power System.[3] As discussed below, the Commission finds that the proposed CIP Reliability Standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest, and address the directives in Order No. 791 by: (1) eliminating the "identify, assess, and correct" language in 17 of the CIP version 5 Standard requirements; (2) providing enhanced security controls for Low Impact assets; (3) 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; and (4) addressing in an equally effective and efficient manner the need for a NERC Glossary definition for the term "communication

[2] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

[3] *See* NERC Petition at 3.

networks." Accordingly, the Commission approves the proposed CIP Reliability Standards because they improve the base-line cybersecurity posture of applicable entities compared to the current Commission-approved CIP Reliability Standards.

3. In addition, pursuant to FPA section 215(d)(5), the Commission directs NERC to develop certain modifications to improve the CIP Reliability Standards. First, NERC is directed to develop modifications to address the protection of transient electronic devices used at Low Impact BES Cyber Systems. As discussed below, the modifications developed by NERC should be designed to effectively address, in an appropriately tailored manner, the risks posed by transient electronic devices to Low Impact BES Cyber Systems. Second, the Commission directs NERC to develop modifications to CIP-006-6 to require protections for communication network components and data communicated between all bulk electric system Control Centers according to the risk posed to the bulk electric system. With regard to the questions raised in the Notice of Proposed Rulemaking (NOPR) concerning the potential need for additional remote access controls, NERC must conduct a comprehensive study that identifies the strength of the CIP version 5 remote access controls, the risks posed by remote access-related threats and vulnerabilities, and appropriate mitigating controls.[4] Third, the Commission directs

[4] *Revised Critical Infrastructure Protection Reliability Standards*, Notice of Proposed Rulemaking, 80 Fed. Reg. 43,354 (July 22, 2015), 152 FERC ¶ 61,054, at 60 (2015).

NERC to develop modifications to its definition for Low Impact External Routable Connectivity, as discussed in detail below.

4. The Commission, in the NOPR, also proposed to direct that NERC develop requirements relating to supply chain management for industrial control system hardware, software, and services.[5] After review of comments on this topic, the Commission scheduled a staff-led technical conference for January 28, 2016, in order to facilitate a structured dialogue on supply chain risk management issues identified by the NOPR. Accordingly, this Final Rule does not address supply chain risk management issues. Rather, the Commission will determine the appropriate action on this issue after the scheduled technical conference.

I. Background

A. Section 215 and Mandatory Reliability Standards

5. Section 215 of the FPA requires a Commission-certified ERO to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval. Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[6] Pursuant to section 215 of the FPA, the

[5] *Id.* P 66.

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

Commission established a process to select and certify an ERO,[7] and subsequently certified NERC.[8]

B. Order No. 791

6. On November 22, 2013, in Order No. 791, the Commission approved the CIP version 5 Standards (Reliability Standards CIP-002-5 through CIP-009-5, and CIP-010-1 and CIP-011-1).[9] The Commission determined that the CIP version 5 Standards improve the CIP Reliability Standards because, *inter alia*, they include a revised BES Cyber Asset categorization methodology that incorporates mandatory protections for all High, Medium, and Low Impact BES Cyber Assets, and because several new security controls should improve the security posture of responsible entities.[10] In addition, pursuant to section 215(d)(5) of the FPA, the Commission directed NERC to: (1) remove the "identify, assess, and correct" language in 17 of the CIP Standard requirements; (2) develop enhanced security controls for Low Impact assets; (3) develop controls to protect transient electronic devices; (4) create a NERC Glossary definition for the term

[7] *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).

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

[9] Order No. 791, 145 FERC ¶ 61,160 at P 41.

[10] *Id.*

"communication networks;" and (5) develop new or modified Reliability Standards to protect the nonprogrammable components of communications networks.

7. The Commission also directed NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition and submit an informational filing within one year.[11] On February 3, 2015, NERC submitted an informational filing assessing the results of a survey conducted to identify the scope of assets subject to the definition of the term BES Cyber Asset as it is applied in the CIP version 5 Standards.

8. Finally, Order No. 791 directed Commission staff to convene a technical conference to examine the technical issues concerning communication security, remote access, and the National Institute of Standards and Technology (NIST) Risk Management Framework.[12] On April 29, 2014, a staff-led technical conference was held pursuant to the Commission's directive. The topics discussed at the technical conference included: (1) the adequacy of the approved CIP version 5 Standards' protections for bulk electric system data being transmitted over data networks; (2) whether additional security controls are needed to protect bulk electric system communications networks, including remote systems access; and (3) the functional differences between the respective methods utilized for the identification, categorization, and specification of appropriate levels of

[11] *Id.* PP 76, 108, 136, 150.

[12] *Id.* P 225.

protection for cyber assets using the CIP version 5 Standards as compared with those employed within the NIST Cybersecurity Framework.

C. NERC Petition

9. On February 13, 2015, NERC submitted a petition seeking approval of Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2, as well as an implementation plan,[13] associated violation risk factor and violation severity level assignments, proposed new or revised definitions,[14] and retirement of Reliability Standards CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, and CIP-011-1.[15] NERC states that the proposed Reliability Standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest because they satisfy the factors set forth in Order No. 672 that the Commission applies when reviewing a proposed Reliability Standard.[16] NERC maintains that the

[13] The proposed implementation plan is designed to match the effective dates of the proposed Reliability Standards with the effective dates of the prior versions of those Reliability Standards under the implementation plan for the CIP version 5 Standards.

[14] The six new or revised definitions proposed for inclusion in the NERC Glossary are: (1) BES Cyber Asset; (2) Protected Cyber Asset; (3) Low Impact Electronic Access Point; (4) Low Impact External Routable Connectivity; (5) Removable Media; and (6) Transient Cyber Asset.

[15] The proposed Reliability Standards are available on the Commission's eLibrary document retrieval system in Docket No. RM15-14-000 and on the NERC website, www.nerc.com.

[16] *See* NERC Petition at 13 and Exhibit C (citing Order No. 672, FERC Stats. & Regs. ¶ 31,204 at PP 323-335).

proposed Reliability Standards "improve the cybersecurity protections required by the CIP Reliability Standards[.]"[17]

10. NERC avers that the proposed CIP Reliability Standards satisfy the Commission directives in Order No. 791. Specifically, NERC states that the proposed Reliability Standards remove the "identify, assess, and correct" language, which represents the Commission's preferred approach to addressing the underlying directive.[18] In addition, NERC states that the proposed Reliability Standards address the Commission's directive regarding a lack of specific controls or objective criteria for Low Impact BES Cyber Systems by requiring responsible entities "to implement cybersecurity plans for assets containing Low Impact BES Cyber Systems to meet specific security objectives relating to: (i) cybersecurity awareness; (ii) physical security controls; (iii) electronic access controls; and (iv) Cyber Security Incident response."[19]

11. With regard to the Commission's directive that NERC develop specific controls to protect transient electronic devices, NERC explains that the proposed Reliability Standards require responsible entities "to implement controls to protect transient devices connected to their high impact and medium impact BES Cyber Systems and associated [Protected Cyber Assets]."[20] In addition, NERC states that the proposed Reliability

[17] NERC Petition at 4.

[18] *Id.* at 4, 15.

[19] *Id.* at 5.

[20] *Id.* at 6.

Standards address the protection of communication networks "by requiring entities to implement security controls for nonprogrammable components of communication networks at Control Centers with high or medium impact BES Cyber Systems."[21] Finally, NERC explains that it has not proposed a definition of the term "communication network" because the term is not used in the CIP Reliability Standards. Additionally, NERC states that "any proposed definition would need to be sufficiently broad to encompass all components in a communication network as they exist now and in the future."[22] NERC concludes that the proposed Reliability Standards "meet the ultimate security objective of protecting communication networks (both programmable and nonprogrammable communication network components)."[23]

12. Accordingly, NERC requests that the Commission approve the proposed Reliability Standards, the proposed implementation plan, the associated violation risk factor and violation severity level assignments, and the proposed new and revised definitions. NERC requests an effective date for the Reliability Standards of the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the effective date of the Commission's order approving the proposed Reliability Standards, although NERC proposes that responsible entities will not have to comply with the

[21] *Id.* at 8.

[22] *Id.* at 51-52.

[23] *Id.* at 52.

requirements applicable to Low Impact BES Cyber Systems (CIP-003-6, Requirement R1, Part 1.2 and Requirement R2) until April 1, 2017.

D. Notice of Proposed Rulemaking

13. On July 16, 2015, the Commission issued a NOPR proposing to approve Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2 and CIP-011-2 as just, reasonable, not unduly discriminatory or preferential, and in the public interest.[24] The NOPR stated that the proposed CIP Reliability Standards appear to improve upon the current Commission-approved CIP Reliability Standards and to address the directives in Order No. 791.

14. While proposing to approve the proposed Reliability Standards, the Commission also proposed to direct that NERC modify certain proposed standards or provide additional information supporting its proposal. First, the Commission directed NERC to provide additional information supporting the proposed limitation in Reliability Standard CIP-010-2 to transient electronic devices used at High and Medium Impact BES Cyber Systems. Second, the Commission stated that, while proposed CIP-006-6 would require protections for communication networks among a limited group of bulk electric system Control Centers, the proposed standard does not provide protections for communication network components and data communicated between all bulk electric system Control Centers. Therefore, the Commission proposed to direct that NERC develop

[24] NOPR, 152 FERC ¶ 61,054 (2015).

modifications to Reliability Standard CIP-006-6 to require physical or logical protections for communication network components between all bulk electric system Control Centers. Third, while the Commission proposed to approve the new or revised definitions for inclusion in the NERC Glossary, it sought comment on the proposed definition for Low Impact External Routable Connectivity. The Commission noted that, depending on the comments received, it may direct NERC to develop modifications to this definition to eliminate possible ambiguities and ensure that BES Cyber Assets receive adequate protection.

15. In addition, the Commission raised a concern that changes in the bulk electric system cyber threat landscape, identified through recent malware campaigns targeting supply chain vendors, have highlighted a gap in the protections under the CIP Reliability Standards. Therefore, the Commission proposed to direct NERC to develop a new Reliability Standard or modified Reliability Standard to provide security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations.[25]

16. In response to the NOPR, 41 entities submitted comments. A list of commenters appears in Appendix A. The comments have informed our decision making in this Final Rule.

[25] *Id.* P 18.

II. Discussion

17. Pursuant to section 215(d)(2) of the FPA, we approve Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2 and CIP-011-2 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. We find that the proposed Reliability Standards address the Commission's directives from Order No. 791 and are an improvement over the current Commission-approved CIP Reliability Standards. Specifically, the CIP Reliability Standards improve upon the existing standards by removing the "identify, assess, and correct" language and addressing the protection of Low Impact BES Cyber Systems. With regard to the directive to create a NERC Glossary definition for the term "communication networks," we approve NERC's proposal as an equally effective and efficient method to achieve the reliability goal underlying that directive in Order No. 791. We also approve NERC's proposed implementation plan, and violation risk factor and violation severity level assignments. Finally, we approve NERC's proposed new or revised definitions for inclusion in the NERC Glossary, subject to certain modifications, discussed below.

18. In addition, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop modifications to the CIP Reliability Standards to address our concerns regarding: (1) the need for mandatory protection for transient electronic devices used at Low Impact BES Cyber Systems in a manner that effectively addresses, and is appropriately tailored to address, the risk posed by those assets; and (2) the need for mandatory protection for communication links and data communicated between bulk electric system Control Centers in a manner that reflects the risks posed to bulk electric system reliability.

In addition, we direct NERC to modify the definition of Low Impact External Routable Connectivity in order to eliminate ambiguities in the language. Finally, we direct NERC to complete a study of the remote access protections in the CIP Reliability Standards within one year of the implementation of the CIP version 5 Standards for High and Medium Impact BES Cyber Systems.

19. As noted above, in the NOPR, the Commission proposed to direct that NERC develop requirements on the subject of supply chain management for industrial control system hardware, software, and services. After review of comments on the subject, the Commission scheduled a staff-led technical conference for January 28, 2016. The Commission will determine the appropriate action on this issue after the scheduled technical conference.

20. Below, we discuss the following matters: (A) protection of transient electronic devices; (B) protection of bulk electric system communication networks; (C) proposed definitions; and (D) NERC's implementation plan.

A. Protection of Transient Electronic Devices

NERC Petition

21. In its Petition, NERC states that the revised CIP Reliability Standards satisfy the Commission's directive in Order No. 791 by requiring that applicable entities: (1) develop plans and implement cybersecurity controls to protect Transient Cyber Assets and Removable Media associated with their High Impact and Medium Impact BES Cyber Systems and associated Protected Cyber Assets; and (2) train their personnel on the risks associated with using Transient Cyber Assets and Removable Media. NERC states that

the purpose of the proposed revisions is to prevent unauthorized access to and use of transient electronic devices, mitigate the risk of vulnerabilities associated with unpatched software on transient electronic devices, and mitigate the risk of the introduction of malicious code on transient electronic devices. NERC explains that the standard drafting team determined that the proposed requirements should only apply to transient electronic devices associated with High and Medium Impact BES Cyber Systems, concluding that "the application of the proposed transient devices requirements to transient devices associated with low impact BES Cyber Systems was unnecessary, and likely counterproductive, given the risks low impact BES Cyber Systems present to the Bulk Electric System."[26]

22. NERC further explains that the controls required under Attachment 1 to CIP-010-2, Requirement R4 address the following areas: (1) protections for Transient Cyber Assets managed by responsible entities; (2) protections for Transient Cyber Assets managed by another party; and (3) protections for Removable Media. NERC indicates that these provisions reflect the standard drafting team's recognition that the security controls required for a particular transient electronic device must account for the functionality of that device and whether the responsible entity or a third party manages the device. NERC also states that Transient Cyber Assets and Removable Media have

[26] NERC Petition at 34-35.

different capabilities because they present different levels of risk to the bulk electric system.[27]

NOPR

23. In the NOPR, the Commission stated that proposed Reliability Standard CIP-010-2 appears to provide a satisfactory level of security for transient electronic devices used at High and Medium Impact BES Cyber Systems. The Commission noted that the proposed security controls required under proposed CIP-010-2, Requirement R4, taken together, constitute a reasonable approach to address the reliability objectives outlined by the Commission in Order No. 791. Specifically, the Commission stated that proposed security controls outlined in Attachment 1 should ensure that responsible entities apply multiple security controls to provide defense-in-depth protection to transient electronic devices in the High and Medium Impact BES Cyber System environments.[28]

24. The Commission raised a concern, however, that proposed CIP-010-2 does not provide adequate security controls to address the risks posed by transient electronic devices used at Low Impact BES Cyber Systems, including Low Impact Control Centers, due to the limited applicability of Requirement R4. The Commission stated that this omission may result in a gap in protection for Low Impact BES Cyber Systems where malware inserted at a single Low Impact substation could propagate through a network of many substations without encountering a single security control. The NOPR noted that

[27] *Id.* at 38.

[28] NOPR, 152 FERC ¶ 61,054 at P 41.

"Low Impact security controls do not provide for the use of mandatory anti-malware/antivirus protections within the Low Impact facilities, heightening the risk that malware or malicious code could propagate through these systems without being detected."[29]

25. The Commission also indicated that the burden of expanding the applicability of Reliability Standard CIP-010-2 to transient electronic devices at Low Impact BES Cyber Systems is not clear from the information in the record, nor is it clear what information and analysis led NERC to conclude that the application of the transient electronic device requirements to Low Impact BES Cyber Systems "was unnecessary." Therefore, the Commission directed NERC to provide additional information supporting the proposed limitation in Reliability Standard CIP-010-2 to High and Medium Impact BES Cyber Systems, stating that the Commission "may direct NERC to address the potential reliability gap by developing a solution, which could include modifying the applicability section of CIP-010-2, Requirement R4 to include Low Impact BES Cyber Systems, that effectively addresses, and is appropriately tailored to address, the risks posed by transient devices to Low Impact BES Cyber Systems."[30]

Comments

26. While two commenters support the Commission's proposal, most commenters, including NERC, advocate approval of CIP-010-2 without expanding the applicability

[29] *Id.* P 42.

[30] *Id.* P 43.

provision of Requirement R4 to include Low Impact BES Cyber Systems. NERC questions the Commission's assertion that "malware inserted via a USB flash drive at a single Low Impact substation could propagate through a network of many substations without encountering a single security control under NERC's proposal."[31] In particular, NERC and others commenters assert that the proposed security controls in CIP-003-6 adequately address the potential for propagation of malicious code or other unauthorized access by requiring: (1) all routable protocol communications between low impact assets be controlled through a Low Impact Electronic Access Point; (2) mandatory cyber security awareness activities; (3) physical security controls; (4) electronic access controls; and (5) incident response activities.[32] Trade Associations assert that all asset-to-asset routable communications must go through the security control of the Low Impact Electronic Access Point under the proposed controls, other than extremely time sensitive device-to-device coordination.[33] Trade Associations and NIPSCO suggest that the impact on reliability in the event of a successful compromise is inherently low.

27. NERC, Trade Associations, Arkansas, G&T Cooperatives, and ITC argue that any Commission proposal to expand the protections of CIP-010-2, Requirement R4 to transient electronic devices used at Low Impact BES Cyber Systems would contradict the underlying principles of the risk-based approach that was adopted in the Commission-

[31] NERC Comments at 26 (quoting NOPR, 152 FERC ¶ 61,054 at P 42).

[32] *Id*. at 27. *See also* Trade Associations Comments at 12; Southern Comments at 5-6; Luminant Comments at 2; G&T Cooperatives Comments at 7.

[33] Trade Associations Comments at 12.

approved CIP version 5 Standards. Likewise, these commenters argue that the resource burden to develop and implement security controls for low impact transient devices would be substantial. NERC, Consumers Energy, and G&T Cooperatives express concern that any requirements for transient electronic devices used at Low Impact BES Cyber Systems may divert resources from the protection of Medium and High Impact BES Cyber Systems.[34]

28. Trade Associations and Southern assert that developing security controls for low impact transient cyber assets would be difficult given that, under CIP-003-6, responsible entities are not required to identify Low Impact BES Cyber Assets. Trade Associations conclude that additional transient cyber asset protections would need to be at the asset level to avoid creating administrative burdens disproportionate to the risk. Arkansas and G&T Cooperatives claim that the Commission's proposal to modify CIP-010-2 could require the implementation of device level controls and assert that the cost for complying with such regulations would be unprecedented because they would be driven by the number of devices and the number of people interacting with those devices.[35]

29. ITC and NIPSCO state that the lack of specificity in CIP-010-2, Requirement R4 raises concerns with how responsible entities will demonstrate compliance, noting that the methods included are general and non-exclusive such that a responsible entity cannot

[34] NERC Comments at 24; Consumers Energy Comments at 3-4; G&T Cooperatives Comments at 5.

[35] Arkansas Comments at 2-3; G&T Cooperatives Comments at 5.

be expected to know with reasonable confidence whether its plan will be deemed compliant. ITC states that, if the Commission intends to approve Standards that contain such broad latitude, it must also be prepared to accept a wide variety of plans as compliant.

30. NERC requests that, should the Commission determine that the risk associated with transient electronic devices used at Low Impact BES Cyber Systems requires expanding protections to those devices, it should recognize the varying risk levels presented by Low Impact BES Cyber Systems and the need to focus on higher risk issues. Other commenters, including Arkansas, KCP&L, and G&T Cooperatives, request that the Commission allow the implementation of the low impact controls in CIP-003-6 and the transient device controls in CIP-10-2 before directing further initiatives to expand the scope of the standards. Reclamation suggests that, if the Commission decides to direct NERC to address this potential reliability gap, the transient device and removable media controls for Low Impact BES Cyber Systems should be less stringent than the controls in CIP-010-2 given the facilities with which they are associated. Luminant and Reclamation also request that any new requirements for low impact transient electronic devices be placed in CIP-003-6.

31. APS and SPP RE generally express support for changes to CIP-010-2, Requirement R4 to address mandatory protection for transient devices used at Low Impact BES Cyber Systems. APS states that extending transient device protection to low impact systems would likely afford some additional security benefits, but notes that there may be cases where these controls would be unduly burdensome. SPP RE states that the

burden of extending certain elements of the Attachment 1 requirements to environments containing Low Impact BES Cyber Systems is reasonable, with the benefit far outweighing the cost if the controls are carefully considered with risk and potential burden in mind. SPP RE suggests that the compliance burden could be reduced by allowing Transient Cyber Assets and Removable Media to be readily moved between assets containing only Low Impact BES Cyber Systems without having to re-perform the Attachment 1 requirements between sites. Finally, NIPSCO seeks clarification on how to determine the "manager" of a Transient Cyber Asset under CIP-010-2, Requirement R4, noting that the requirement appears to allow a Transient Cyber Asset to be owned by the responsible entity, but used by a vendor on a day-to-day basis.[36]

Commission Determination

32. After consideration of the comments received on this issue, we conclude that the adoption of controls for transient devices used at Low Impact BES Cyber Systems, including Low Impact Control Centers, 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. Accordingly, we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC

[36] NIPSCO Comments at 9-10.

has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards.

33. We are not persuaded by NERC and other commenters that the security controls in CIP-003-6 adequately address the potential for propagation of malicious code or other unauthorized access stemming from transient devices used at Low Impact BES Cyber Systems. CIP-003-6 requires responsible entities, for any Low Impact External Routable Connectivity, to implement a Low Impact Electronic Access Point to "permit only necessary inbound and outbound bi-directional routable protocol access." In doing so, however, responsible entities may not foresee and configure their devices to limit all unwanted traffic. Firewalls only accept or drop traffic as dictated by a preprogrammed rule set. In other words, if a piece of malicious code were to leverage permissible traffic or protocol patterns, the firewall could not detect a malicious file signature. In short, under this requirement of CIP-003-6, responsible entities have discretion to determine what access and traffic are necessary, which does not provide enough certainty that the protocols used or ports targeted by future, as-yet-unknown malware would result in the firewall rules dropping the malicious traffic.

34. Second, the firewalls and other security devices installed at Low Impact Electronic Access Points for Low Impact BES Cyber Systems may not be actively monitored. The system security management controls in CIP-007-6 that require logging, alerting, and event review are not mandated for low impact BES Cyber Systems under CIP-003-6. As

a result, even if a security device installed at a Low Impact Electronic Access Point successfully logged suspicious network traffic, there is no assurance that a responsible entity would have processes in place to take swift action to prevent malicious code from spreading to other Low Impact BES Cyber Systems.

35. In addition, we disagree with the assertion raised by some commenters that directing NERC to address the reliability gap created by the limited applicability of CIP-010-2 contradicts the risk-based approach adopted in the CIP version 5 Standards,[37] or will result in an unreasonable resource burden or diversion of resources from the protection of Medium and High Impact BES Cyber Systems. Rather, in the NOPR, the Commission noted that *one means* to address the identified reliability concern would be to modify the applicability section of CIP-010-2, Requirement R4 to include Low Impact BES Cyber Systems. This is not, however, the only means available to address the Commission's concerns. The Commission was clear that any proposal submitted by NERC should be designed to effectively address, in a manner that is "appropriately tailored to address, the risks posed by transient devices to Low Impact BES Cyber Systems."[38] We intend that NERC's proposed modifications will be designed to address the risk posed by the assets being protected in accordance with the risk-based approach reflected in the CIP version 5 Standards, i.e., the modifications to address Low Impact

[37] *See* NERC Comments at 24; G&T Cooperatives Comments at 6.

[38] NOPR, 152 FERC ¶ 61,054 at P 43.

BES Cyber Systems may be less stringent than the provisions that apply to Medium and High Impact Cyber Systems – commensurate with the risk.

36. We agree with the Trade Associations that controls for low impact transient cyber assets could be adopted at the asset level (i.e., facility or site-level) to avoid overly-burdensome administrative tasks that could be associated with identifying discrete Low Impact BES Cyber Assets.[39] While responsible entities are not explicitly required by the CIP standards to maintain a list of discrete Low Impact BES Cyber Assets, entities should be aware of where such assets reside in order to apply the existing protections already reflected in the policies required under CIP-003-6. As noted above, the Commission offered that one possible solution to address the reliability gap could be to modify the applicability section of CIP-010-2, Requirement R4. However, should modifying CIP-010-2 prove overly burdensome as asserted by Arkansas and G&T Cooperatives, NERC may propose an equally effective and efficient solution. For example, we believe it would be reasonable for NERC to consider modifications to CIP-003-6, as suggested by Luminant and Reclamation, since the existing low impact controls reside in that standard.

37. With respect to ITC and NIPSCO's comments regarding potential ambiguity in CIP-010-2, Requirement R4, we reiterate that CIP-010-2, Requirement R4 contains sufficiently clear control objectives to inform responsible entities about the activities that

[39] Trade Associations Comments at 13.

must be performed in order for a transient device program to be deemed compliant. We believe that the flexibility reflected in Requirement R4 will help responsible entities to develop secure and cost effective compliance solutions. To the extent that concerns arise in the implementation process, we encourage responsible entities to work with NERC and the Regional Entities to ensure that responsible entities will have reasonable confidence about compliance expectations. Finally, regarding NIPSCO's request for clarification, we clarify our understanding that the phrase "managed by" as it is used in CIP-010-2, Requirement R4, is intended to distinguish between situations where a responsible entity has complete control over a Transient Cyber Asset as opposed to situations where a third party shares some measure of control, as discussed in the Guidelines and Technical Basis section of CIP-010-2.

B. Protection of Bulk Electric System Communication Networks

NERC Petition

38. In its Petition, NERC states that the standard drafting team concluded that it need not create a new definition for communication networks because the term "is generally understood to encompass both programmable and nonprogrammable components (i.e., a communication network includes computer peripherals, terminals, and databases as well as communication mediums such as wires)."[40] According to NERC, the revised CIP Reliability Standards contain reasonable controls to secure the types of equipment and

[40] NERC Petition at 52 (citing *North American Electric Reliability Corp.*, 142 FERC ¶ 61,203, at PP 13-14 (2013)).

components that responsible entities must protect based on the risk they pose to the bulk electric system, as opposed to a specific definition of communication networks. Further, NERC explains that the standard drafting team focused on nonprogrammable communication components at control centers with High or Medium Impact BES Cyber Systems because those locations present a heightened risk to the Bulk-Power System, warranting the increased protections.[41]

39. NERC states that proposed Reliability Standard CIP-006-6 provides flexibility for responsible entities to implement the physical security measures that best suit their needs and to account for configurations where logical measures are necessary because the entity cannot effectively implement physical access restrictions. According to NERC, responsible entities have the discretion as to the type of physical or logical protections to implement pursuant to Part 1.10 of this Standard, provided that the protections are designed to meet the overall security objective.[42]

NOPR

40. In the NOPR, the Commission indicated that NERC's proposed alternative approach to addressing the Commission's Order No. 791 directive regarding the definition of communication networks adequately addresses part of the underlying concerns set forth in Order No. 791.[43] The Commission proposed to accept NERC's

[41] *Id.* at 48.

[42] *Id.* at 49-50.

[43] NOPR, 152 FERC ¶ 61,054 at P 53.

explanation that responsible entities must develop controls to secure the nonprogrammable components of communication networks based on the risk they pose to the bulk electric system, rather than develop a specific definition of communication networks to identify assets for protection.

41. However, the Commission also indicated that NERC's proposed solution for the protection of nonprogrammable components of communication networks does not fully meet the intent of the Commission's Order No. 791 directive, because proposed CIP-006-6, Requirement R1, Part 1.10 would only apply to nonprogrammable components of communication networks within the same Electronic Security Perimeter, excluding from protection other programmable and non-programmable communication network components that may exist outside of a discrete Electronic Security Perimeter.[44] Therefore, the Commission proposed to direct that NERC develop a modification to proposed Reliability Standard CIP-006-6 "to require responsible entities to implement controls to protect, at a minimum, all communication links and sensitive bulk electric system data communicated between all bulk electric system Control Centers," including communication between two (or more) Control Centers, but not between a Control Center and non-Control Center facilities such as substations.[45] In addition, the Commission sought comments that address "the value achieved if the CIP Standards were to require the incorporation of additional network segmentation controls, connection

[44] *Id.* P 55.

[45] *Id.* P 59.

monitoring, and session termination controls behind responsible entity intermediate systems," including whether these or other steps to improve remote access protection are needed, and whether the adoption of any additional security controls addressing this topic would provide substantial reliability and security benefits.[46]

Comments

42. NERC and a number of commenters generally agree that inter-Control Center communications play a critical role in maintaining bulk electric system reliability and do not oppose further evaluation of the risks described by the Commission in the NOPR.[47] NERC states that timely and accurate communication between Control Centers is important to maintaining situational awareness and reliable bulk electric system operations, and notes that the interception or manipulation of data communicated between Control Centers "could be used to carry out successful cyberattacks against the [bulk electric system]."[48]

43. However, NERC and other commenters also assert that NERC should take steps to ensure that reliability is not adversely impacted with the adoption of any additional controls.[49] SPP RE and EnergySec indicate that latency should not be a concern for protecting Control Center communications. Specifically, SPP RE states that the latency

[46] *Id.* P 60.

[47] NERC Comments at 20. *See also* Comments of IRC, IESO and ITC.

[48] NERC Comments at 20.

[49] NERC Comments at 20. *See also* Arkansas Comments at 3-4; APS Comments at 4; EnergySec Comments at 4; IESO Comments at 4.

introduced by encryption is typically not an operational issue for inter-Control Center communications, since regular inter-Control Center communications do not require the same millisecond response time as communications between protective relays in substations. In addition, SPP RE states that protections other than encryption are not as effective in protecting sensitive operational data from alteration or replay.

44. A number of commenters request that the Commission provide flexibility to the extent that it issues a directive on this topic. NERC, EnergySec, APS, and IESO state that the Commission should allow NERC the opportunity to develop an appropriate and risk informed approach to any new Reliability Standard or requirement, while APS and EnergySec also suggest that NERC be granted the flexibility to determine the placement of any new security controls in the body of standards.[50] Trade Associations and Arkansas state that NERC should determine the appropriate controls to implement to meet the Commission's objectives. Luminant, PNM Resources, and Southern suggest that any new standard or requirement should be results-based and not prescriptive, affording some measure of flexibility to responsible entities.

45. Trade Associations, Southern, Wisconsin, and NEI generally agree that protections should be applied to the High and Medium Impact BES Cyber System environment, but oppose extending mandatory protection to the Low Impact Control Center environment without additional study. Trade Associations and PNM also take issue with the blanket

[50] NERC Comments at 20-21; EnergySec Comments at 4; APS Comments at 4; IESO Comments at 4.

application of security controls over all bulk electric system Control Center data and believe that NERC should have the opportunity to determine what data is truly sensitive.

46. A number of commenters oppose the Commission's proposal to require responsible entities to implement controls to protect all communication links and sensitive bulk electric system data communicated between all bulk electric system Control Centers. NIPSCO and G&T Cooperatives argue that the risks posed by such communication networks do not justify the costs of implementing a new standard and, therefore, the standard should, at a minimum, not apply to Low Impact BES Cyber Systems. NIPSCO opines that the Commission's proposal may cause unintentional consequences since data and communications exchanged between Control Centers is often time-sensitive. SCE suggests that the Commission's proposal is premature and that the risks should be studied before taking further actions. Foundation opposes the Commission's proposal because it objects to the exclusion of secure connections to grid facilities other than Control Centers, stating that the Commission should do more to protect the grid.[51]

47. Other commenters request clarification of the Commission's proposal. KCP&L, PNM, UTC, TVA, Idaho Power, and NIPSCO seek clarification whether Control Centers owned by multiple, different registered entities would be included in the Commission's proposal. TVA asks whether the Commission's proposal is focused on protecting the

[51] Foundation Comments at 47-48.

data link or the data itself. UTC questions the nature of the reliability gap described in the NOPR given the protections in CIP-005-5 for inbound and outbound communications. In addition, APS and EnergySec seek clarification regarding the term "control center" in the context of adopting controls to protect reliability-related data. APS and EnergySec note that transmission owner SCADA systems do not meet the current definition of control centers despite the fact that these systems contain identical reliability data as the systems operated by reliability coordinators, balancing authorities, and transmission operators. As a result, APS and EnergySec ask that the Commission clarify what constitutes a "control center" for the purposes of communication security.[52] Finally, Idaho Power, KCP&L, and UTC seek clarification whether responsible entities would be held individually accountable for implementing the controls adopted under the CIP Standards when there may be overlapping responsibilities associated with the protection of inter-entity control center communication.[53] For example, Idaho Power opines that two neighboring responsible entities with control centers that communicate with each other should both be equally responsible for implementing the CIP Standards, but states that it is unclear how compliance would be measured.

48. PNM and NIPSCO suggest that, if the NOPR proposal is aimed at protecting intra-control center communications, the Commission should consider modifications to Reliability Standard EOP-008-1. TVA requests that the Commission consider removing

[52] *See* APS Comments at 4; EnergySec Comments at 3.

[53] Idaho Power Comments at 2; UTC Comments at 2; KCP&L Comments at 5.

the requirement for protecting "all communication links" and focus on the "sensitive bulk electric system data" moving between Control Centers. TVA states that physical and logical protections for communications network components between bulk electric system Control Centers should be limited to only essential communications networks.

49. With regard to the Commission's question on the potential need for additional remote access protections, NERC and a number of commenters argue that there are not enough data to conclude that the proposed controls for remote access will be ineffective and suggest that the Commission delay consideration of additional remote access protections until after the CIP version 5 remote access provisions are implemented.[54] NERC and IRC provide a list of the relevant controls applied to remote access systems as evidence that there are substantial controls already in place to address threats associated with remote access. APS and Arkansas assert that the current Standards and industry-developed guidance provide sufficient tools for securing interactive remote access and, thus, additional controls would not provide significant reliability or security benefits. TVA claims that the current requirement language is too prescriptive because it precludes a registered entity's usage of specific technologies due to prejudices against certain "architectures."[55]

[54] NERC Comments at 21-23. *See also* Trade Association Comments at 14; KCP&L Comments at 4; Southern Comments at 7; IRC Comments at 6.

[55] TVA Comments at 5.

50. Commenters supporting the development of additional remote access controls for the CIP Standards contend that the current suite of CIP Standards fails to adequately address specific threats and vulnerabilities. SPP RE and CyberArk note the lack of restrictions on what systems remote users can access after successfully logging on to the intermediate system.[56] CyberArk also asserts that there is a lack of protection for remote user credentials after successfully logging onto the intermediate system and a lack of controls to regulate encryption strength and key management. Waterfall states that the proposed controls lack methods to detect and prevent compromised endpoint devices, which, according to Waterfall and SPP RE, presents the opportunity for an attacker to access multiple remote sites from a compromised central site.

51. PNM agrees that some of the controls mentioned by panelists at the April 2014 FERC technical conference may improve reliability and security. However, PNM states that such controls may have only marginal benefits to reliability and security since the increased complexity of these steps would present problems with staff support for such systems.[57] AEP asserts that, while additional controls may enhance a defense-in-depth strategy, prescriptive requirements on intermediate systems may create a need for technical feasibility exceptions for situations where security could impede reliability.

[56] SPP RE Comments at 7-8; CyberArk Comments at 1-2.

[57] PNM Comments at 2.

Commission Determination

52. We adopt the NOPR proposal and find that NERC's alternative approach to addressing the Commission's Order No. 791 directive regarding the definition of communication networks adequately addresses part of the underlying concerns set forth in Order No. 791.[58] In accepting this alternative approach, we accept NERC's explanation that responsible entities must develop controls to secure the nonprogrammable components of communication networks at Control Centers with High or Medium Impact BES Cyber Systems.

53. As discussed in detail below, however, the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication 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).

[58] NOPR, 152 FERC ¶ 61,054 at P 53.

54. NERC and other commenters recognize that inter-Control Center communications play a critical role in maintaining bulk electric system reliability by, among other things, helping to maintain situational awareness and reliable bulk electric system operations through timely and accurate communication between Control Centers.[59] We agree with this assessment. In order for certain responsible entities such as reliability coordinators, balancing authorities, and transmission operators to adequately perform their reliability functions, their associated control centers must be capable of receiving and storing a variety of sensitive bulk electric system data from interconnected entities. Accordingly, we find that additional measures to protect both the integrity and availability of sensitive bulk electric system data are warranted.[60] We also understand that the attributes of the data managed by responsible entities could require different information protection controls.[61] For instance, certain types of reliability data will be sensitive to data manipulation type attacks, while other types of reliability data will be sensitive to

[59] NERC Comments at 20.

[60] Protecting the integrity of bulk electric system data involves maintaining and ensuring the accuracy and consistency of inter-Control Center communications. Protecting the availability of bulk electric system data involves ensuring that required data is available when needed for bulk electric system operations.

[61] Moreover, in order for certain responsible entities to adequately perform their Reliability Functions, the associated control centers must be capable of receiving and storing a variety of sensitive data as specified by the IRO and TOP Standards. For instance, pursuant to Reliability Standard TOP-003-3, Requirements R1, R3 and R5, a transmission operator must maintain a documented specification for data and distribute its data specification to entities that have data required by the transmission operator's Operational Planning Analyses, Real-time Monitoring and Real-time Assessments. Entities receiving a data specification must satisfy the obligation of the documented specification.

eavesdropping type attacks aimed at collecting operational information (such as line and equipment ratings and impedances). NERC should consider the differing attributes of bulk electric system data as it assesses the development of appropriate controls.

55. With regard to NERC's development of modifications responsive to our directive, we agree with NERC and other commenters that NERC should have flexibility in the manner in which it addresses the Commission's directive. Likewise, we find reasonable the principles outlined by NERC that protections for communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers: (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.[62]

56. We disagree with the assertion of NIPSCO and G&T Cooperatives that the risk posed by bulk electric system communication networks does not justify the costs of implementing controls. Communications between Control Centers over such networks are fundamental to the operations of the bulk electric system, and the record here does not persuade us that controls for such networks are not available at a reasonable cost (through

[62] *See* NERC Comments at 20-21.

encryption or otherwise). Nonetheless, we recognize 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. We expect NERC to develop controls that reflect the risk posed by the asset or data being protected, and that can be implemented in a reasonable manner. It is important to recognize that certain entities are already required to exchange necessary real-time and operational planning data through secured networks using a "mutually agreeable security protocol," regardless of the entity's size or impact level.[63] NERC's response to the directives in this Final Rule 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.

57. With regard to Foundation's argument that the Commission should do more to promote grid security by mandating secure communications between all facilities of the bulk electric system, such as substations, the record in the immediate proceeding does not support such a broad requirement at this time. However, if in the future it becomes evident that such action is warranted, the Commission may revisit this issue.

58. Several commenters sought clarification whether Control Centers owned by multiple registered entities would be included under the Commission's proposal. We clarify that the scope of the directed modifications apply to Control Center

[63] *See* Reliability Standards TOP-003-3, Requirement R5 and IRO-010-2, Requirement R3.

communications from facilities at all impact levels, regardless of ownership. The directed modification should encompass communication links and data for intra-Control Center and inter-Control Center communications.

59. Idaho Power, KCP&L, and UTC seek clarification whether entities would be held individually accountable for implementing the Standard when there may be overlapping responsibilities. We clarify that responsible entities may be held individually accountable depending upon the security arrangements with their neighbors and functional partners. Many organizations currently use joint and coordinated functional registration agreements to assign accountability for reliability tasks with joint functional obligations.[64] These mechanisms could be leveraged to address responsibilities under the CIP Standards. For example, if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system.

60. UTC seeks further explanation regarding the nature of the reliability gap described in the NOPR given the protections in CIP-005-5 for inbound and outbound communications. We clarify that the reliability gap addressed in this Final Rule pertains to the lack of mandatory security controls to address how responsible entities should protect sensitive bulk electric system communications and data. As noted above, while

[64] *See* NERC Compliance Public Bulletin #2010-004, available on the NERC website at www.NERC.com.

responsible entities are required to exchange real-time and operational planning data necessary to operate the bulk electric system using mutually agreeable security protocols, there is no technical specification for how this transfer of information should incorporate mandatory security controls. Although the CIP Standards provide a measure of defense-in-depth for responsible entity information systems, the current security controls primarily focus on boundary protection controls. For instance, CIP-005-5 focuses on access control and malicious code prevention, which requires authentication of the user and ensuring that no malware is included in the communication, but does not provide for security of the actual data while it is being transmitted between Electronic Security Perimeters. Thus, the current CIP Reliability Standards do not adequately address how to protect the transfer of sensitive bulk electric system data between facilities at discrete geographic locations.

61. With respect to APS and EnergySec's request for clarification regarding the meaning of the term "control center" in the context of adopting controls to protect reliability-related data, we clarify that we are using here the NERC Glossary definition of a Control Center.[65] Whether particular facilities meet or do not meet this definition

[65] The NERC Glossary defines Control Center as "One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations."

should be determined outside of this rulemaking. However, the proposed modification will apply to Control Centers at all impact levels (high, medium, or low).

62. Several commenters addressed encryption and latency. Based on the record in this proceeding, it is reasonable to conclude that any lag in communication speed resulting from implementation of protections should only be measureable on the order of milliseconds and, therefore, will not adversely impact Control Center communications. Several commenters raise possible technical implementation difficulties with integrating encryption technologies into their current communications networks. Such technical issues should be considered by the standard drafting team when developing modifications in response to this directive, and may be resolved, e.g., by making certain aspects of the revised CIP Standards eligible for Technical Feasibility Exceptions.

63. We reject the suggestion of two commenters that any efforts to protect intra-Control Center communications should be considered through modifications in Reliability Standard EOP-008-1. As an initial matter, Reliability Standard EOP-008-1 focuses on backup functionality in the event that primary control center functionality is lost.[66] Reliability Standard EOP-008-1 also does not provide security for communication links or data and, therefore, does not provide for the protection of communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers.

[66] *See* http://www.nerc.com/files/eop-008-1.pdf.

64. Finally, with regard to the NOPR discussion regarding the potential need for additional protections related to remote access,[67] we are persuaded by commenters' suggestions that it would be prudent to assess the extent to which the CIP version 5 Standards provide effective controls for remote access before pursuing additional revisions to the CIP Standards.[68] Therefore, we direct NERC to conduct a study that assesses the effectiveness of the CIP version 5 remote access controls, the risks posed by remote access-related threats and vulnerabilities, and appropriate mitigating controls for any identified risks. NERC should consult with Commission staff to determine the general contents of the directed report. We direct NERC to submit a report on the above-outlined study within one year of the implementation of the CIP version 5 Standards for High and Medium Impact BES Cyber Systems.

C. Proposed Definitions

NERC Petition

65. In its Petition, NERC proposes the following definition for Low Impact External Routable Connectivity:

> Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bidirectional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between

[67] *See* NOPR, 152 FERC ¶ 61,054 at P 60.

[68] *See* NERC Comments at 21-23; Trade Association Comments at 14; KCP&L Comments at 4; Southern Comments at 7; IRC Comments at 6.

> Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).[69]

66. NERC explains that the proposed definition describes the scenarios where responsible entities are required to apply Low Impact access controls under Reliability Standard CIP-003-6, Requirement R2 to their Low Impact assets. Specifically, if Low Impact External Routable Connectivity is used, a responsible entity must implement a Low Impact Electronic Access Point to permit only necessary inbound and outbound bidirectional routable protocol access.[70]

NOPR

67. In the NOPR, the Commission sought comment on the proposed definition for Low Impact External Routable Connectivity. First, the Commission sought comment on the purpose of the meaning of the term "direct" in relation to the phrases "direct user-initiated interactive access" and "direct device-to-device connection" within the proposed definition.[71] In addition, the Commission sought comment on the implementation of the "layer 7 application layer break" contained in certain reference diagrams in the Guidelines and Technical Basis section of proposed Reliability Standard CIP-003-6, noting that the guidance provided in the Guidelines and Technical Basis section of the

[69] NERC Petition at 28.

[70] *Id*. at 29.

[71] *See* NOPR, 152 FERC ¶ 61,054 at P 70.

proposed standard may conflict with the plain reading of the term "direct."[72] The Commission noted a concern that a conflict in the reading of the term "direct" could lead to complications in the implementation of the proposed CIP Reliability Standards, hindering the adoption of effective security controls for Low Impact BES Cyber Systems. The Commission indicated that, depending upon the responses received, the final rule may direct NERC to develop a modification to the definition of Low Impact External Routable Connectivity to eliminate ambiguities.

Comments

68. NERC and other commenters do not oppose a modification of the Low Impact External Routable Connectivity definition, so long as it remains consistent with the Guidelines and Technical Basis for section for CIP-003-6.[73] NERC, referencing the Guidelines and Technical Basis section of proposed CIP-003-6, explains that the purpose of the term "direct" is to distinguish between the scenarios where an external user or device could electronically access the Low Impact BES Cyber System without a security break (i.e., direct access) from those situations where an external user or device could

[72] *See* CIP-003-6 Guidelines and Technical Basis Section, Reference Model 6 at p. 39. The layer 7 application layer break concept appears to permit a responsible entity to log into an intermediate application or device to access the Low Impact BES Cyber System or device to avoid implementing Low Impact Electronic Access Point security controls under CIP-003-6, Attachment 1, Section 3.

[73] NERC Comments at 31. *See also* Trade Associations Comments at 15; Southern Comments at 8.

only access the Low Impact BES Cyber System following a security break (i.e., indirect access).

69. NERC explains further that Low Impact External Routable Connectivity would exist and a Low Impact Electronic Access Point would be required if an entity's implementation of a layer 7 application layer break does not provide a sufficient security break (*i.e.*, the layer 7 application does not prevent direct access to the Low Impact BES Cyber System).[74] Southern states that it believes that the Low Impact External Routable Connectivity definition, when combined with the language in the Guidelines and Technical Basis section for CIP-003-6, is sufficiently clear.

70. SPP RE, EnergySec, and APS recommend that the Commission direct NERC to revise the Low Impact External Routable Connectivity definition because the definition, as drafted, would permit transitive connections through out of scope cyber assets at sites containing Low Impact BES Cyber Systems with no required security controls.[75] SPP RE posits that indirect access, through an intervening or intermediate system such as the non-BES Cyber Asset on the same network segment, should also be considered Low Impact External Routable Connectivity because this kind of access would enable "pivot attacks" on low impact networks.

71. SPP RE, EnergySec, TVA, and APS assert that any electronic remote access into a routable network containing BES Cyber Systems should be construed as External

[74] NERC Comments at 30.

[75] SPP RE Comments at 14-18; EnergySec Comments at 2-3; APS Comments at 7.

Routable Connectivity and protected.[76] SPP RE suggests that the layer 7 application layer break language is not well understood by industry, as some responsible entities currently hold the view that a security gateway appliance effectively serves as the layer 7 protocol break eliminating Low Impact External Routable Connectivity. SPP RE asserts that the security gateway appliance acting in this way does not maintain two independent conversations and, as a result, should still be considered as externally routable connected.

72. ITC states that it considers the layer 7 application layer break referenced in Model 6 of the Guidelines and Technical Basis section to be an illustrative example that in no way requires integrity of the data stream down to layer 7 for compliance with CIP-003-6.[77] ITC notes that the illustrative example referenced by the Commission is contained within the non-binding Guidelines and Technical basis section, and does not believe that the controlling language of CIP-003-6 requires such a control.

Commission Determination

73. Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition.

[76] SPP RE Comments at 14-18; EnergySec Comments at 2-3; TVA Comments at 1-2; APS Comments at 7.

[77] ITC Comments at 10-11.

Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.[78]

74. As discussed above, NERC clarifies that the purpose of the "direct" language in the Low Impact External Routable Connectivity definition is to distinguish between scenarios where an external user or device could electronically access a Low Impact BES Cyber System without a security break (direct access) from those situations where an external user or device could only access a Low Impact BES Cyber System following a security break (indirect access); therefore, in order for there to be no Low Impact External Routable Connectivity, the security break must be "complete" (i.e., it must prevent allowing access to the Low Impact BES Cyber Systems from the external cyber asset). 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.

[78] *E.g.*, NERC Comments at 31; Trade Associations Comments at 15.

75. We decline to adopt the recommendations from EnergySec and APS that the Commission direct NERC to modify the standards to utilize the concept of Electronic Security Perimeters for low impact systems and to leverage existing definitions for Electronic Access Point and External Routable Connectivity. The Commission believes that the electronic security protections developed by the standard drafting team for Low Impact BES Cyber Systems will provide sufficient protection to these systems with the modifications that we are directing to the Low Impact External Routable Connectivity definition. However, we may revisit this decision in the future if we determine that CIP-003-6, Requirement R2 and the Low Impact External Routable Connectivity definition provide insufficient electronic access protection for Low Impact BES Cyber Systems.

D. Implementation Plan

NERC Petition

76. In its Petition, NERC explains that the proposed implementation plan for the revised CIP Reliability Standards is designed to match the effective dates of the proposed Reliability Standards with the effective dates of the prior versions of the related Reliability Standards under the implementation plan of the CIP version 5 Standards. NERC states that the purpose of this approach is to provide regulatory certainty by limiting the time, if any, that the CIP version 5 Standards with the "identify, assess, and correct" language would be effective. Specifically, NERC explains that, pursuant to the CIP version 5 implementation plan, the effective date of each of the CIP version 5 Standards is April 1, 2016, except for the effective date for Requirement R2 of CIP-003-5 (i.e., controls for Low Impact BES Cyber Systems), which is April 1, 2017. NERC

explains further that the proposed implementation plan provides that: (1) each of the proposed reliability Standards shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the effective date of the Commission's order approving the proposed Reliability Standard; and (2) responsible entities will not have to comply with the requirements applicable to Low Impact BES Cyber Systems (CIP-003-6, Requirement R1, Part 1.2 and Requirement R2) until April 1, 2017.[79]

77. NERC also explains that the proposed implementation plan includes effective dates for the new and modified definitions associated with: (1) transient devices (*i.e.*, BES Cyber Asset, Protected Cyber Asset, Removable Media, and Transient Cyber Asset); and (2) Low Impact controls (*i.e.*, Low Impact Electronic Access Point and Low Impact External Routable Connectivity). Specifically, NERC proposes that: (1) the definitions associated with transient device become effective on the compliance date for Reliability Standard CIP-010-2, Requirement R4; and (2) the definitions addressing the Low Impact controls become enforceable on the compliance date for Reliability Standard CIP-003-6, Requirement R2. Lastly, NERC proposes that the retirement of Reliability Standards CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1 and CIP-011-1 become effective on the effective date of the proposed Reliability Standards.

[79] NERC Petition at 53-54.

NOPR

78. In the NOPR, the Commission proposed to approve NERC's implementation plan for the proposed CIP Reliability Standards.[80]

Comments

79. A number of commenters request that the Commission act on the proposed revisions to the CIP Standards in a manner that avoids a different implementation date than the CIP version 5 Standards (i.e., April 1, 2016) in order to avoid confusion and unnecessary burdens.[81] Trade Associations encourage the Commission to take alternative actions to avoid unnecessary burden if a Final Rule facilitating an April 1, 2016 effective date for the revised CIP Standards is not feasible. Reclamation suggests that the Commission update and extend the standards implementation plan for each of the CIP version 5 Standards to April 1, 2017, except for the effective date for Requirement R2 of CIP-003-5, which Reclamation argues should be updated to April 1, 2018. ITC contends that April 1, 2016 is an unreasonably aggressive compliance deadline and urges the Commission to consider extending the deadline by one year to April 1, 2017.

Commission Determination

80. The Commission approves NERC's proposed implementation plan. As a result, the proposed CIP Reliability Standards will be effective the first day of the first calendar

[80] NOPR, 152 FERC ¶ 61,054 at P 73.

[81] Trade Associations Comments at 6; SCE Comments at 4-5; Reclamation Comments at 2-3; Wisconsin Comments at 3; Luminant Comments at 2-3; NextEra Comments at 4.

quarter that is three months after the effective date of the Commission's order approving the proposed Reliability Standard (i.e., July 1, 2016). Responsible entities must comply with the requirements applicable to Low Impact BES Cyber Systems (CIP-003-6, Requirement R1, Part 1.2 and Requirement R2) beginning April 1, 2017, consistent with NERC's proposed implementation plan.

81. We recognize the concerns raised by Trade Associations and other commenters regarding the potential burden of implementing two versions of certain CIP Reliability Standards within a short period of time. The Commission is willing to consider a request to align the implementation dates of certain CIP Reliability Standards or another reasonable alternative approach to addressing potential implementation issues, should NERC or another interested entity submit such a proposal.[82]

III. Information Collection Statement

82. The FERC-725B information collection requirements contained in this Final Rule are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.[83] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[84] Upon approval

[82] Given the upcoming April 1, 2016 implementation date for the CIP version 5 Standards, NERC or another interested entity may wish to consider seeking expedited action for any request to address potential implementation issues. The Commission would be cognizant, in considering any request, of the need to provide adequate notice of any changes prior to April 1, 2016.

[83] 44 U.S.C. 3507(d).

[84] 5 CFR 1320.11.

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.

83. The Commission solicited comments on the need for and purpose of the information contained in the proposed CIP Reliability Standards, including 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. The Commission received no comments regarding the need for the information collection or the burden estimates associated with the proposed CIP Reliability Standards as described in the NOPR.

84. Public Reporting Burden: The Commission based its paperwork burden estimates on the changes in paperwork burden presented by the proposed CIP Reliability Standards as compared to the CIP version 5 Standards. The Commission has already addressed the burden of implementing the CIP version 5 Standards.[85] As discussed above, the immediate rulemaking addresses four areas of modification to the CIP version 5 Standards: (1) removal of the "identify, assess, and correct" language from 17 CIP requirements; (2) development of enhanced security controls for low impact assets;

[85] *See* Order No. 791, 145 FERC ¶ 61,160 at PP 226-244.

(3) development of controls to protect transient electronic devices (e.g., thumb drives and laptop computers); and (4) protection of communications networks. We do not anticipate that the removal of the "identify, assess, and correct" language will impact the reporting burden, as the substantive compliance requirements would remain the same, while NERC indicates that the concept behind the deleted language continues to be implemented within NERC's compliance function. The development of controls to protect transient devices and protection of communication networks (as proposed by NERC) have associated reporting burdens that will affect a limited number of entities, i.e., those with Medium and High Impact BES Cyber Systems. The enhanced security controls for Low Impact assets are likely to impose a reporting burden on a much larger group of entities.

85. The NERC Compliance Registry, as of June 2015, identifies approximately 1,435 U.S. entities that are subject to mandatory compliance with Reliability Standards. Of this total, we estimate that 1,363 entities will face an increased paperwork burden under the proposed CIP Reliability Standards, and we estimate that a majority of these entities will have one or more Low Impact assets. In addition, we estimate that approximately 23 percent of the entities have assets that will be subject to Reliability Standards CIP-006-6 and CIP-010-2. Based on these assumptions, we estimate the following reporting burden for entities with Medium and/or High Impact Assets:

Registered Entities	Number of Entities	Total Burden Hours in Year 1	Total Burden Hours in Year 2	Total Burden Hours in Year 3
Entities subject to CIP-006-6 and CIP-	313	75,120	130,208	130,208

010-2 with Medium and/or High Impact Assets				
Totals	313	75,120	130,208	130,208

86. The following shows the annual cost burden for the group with Medium and/or High Impact Assets, based on the burden hours in the table above:

- Year 1: Entities subject to CIP-006-6 and CIP-010-2 with Medium and/or High Impact Assets: 313 entities x 240 hours/entity * $76/hour = $5,709,120.
- Years 2 and 3: 313 entities x 416 hours/entity * $76/hour = $9,895,808 per year.
- The paperwork burden estimate includes costs associated with the initial development of a policy to address requirements relating to transient electronic devices, as well as the ongoing data collection burden. 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.

Based on the assumptions, we estimate the following reporting burden for entities with Low Impact Assets:

Registered Entities	**Number of Entities**	**Total Burden Hours in Year 1**	**Total Burden Hours in Year 2**	**Total Burden Hours in Year 3**
Entities subject to CIP-003-6 with low	1,363	163,560	283,504	283,504

impact Assets				
Totals	1,363	163,560	283,504	283,504

87. The following shows the annual cost burden for the group with Low Impact Assets, based on the burden hours in the table above:

- Year 1: Entities subject to CIP-003-6 with Low Impact Assets: 1,363 entities x 120 hours/entity * $76/hour = $12,430,560.
- Years 2 and 3: 1,363 entities x 208 hours/entity * $76/hour = $21,546,304 per year.
- The paperwork burden estimate includes costs associated with the modification of existing policies to address requirements relating to low impact assets, as well as the ongoing data collection burden, as set forth in CIP-003-6, Requirements R1.2 and R2, and Attachment 1. Further, the estimate reflects the assumption that costs incurred in year 1 will pertain to revising existing policies, while costs in years 2 and 3 will reflect the burden associated with maintaining logs and other records to demonstrate ongoing compliance.

88. The estimated hourly rate of $76 is the average (rounded) loaded cost (wage plus benefits) of legal services ($129.68 per hour), technical employees ($58.17 per hour) and

administrative support ($39.12 per hour), based on hourly rates and average benefits data from the Bureau of Labor Statistics.[86]

89. Title: Mandatory Reliability Standards, Revised Critical Infrastructure Protection 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 Final Rule approves the requested modifications to Reliability Standards pertaining to critical infrastructure protection. As discussed above, the Commission approves NERC's proposed revised CIP Reliability Standards pursuant to section 215(d)(2) of the FPA because they improve 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.

90. 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].

[86] *See* http://bls.gov/oes/current/naics2_22.htm and http://www.bls.gov/news.release/ecec.nr0.htm. Hourly figures as of June 1, 2015.

91. 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) 395-0710, 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 RM15-14-000 and OMB Control Number 1902-0248.

IV. Regulatory Flexibility Act Analysis

92. 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.[87] The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.[88] 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).[89] Proposed Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2 are expected to impose an additional

[87] 5 U.S.C. 601-12.

[88] 13 CFR 121.101.

[89] SBA Final Rule on "Small Business Size Standards: Utilities," 78 Fed. Reg. 77,343 (Dec. 23, 2013).

burden on 1,363 U.S. entities[90] (reliability coordinators, generator operators, generator owners, interchange coordinators or authorities, transmission operators, balancing authorities, transmission owners, and certain distribution providers).

93. Of the 1,363 affected entities discussed above, we estimate that 444 entities are small entities. We estimate that 399 of these 444 small entities do not own BES Cyber Assets or BES Cyber Systems that are classified as Medium or High Impact and, therefore, will only be affected by the proposed modifications to Reliability Standard CIP-003-6. As discussed above, proposed Reliability Standard CIP-003-6 enhances reliability by providing criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for Low Impact BES Cyber Assets. We estimate that each of the 399 small entities to whom the proposed modifications to Reliability Standard CIP-003-6 applies will incur one-time costs of approximately $149,358 per entity to implement this standard, in addition to the ongoing paperwork burden reflected in the Information Collection Statement (a total of $40,736 per entity over Years 1-3), giving a total one-time cost of $190,094 per entity. We do not consider the estimated one-time costs for these 399 small entities a significant economic impact.

94. In addition, we estimate that 14 small entities own Medium Impact substations and that 31 small transmission operators own Medium or High impact control centers. These

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

45 small entities represent 10.1 percent of the 444 affected small entities. We estimate that each of these 45 small entities may experience an economic impact of $50,000 per entity in the first year of initial implementation to meet proposed Reliability Standard CIP-010-2 and $30,000 in ongoing annual costs.[91] In addition, those 45 small entities will have paperwork burden (reflected in the Information Collection Statement) of $81,472 per entity over Years 1-3. Therefore, we estimate that each of these 45 small entities will incur a total of $191,472 in costs over the first three years. We conclude that 10.1 percent of the total 444 affected small entities does not represent a substantial number in terms of the total number of regulated small entities.

95. Based on the above analysis, the Commission certifies that the proposed Reliability Standards will not have a significant economic impact on a substantial number of small entities. Accordingly, no regulatory flexibility analysis is required.

V. Environmental Analysis

96. 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.[92] 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

[91] Estimated annual cost for year 2 and forward.

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

not substantially change the effect of the regulations being amended.[93] The actions proposed herein fall within this categorical exclusion in the Commission's regulations.

VI. Effective Date and Congressional Notification

97. This Final Rule is effective **[insert date 65 days after publication in the Federal Register]**. The Commission has determined, with the concurrence of the Administrator of the Office of Information and Regulatory Affairs of OMB, that this rule is a "major rule" as defined in section 351 of the Small Business Regulatory Enforcement Fairness Act of 1996. This Final Rule is being submitted to the Senate, House, and Government Accountability Office.

VII. Document Availability

98. 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.

99. 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

[93] 18 CFR 380.4(a)(2)(ii).

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

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

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

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

Appendix
Commenters

Abbreviation	Commenter
AEP	American Electric Power Service Corporation
ACS	Applied Control Solutions, LLC
APS	Arizona Public Service Company
Arkansas	Arkansas Electric Cooperative
BPA	Bonneville Power Administration
CEA	Canadian Electricity Association
Consumers Energy	Consumers Energy Company
CyberArk	CyberArk
EnergySec	Energy Sector Security Consortium, Inc
Ericsson	Ericsson
Foundation	Foundation for Resilient Societies
G&T Cooperatives	Associated Electric Cooperative, Inc., Basin Electric Power Cooperative, and Tri-State Generation and Transmission Association, Inc.
Gridwise	Gridwise Alliance
Idaho Power	Idaho Power Company
Indegy	Indegy
IESO	Independent Electricity System Operator
IRC	ISO/RTO Council
ISO New England	ISO New England Inc.
ITC	ITC Companies
Isologic	Isologic, LLC
KCP&L	Kansas City Power & Light Company and KCP&L Greater Missouri Operations Company
Luminant	Luminant Generation Company, LLC
NEMA	National Electrical Manufacturers Association
NERC	North American Electric Reliability Corporation
NextEra	NextEra Energy, Inc.
NIPSCO	Northern Indiana Public Service Co.
NWPPA	Northwest Public Power Association
Peak	Peak Reliability
PNM	PNM Resources
Reclamation	Department of Interior Bureau of Reclamation
SIA	Security Industry Association
SCE	Southern California Edison Company
Southern	Southern Company Services

SPP RE	Southwest Power Pool Regional Entity
SWP	California Department of Water Resources State Water Project
TVA	Tennessee Valley Authority
Trade Associations	Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Electric Power Supply Association, Transmission Access Policy Study Group, and Large Public Power Council
UTC	Utilities Telecom Council
Waterfall	Waterfall Security Solutions, Ltd.
Wisconsin	Wisconsin Electric Power Company
Weis	Joe Weis