156 FERC ¶ 61,052
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. RM15-14-001

ORDER NO. 822-A

ORDER DENYING REHEARING

(Issued July 21, 2016)

1. In Order No. 822, the Commission approved seven modified critical infrastructure protection (CIP) Reliability Standards submitted by the North American Electric Reliability Corporation (NERC).[1] In addition, pursuant to section 215(d)(5) of the Federal Power Act (FPA), the Commission directed NERC to develop additional modifications to the Critical Infrastructure Protection (CIP) Reliability Standards.[2] Foundation for Resilient Societies (Resilient Societies) and Isologic filed requests for

[1] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 81 Fed. Reg. 4177 (January 26, 2016), 154 FERC ¶ 61,037 (2016) (approving Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2 and CIP-011-2).

[2] 16 U.S.C. § 824o(d)(5) (2012).

rehearing of Order No. 822.[3] For the reasons discussed in the body of this order, we deny rehearing.[4]

I. Background

2. In Order No. 791, the Commission approved the CIP version 5 Standards.[5] In addition, pursuant to section 215(d)(5) of the FPA, the Commission directed NERC, *inter alia*, to develop a definition for the term "communication networks" for inclusion in the NERC Glossary of Terms and to develop new or modified Reliability Standards to address the protection of nonprogrammable components of communications networks.[6] Order No. 791 concluded that, without the modifications directed by the Commission, a reliability gap might exist because the CIP version 5 Standards "do not address security controls needed to protect the nonprogrammable components of communications networks."[7] On February 13, 2015, NERC submitted a petition seeking approval of the revised CIP Reliability Standards that NERC developed in response to the directives in Order No. 791.

---

[3] The rehearing requests submitted by Resilient Societies and Isologic raise similar issues and cite to each other for support. *See, e.g.*, Resilient Societies Request at 13; Isologic Request at 2.

[4] On March 29, 2016, Resilient Societies, Isologic and Applied Control Solutions, LLC filed a joint motion to "reopen the evidentiary record in Docket No. RM15-14-000." However styled, the joint motion is a supplemental request for rehearing of Order No. 822. As the joint motion was filed beyond the 30 days allowed by statute, 16 U.S.C. § 825l(a) (2012), the Federal Power Act does not allow us to consider the supplement here. *See also* 18 C.F.R. § 385.713(b) (2014); *Public Service Company of New Hampshire*, 134 FERC ¶ 61,041, at P 7 n.13 (2011). We note, however, that certain issues raised in the joint motion may be considered through other procedures discussed below.

[5] *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) (approving Reliability Standards CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 (CIP version 5 Standards)).

[6] Order No. 791, 145 FERC ¶ 61,160 at P 150.

[7] *Id.* P 149.

II. Discussion

A. Communication Networks and Substations

Order No. 822

3. Order No. 822 approved NERC's proposed alternative to the directive in Order No. 791 that NERC develop a definition of "communication networks." The approved alternative required responsible entities to develop controls to secure nonprogrammable components of communication networks at Control Centers with High or Medium Impact BES Cyber Systems.[8] The Commission determined that NERC's alternative addressed, in part, the concerns in Order No. 791 regarding the security of nonprogrammable components of communication networks. However, the Commission determined that further "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."[9] Accordingly, in addition to approving the CIP Reliability Standards, the Commission directed NERC, pursuant to section 215(d)(5) of the FPA, to modify Reliability Standard CIP-006-6 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).[10]

4. In addition, Order No. 822 directed NERC to conduct a study to assess the effectiveness of the CIP version 5 Standards regarding remote access controls, the risks posed by remote-access related threats and vulnerabilities, and appropriate mitigating controls for any identified risks. The Commission directed NERC to consult with Commission staff on the general content of the remote access report, which is due within one year of the implementation of the CIP version 5 Standards for High and Medium Impact BES Cyber Systems.[11]

---

[8] Order No. 822, 154 FERC ¶ 61,037 at P 52.

[9] *Id.* P 53.

[10] *Id.*

[11] *Id.* P 64.

Request

5. Resilient Societies and Isologic contend that the Commission erred in approving NERC's alternative approach to the Order No. 791 directive to create a NERC Glossary of Terms definition for "communication networks." Resilient Societies and Isologic maintain that the Commission's decision to approve NERC's alternative approach and not to require an "inclusive" definition of communication networks, which includes substations, violates the intent of FPA section 215.[12] Resilient Societies cites the definition of "reliable operation" and "cybersecurity incident" in FPA section 215 to assert that the "unambiguous Congressional intent to protect 'communication networks' from 'cybersecurity incidents' … is indicated by the careful definition of 'cybersecurity incident' in Section 215."[13] Resilient Societies also contends that the Commission, by approving NERC's alternative approach, unlawfully delayed consideration of protecting a broader definition of communication networks.

6. Resilient Societies maintains that Order No. 822 erred by excluding electric grid substations from mandatory cyber protections in the CIP Reliability Standards.[14] In addition, Resilient Societies raises a concern that Order No. 822 does not reflect lessons learned from a December 23, 2015 cyber attack on Ukraine's electric grid. In particular, Resilient Societies notes that the targets of the attack in the Ukraine incident were, in relevant part, electric grid substations and associated control centers.[15]

Commission Determination

7. We deny rehearing of the determinations contained in Order No. 822 pertaining to the protection of communication networks in the CIP Reliability Standards.

8. There is no support for Resilient Societies' assertion that FPA section 215 requires development of a definition of communication networks for inclusion in the NERC Glossary of Terms. While the definition of "cybersecurity incident" in FPA section 215(a)(7) contains the term "communication networks," section 215 nowhere directs the Electric Reliability Organization (ERO) or the Commission to define that

[12] *See* Resilient Societies Request at 3-6; Isologic Request at 17-18.

[13] Resilient Societies Request at 5.

[14] *Id.* at 6-9.

[15] *Id.* at 8.

term. The Commission also rejects the contention that the definition of "reliable operation" in FPA section 215(a)(4) mandates the broader definition of "communication networks" advocated by Resilient Societies, which includes substations.

9. FPA section 215(d)(2) states that the Commission "may approve, by rule or order, a proposed reliability standard or modification to a reliability standard if it determines that the standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest." In Order No. 822, the Commission determined that the CIP Reliability Standards, by protecting control centers with High and Medium Impact BES Cyber Systems, met that standard and satisfied in part the reliability gap discussed in Order No. 791. The Commission concluded, however, that modifications to the CIP Reliability Standards "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."[16] Order No. 822 also directed NERC to develop modifications to Reliability Standard CIP-006-6 to protect control centers with Low Impact assets. These determinations, taken together, address Resilient Societies' assertions of error regarding the need to define the term communication networks and, instead, reflect ongoing efforts by the ERO and Commission to develop and approve CIP Reliability Standards that satisfy the standard set forth in FPA section 215(d)(2) for approving Reliability Standards and address evolving cybersecurity threats to the Bulk-Power System.[17]

10. We also reject the claim that substations are excluded from protection under the CIP Reliability Standards. All bulk electric system substations within the Commission's jurisdiction under FPA section 215 are protected under the CIP Reliability Standards. All BES Cyber Assets contained in those substations are classified as High, Medium or Low Impact under the CIP Reliability Standards and, thus, are subject to the corresponding controls imposed by the CIP Reliability Standards.[18] Further, Resilient Societies appears to advocate for the protection of distribution level substations that are not included in the bulk power system. Section 215 of the FPA, however, authorizes the ERO to develop

[16] Order No. 822, 154 FERC ¶ 61,037 at P 53.

[17] Order No. 822 explained the Commission's reasons for accepting NERC's alternative proposal to the Order No. 791 directive to create a NERC Glossary of Terms definition for "communication networks." *See* Order No. 822, 154 FERC ¶ 61,037 at PP 52-55.

[18] *See* Order No. 791, 145 FERC ¶ 61,160 at P 41 (citing Reliability Standard CIP-002-5).

and the Commission to approve Reliability Standards that "provide for the protection of the bulk power system," and does not apply to local distribution facilities.[19] Thus, we deny this aspect of the request for rehearing as outside the scope of the Commission's authority.

11. With respect to Resilient Societies' concern that Order No. 822 did not incorporate lessons learned from the Ukraine incident, any relevant lessons from the Ukraine incident could be considered in future versions of the CIP Reliability Standards.[20] As discussed above, Order No. 822 directed NERC to conduct a study to assess the effectiveness of the CIP version 5 Standards remote access controls, the risks posed by remote-access related threats and vulnerabilities, and appropriate mitigating controls for any identified risks. We expect the remote access study to address remote communications associated with Control Centers and substations. In addition, we expect NERC to incorporate analyses of the Ukraine incident conducted by the Department of Homeland Security, NERC and others in the remote access study, and we direct Commission staff, as part of the consultative process between NERC staff and Commission staff directed in Order No. 822, to work with NERC staff to evaluate the Ukraine incident in the remote access study.[21] In addition to the remote access study, the Commission is also concurrently issuing a Notice of Inquiry concerning: (1) isolation between the internet and cyber systems in control centers performing transmission operator functions; and (2) mandatory application "whitelisting" for all cyber systems in control centers.[22]

---

[19] *See* 16 U.S.C. § 824o(a)(3).

[20] The Commission issued Order No. 822 less than one month after the Ukraine incident and more than one month prior to the release of a Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team alert on the Ukraine incident. *See* ICS-CERT Alert IR-ALERT-H-16-056-01, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[21] Order No. 822, 154 FERC ¶ 61,037 at P 64 ("NERC should consult with Commission staff to determine the general contents of the directed report.").

[22] *See Cyber Systems in Control Centers*, Notice of Inquiry, Docket No. RM16-18-000 (2016).

B. Removal of Malware under CIP Reliability Standards

Request

12. Resilient Societies contends that Order No. 822 erred by not requiring the removal of cyber malware embedded in the Bulk-Power System. Resilient Societies requests that the Commission modify Order No. 822 "to include the duty to assess, to monitor, and to remove cyber malware from the system components of NERC-registered entities subject to FERC jurisdiction."[23]

Commission Determination

13. We deny Resilient Societies' rehearing request regarding the removal of malware under the CIP Reliability Standards. The CIP Reliability Standards already address the threat posed by malicious code to the Bulk-Power System. Specifically, Reliability Standard CIP-007-6, Requirement R3 requires responsible entities to "[d]eploy method(s) to deter, detect, or prevent malicious code" (Requirement R3.1) and to "mitigate the threat of detected malicious code" (Requirement R3.2). In the Guidelines and Technical Basis section of Reliability Standard CIP-007-6, the subsection devoted to Requirement R3.2 makes clear that "[w]hen malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated."

C. Other Request

Request

14. Resilient Societies requests that "the Commission modify its Order No. 822 to clarify that it is not the intent of the Commission to preclude complementary operational cybersecurity programs; and that the requirements of [Commission] Order No. 822 are not intended as a barrier to essential cybersecurity protections otherwise duly authorized."[24]

---

[23] Resilient Societies Request at 10.

[24] *Id.* at 12.

Commission Determination

15. In Order No. 822, the Commission approved the CIP Reliability Standards pursuant to FPA section 215(d)(2). Nothing in Order No. 822 or the CIP Reliability Standards purports to preclude additional measures designed to address cybersecurity threats.[25]

The Commission orders:

The Commission hereby denies rehearing, for the reasons discussed in the body of this order.

By the Commission.

(S E A L)

Kimberly D. Bose,
Secretary.

[25] *See, e.g.*, 16 U.S.C. § 824o(i)(3) (2012) ("nothing in this section shall be construed to preempt any authority of any State to take action to ensure the safety, adequacy, and reliability of electric service within that State, as long as such action is not inconsistent with any reliability standard").