146 FERC ¶ 61,188
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Cheryl A. LaFleur, Acting Chairman;
Philip D. Moeller, John R. Norris,
and Tony Clark.

Version 5 Critical Infrastructure Protection Reliability Standards — Docket No. RM13-5-001

ORDER NO. 791-A

ORDER ON CLARIFICATION AND REHEARING

(Issued March 20, 2014)

1. In Order No. 791, the Commission approved the Version 5 Critical Infrastructure Protection (CIP) Reliability Standards, CIP-002-5 through CIP-011-1 (CIP version 5 Standards), submitted by the North American Electric Reliability Corporation (NERC).[1] American Public Power Association (APPA) and National Rural Electric Cooperative Association (NRECA) filed a joint request for clarification of Order No. 791, as did Utility Services, Inc. (Utility Services). Edison Electric Institute (EEI) and Electric Power Supply Association (EPSA) jointly filed requests for clarification and rehearing of Order No. 791. For the reasons discussed in the body of this order, we grant clarification in part and deny rehearing.

I. Background

A. NERC Petition

2. On January 31, 2013, NERC filed a petition seeking Commission approval of the CIP version 5 Standards.[2] The CIP version 5 Standards require responsible entities to

[1] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160 (2013).

[2] In addition to the petition, NERC submitted an informational filing in this docket describing a pilot program that NERC plans to conduct during the transition from the Version 3 CIP Reliability Standards to the CIP version 5 Standards. NERC October 11, 2013 Information Filing (NERC Informational Filing).

identify and categorize bulk electric system (BES) Cyber Systems using a new methodology based on whether a BES Cyber System has a Low, Medium, or High Impact on the reliable operation of the bulk electric system. At a minimum, a BES Cyber System must be categorized as a Low Impact asset. Once a BES Cyber System is categorized, a responsible entity must comply with the associated requirements of the CIP version 5 Standards that apply to the impact category.

B. NOPR

3. On April 18, 2013, the Commission issued a Notice of Proposed Rulemaking (NOPR) proposing to approve the CIP version 5 Standards.[3] While proposing to approve the CIP version 5 Standards, the NOPR posed questions or proposed directives to NERC regarding possible revisions to the CIP Reliability Standards. These issues included: (1) the CIP version 5 Standards implementation plan; (2) the language in 17 requirements of the CIP version 5 Standards that would require responsible entities to implement the requirements in a manner to "identify, assess, and correct" deficiencies; and (3) the proposed definitions of BES Cyber Asset and Cyber Asset. The NOPR also proposed to certify that a full Regulatory Flexibility Act (RFA) analysis was not necessary because the CIP version 5 Standards will not have a significant impact on a substantial number of small entities.[4]

4. In response to the NOPR, interested entities filed 62 comments.

C. Order No. 791

5. In Order No. 791, the Commission adopted the NOPR proposal to approve the CIP version 5 Standards, including the implementation plan. Order No. 791 also adopted in part some of the directives proposed in the NOPR. Order No. 791 directed NERC to remove the "identify, assess, and correct" language or to propose modifications that addressed the Commission's concerns about the ambiguity and enforceability of that language. Order No. 791 also directed NERC to conduct a survey of responsible entities during the CIP version 5 Standards implementation period to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter and to submit an informational filing assessing, based on the survey results, whether the BES Cyber Asset definition will, with the 15-minute parameter, cover the assets that are necessary to ensure the reliable operation of

[3] *Version 5 Critical Infrastructure Protection Reliability Standards*, Notice of Proposed Rulemaking, 78 Fed. Reg. 24,107 (Apr. 24, 2013), 143 FERC ¶ 61,055 (2013).

[4] 5 U.S.C. 601-612 (2012).

the Bulk-Power System.[5] Order No. 791 further directed NERC to create a definition of communication networks and to develop new or modified Reliability Standards that address the protection of communication networks. Order No. 791 also certified that a full RFA analysis was not required.

II. Discussion

6. The Commission grants clarification in part and denies rehearing, as discussed below.

A. Implementation Plan

Order No. 791

7. In Order No. 791, the Commission approved NERC's proposed implementation plan for the CIP version 5 Standards.[6] The effective date of Order No. 791 was February 3, 2014. NERC's implementation plan provides that responsible entities must achieve compliance by the first day of the first calendar quarter that is 24 months after the effective date of the final rule for provisions pertaining to High and Medium Impact assets (i.e., by April 1, 2016) and that is 36 months for Low Impact assets (i.e., by April 1, 2017).

Request

8. Utility Services requests that the Commission clarify that the 24- and 36-month implementation periods for the CIP version 5 Standards should start beginning April 1, 2016 rather than from the effective date of Order No. 791. Utility Services recognizes that under the 24- and 36-month implementation periods approved in Order No. 791, responsible entities must be in compliance by April 1, 2016 or April 1, 2017. However,

[5] The BES Cyber Asset definition includes Cyber Assets that "if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment …" Order No. 791, 145 FERC ¶ 61,160 at P 6 n.6.

[6] NERC's implementation plan stated: "24 Months Minimum – The Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval." NERC January 31, 2013 Petition, Exhibit B at 2.

Utility Services maintains that responsible entities should have the full benefit of the NERC pilot program during the entire implementation period. Utility Services states that, because the NERC pilot program will be "completed [in] April 2014, with the transition document to follow," the 24- and 36-month implementation periods should commence beginning on April 1, 2016.[7] In the alternative, Utility Services requests clarification that the implementation plan for entities not subject to the Version 3 CIP Reliability Standards and "entities with potential for Low Impact assets [should] start after the CIP V5 Reliability Standards become effective."[8] Utility Services maintains that to do otherwise would force entities not currently subject to the CIP Reliability Standards to create a CIP compliance program from scratch "for a set of standards that are not yet effective and without the benefit of the NERC pilot program or transition guidance document."[9] Utility Services also states that responsible entities would benefit from knowing how NERC will respond to the directive in Order No. 791 that NERC address the protection of Low Impact assets before developing their compliance programs.

9. EEI-EPSA also seek rehearing or, in the alternative, clarification that the implementation plan submitted by NERC "is the controlling reference and that the effective date of the standard for high and medium assets, as determined under the current implementation plan, is April 1, 2016."[10] EEI-EPSA further request that the Commission stay the implementation date for Low Impact assets in light of the directive in Order No. 791 requiring NERC to address the protection of Low Impact assets. EEI-EPSA maintain that it would be more appropriate for NERC to propose an implementation date for Low Impact assets when NERC submits the proposed Low Impact asset protections in compliance with Order No. 791.

Commission Determination

10. We deny the request for clarification by Utility Services. In Order No. 791, the Commission approved the 24- and 36-month implementation periods proposed by NERC, commencing from the effective date of the Final Rule. NERC's proposal did not contemplate linking the 24- and 36-month implementation periods to the completion of the NERC pilot program. Moreover, because NERC states that the pilot program will be completed in April 2014, responsible entities will benefit from any lessons learned well

[7] Utility Services Request at 5.

[8] *Id.* at 6.

[9] *Id.*

[10] *Id.* at 12.

before the 24- and 36-month implementation deadlines. The NERC Informational Filing further supports our conclusion in stating that, "[t]o ensure that all Responsible Entities are adequately prepared to implement CIP Version 5, NERC expects to keep industry informed regarding progress compared with key Study milestones, key issues that arise and solutions to address them, lessons that are learned by Study Participants throughout the Study, best technical practices to meet the intent of CIP Version 5, best practices to demonstrate compliance with CIP Version 5, and recommendations for future action outside the scope of the Study."[11] Accordingly, responsible entities will benefit from the pilot program even before its completion.

11. We also reject the request by Utility Services to extend the implementation period for Low Impact assets and for responsible entities that are currently not subject to the CIP Reliability Standards. The implementation plan proposed by NERC and approved in Order No. 791 provided a longer implementation period for Low Impact assets (i.e., 36 months). We see no reason to alter that schedule. We reject the argument that the directive in Order No. 791 that NERC address security controls for Low Impact assets justifies a delay of the implementation schedule. The Commission did not impose a deadline on NERC to comply with this directive, and the Commission expects that the directive will be satisfied in future revisions of the CIP Reliability Standards. As such, the directive concerning Low Impact assets in Order No. 791 should not affect or delay the implementation of the CIP version 5 Standards.[12]

12. In response to EEI-EPSA, as discussed above, we clarify that the implementation plan submitted by NERC and approved in Order No. 791 requires responsible entities to comply with the High and Medium Impact asset requirements by April 1, 2016.

B. "Identify, Assess, and Correct" Language

Order No. 791

13. The CIP version 5 Standards incorporate "a requirement that Responsible Entities implement cyber policies in a manner to 'identify, assess, and correct' deficiencies" in 17 CIP requirements. NERC explained that the "identify, assess and correct" language was intended to encourage the development of strong internal controls by responsible entities while minimizing the compliance burdens associated with high frequency (i.e., recurring, security obligations).

---

[11] NERC Informational Filing at 6.

[12] For the same reasons, we reject EEI-EPSA's request to stay the implementation schedule for Low Impact assets.

14. In Order No. 791, the Commission determined that the "identify, assess, and correct" language would impose implementation and compliance obligations that are unclear and too vague to audit and enforce. Order No. 791 directed that, "[p]referably, NERC should remove the 'identify, assess, and correct' language from the 17 CIP version 5 requirements, while retaining the substantive provisions of those requirements. Alternatively, NERC may propose equally efficient and effective modifications that address the Commission's concerns regarding the 'identify, assess, and correct' language."[13]

Request

15. APPA-NRECA request clarification whether the "identify, assess, and correct" language should be deemed eliminated from the CIP version 5 Standards, subject to the outcome of Commission action on NERC's Order No. 791 compliance filing due by February 3, 2015, or if responsible entities should work towards implementing the "identify, assess, and correct" language. To the extent the Commission expects responsible entities to develop a compliance program to implement the "identify, assess, and correct language," APPA-NRECA request clarification as to "what is to be complied with and what processes should be adopted."[14]

Commission Determination

16. We deny APPA-NRECA's request for clarification concerning how responsible entities should address the "identify, assess, and correct" language pending NERC's Order No. 791 compliance filing. In Order No. 791, the Commission highlighted its support for a move away from a "zero tolerance" approach to compliance; the development and adoption of strong internal controls by responsible entities; and the development of Reliability Standards that focus on those activities with the greatest impact on Bulk-Power System reliability.[15] The Commission also noted its willingness to consider various approaches to address concerns associated with the compliance aspects of the CIP Reliability Standards but concluded that "the 'identify, assess, and correct' language, as currently proposed, injects an unacceptable degree of ambiguity into the otherwise reasonable substantive requirements of the CIP version 5 Standards."[16] Although Order No. 791 determined that the inclusion of the "identify, assess, and

[13] Order No. 791, 145 FERC ¶ 61,160 at P 67.

[14] APPA-NRECA Request at 4.

[15] *See* Order No. 791, 145 FERC ¶ 61,160 at P 69.

[16] *Id.* P 72.

correct" language, as proposed, is not acceptable, the Commission found that the substantive, technical requirements of the CIP version 5 Standards are just and reasonable. As a result, NERC's Order No. 791 compliance filing should address the compliance aspects of the 17 requirements at issue as opposed to the substantive, technical controls. We expect responsible entities to move forward with implementation of the substantive, technical controls approved in Order No. 791 while NERC addresses the Commission's directive regarding the "identify, assess, and correct" compliance language.

C. BES Cyber Asset Definition and Communication Networks

Order No. 791

17. In its petition, NERC proposed a definition of BES Cyber Asset that, in relevant part, encompasses Cyber Assets that "if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment …"[17] The Commission, in Order No. 791, approved the definition of BES Cyber Asset but directed NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods. Order No. 791 directed that, based on the survey data, NERC should explain in an informational filing: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition.[18]

18. NERC also proposed to revise the definition of Cyber Asset to remove the phrase "communication networks." In Order No. 791, the Commission approved the proposed definition but determined that a reliability gap may exist, as the CIP version 5 Standards do not address security controls needed to protect the nonprogrammable components of communications networks. Accordingly, Order No. 791 directed NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the reliability gap discussed above.

---

[17] *Id.* P 6 n.6.

[18] *Id.* P 124.

Request

19. EEI-EPSA seek rehearing or, in the alternative, clarification of the directive in Order No. 791 requiring NERC to conduct a survey and submit an informational filing regarding the "15-minute parameter" in the definition of BES Cyber Asset. EEI-EPSA seek rehearing to the extent that Order No. 791 directed NERC to make an "inventory-type of survey." EEI-EPSA maintain that an inventory-type survey would impose an unreasonable burden on responsible entities and would not be the most effective means of obtaining the information that Order No. 791 seeks. EEI-EPSA state that such an understanding would be better developed by a separate technical workshop. In the alternative, EEI-EPSA request clarification that Order No. 791 intended to direct NERC to conduct a survey in order to foster "a high-level discussion of the issues raised by the 15-minute parameter (as articulated in P 124 of the Final Rule), as opposed to specific questions that would require a survey similar to the inventory of low assets that FERC has already conceded would be overly burdensome."[19]

20. EEI-EPSA also seek clarification that the Commission does not expect industry to develop controls for any components of communications networks that are outside the control of responsible entities.

Commission Determination

21. The Commission grants clarification and denies rehearing with respect to EEI-EPSA's requests. We clarify that Order No. 791 did not direct NERC to conduct an inventory-type survey of all Cyber Assets impacted by the 15-minute parameter. Instead, the scope of the survey was left for NERC to determine. Order No. 791 intended that NERC develop a survey of sufficient scope in order to respond to the questions posed in Order No. 791 in the required NERC informational filing. For example, NERC could use the participants in the pilot program, discussed above, as the basis for the survey.[20]

22. We further clarify that, with respect to the directive concerning the development of Reliability Standards that "require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks," Order No. 791 did not require the development of controls for third-party communications networks. However, we expect that the April 29, 2014 staff-led technical conference will address the possible need for registered entities to use techniques such as encryption if they choose to rely on

[19] EEI-EPSA Request at 7.

[20] *See supra* note 2.

third-party communication networks, or to limit themselves to using networks meeting appropriate security criteria.[21]

D. Regulatory Flexibility Act

Order No. 791

23. Order No. 791 certified that a full RFA analysis was not required. In the NOPR, the Commission applied the Small Business Administration's (SBA) definition of "small entity" to data from the Department of Energy's Energy Information Administration and NERC's Compliance Registry, to estimate that the CIP version 5 Standards would impact 536 small entities but that only 14 small entities (2.6 percent of the impacted small entities) would experience a significant economic impact. In response to NOPR comments submitted by APPA, Order No. 791 raised the estimated number of small entities that would be significantly impacted by the CIP version 5 Standards from 14 to 45 (or 8.4 percent of impacted small entities).[22] Order No. 791 also adopted APPA's cost estimates for the 31 additional small entities but maintained the cost estimates set out in the NOPR for the 14 original small entities. Order No. 791 ultimately determined that 8.4 percent of the affected small entities still does not constitute a substantial number relative to the total number of regulated small entities applicable to Order No. 791.

Request

24. APPA-NRECA seek clarification regarding the RFA certification in Order No. 791. APPA-NRECA request clarification of the Commission's rationale for certifying that no RFA analysis was necessary. Specifically, APPA-NRECA seek clarification why the cost estimates for the 14 small entities set forth in the NOPR were not the same (i.e., as high) as the cost estimates for the 31 new small entities identified by APPA in its comments that the Commission adopted in Order No. 791. APPA-NRECA also maintain that Order No. 791 provided no detail regarding how the Commission estimated that 1.5 percent of the total 305 small entities registered as distribution providers would own underfrequency or undervoltage load shedding systems that were previously not subject to the CIP Reliability Standards, and that 10 percent of the 94 total small entities registered as transmission owners would own Medium Impact assets that are subject to CIP version 5 Standards for the first time.

---

[21] On February 27, 2014, a notice of technical conference issued in this docket indicating that the technical conference directed in Order No. 791 will occur on April 29, 2014.

[22] Order No. 791, 145 FERC ¶ 61,160 at P 256.

Commission Determination

25. We deny APPA-NRECA's request for clarification regarding the Order No. 791 RFA certification that the CIP version 5 Standards will not have a significant economic impact on a substantial number of small entities. As an initial matter, the Commission's certification of the potential economic impact of the CIP version 5 Standards on small entities satisfies the RFA requirement with a "statement providing the factual basis for such certification," including the number of affected entities, the size of the economic impacts, underlying assumptions and an explanation why certification was appropriate.[23] The Order No. 791 RFA certification also reflects the comments submitted by entities in response to the RFA certification proposed in the NOPR.

26. As noted above, APPA-NRECA seek clarification why the cost estimates for the 14 small entities set forth in the NOPR were not the same (i.e., as high) as the cost estimates for the 31 additional small transmission operators identified by APPA. First, with regard to the number of entities, the Commission explained in Order No. 791 that it "did not count the small transmission operators identified by APPA because the Commission's analysis assumed that entities had secured the control centers under the CIP version 3 Standards."[24] Second, the Commission documented its cost estimates for the original 14 entities based on an assumption that certain small distribution providers and small transmission owners own Medium Impact assets other than control centers (e.g., underfrequency or undervoltage load shedding systems, and substations) that are subject to CIP version 5 Standards for the first time.[25] The Commission ultimately

[23] 5 U.S.C. § 605(b). The SBA offers the following guidance on the meaning of "factual basis":

> What is a "factual basis?" The Office of Advocacy interprets the "factual basis" requirement to mean that, at a minimum, a certification should contain a description of the number of affected entities and the size of the economic impacts and why either the number of entities or the size of the impacts justifies the certification. The agency's reasoning and assumptions underlying its certification should be explicit in order to elicit public comment.

Small Business Administration, *A Guide for Government Agencies: How to Comply with Regulatory Flexibility Act* (May 2012), *available at:* http://www.sba.gov/sites/default/files/rfaguide_0512_0.pdf .

[24] Order No. 791, 145 FERC ¶ 61,160 at P 258.

[25] *Id.* P 257.

included the 31 small transmission operator control centers in the RFA analysis, including APPA's suggested cost figures.[26] In adopting APPA's suggested cost figures, however, the Commission noted that "APPA provides no detail or support for this figure, as we requested, other than one of its members' planned budgeting for these amounts."[27] While we find it reasonable in this instance to accept APPA's cost figures as they apply to the 31 entities identified by APPA, we will not adopt unsupported cost estimates for other aspects of the analysis.

27. APPA-NRECA also question how the Commission estimated that 1.5 percent of the total 305 small entities registered as distribution providers would own underfrequency or undervoltage load shedding systems that were previously not subject to the CIP Reliability Standards, and that 10 percent of the 94 total small entities registered as transmission owners would own Medium Impact assets that are subject to CIP version 5 Standards for the first time. However, APPA-NRECA do not challenge either of the Commission's assumptions or submit evidence that contradicts those assumptions. Absent any facts that undermine the Commission's clearly-expressed assumptions (i.e., that 1.5 percent of the total 305 small entities registered as distribution providers would own underfrequency or undervoltage load shedding systems that were previously not subject to the CIP Reliability Standards, and that 10 percent of the 94 total small entities registered as transmission owners would own Medium Impact assets that are subject to CIP version 5 Standards for the first time), we see no basis to modify the Order No. 791 RFA certification.

The Commission orders:

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

By the Commission.

(S E A L)

Kimberly D. Bose,
Secretary.

[26] The adoption of APPA's figures was done out of an abundance of caution and not necessarily because the available data actually supported APPA's position. *Id.* P 256, n.291.

[27] *Id.* P 258.