United Arab Emirates.

Shaji Muhammed Basheer, a.k.a. the following alias: 
—S. Basheer.

Shop No. 3 & 4, Sharafia Ahmed Ali Bldg., 
Al Nakheel St., Deira, P.O. Box 171978, 
Dubai, U.A.E.

For all items subject to the EAR. (See § 744.11 of the EAR).


United Kingdom

IKCO Finance 6 Lothbury, London, England, 
EC2R 7HH.

For all items subject to the EAR. (See § 744.11 of the EAR).


Dated: April 18, 2012.

Kevin J. Wolf,
Assistant Secretary for Export Administration.

[FR Doc. 2012–9905 Filed 4–24–12; 8:45 am]
BILLING CODE 3510–33–P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

18 CFR Part 40

[Docket No. RM11–11–000; Order No. 761]

Version 4 Critical Infrastructure Protection Reliability Standards

AGENCY: Federal Energy Regulatory Commission, DOE.

ACTION: Final rule.


DATES: This rule will become effective June 25, 2012.

FOR FURTHER INFORMATION CONTACT: 


SUPPLEMENTARY INFORMATION:

139 FERC ¶ 61,058
Before Commissioners: Jon Wellinghoff, Chairman; Philip D. Moeller, John R. Norris, and Cheryl A. LaFleur.
to meet the deadline and describe the status of its CIP standard development efforts.

I. Background

A. Mandatory Reliability Standards

5. Section 215 of the FPA requires a Commission-certified ERO to develop mandatory and enforceable Reliability Standards, which are subject to Commission review and approval. Once approved, the Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.4

6. Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,5 and subsequently certified NERC as the ERO.6 On January 18, 2008, the Commission issued Order No. 706 approving eight CIP Reliability Standards proposed by NERC. Pursuant to section 215(d)(5) of the FPA,7 the Commission directed NERC to develop modifications to the CIP Reliability Standards to address concerns discussed in Order No. 706. Subsequently, the Commission approved Version 2 and Version 3 of the CIP Reliability Standards, each version including changes responsive to some but not all of the directives in Order No. 706.

B. NERC Petition

7. On February 10, 2011, NERC filed a petition seeking Commission approval of the Version 4 CIP Reliability Standards, CIP–002–4 through CIP–009–4. In the petition, NERC states that the principal differences between Version 3 and Version 4 are found in CIP–002–02, where NERC replaced the risk-based assessment methodology for identifying Critical Assets with 17 uniform “bright line” criteria for identifying Critical Assets. Concerning the process of identifying the associated Critical Cyber Assets that are subject to the cyber security protections required by CIP–003 through CIP–009, NERC made changes for certain generation Critical Assets. NERC submitted proposed VRFs and VSLs and an implementation plan governing the transition to Version 4.

NERC proposed that the Version 4 CIP Reliability Standards become effective the first day of the eighth calendar quarter after applicable regulatory approvals have been received.

8. On April 12, 2011, NERC made an errata filing correcting certain errors in the petition and furnishing corrected exhibits and the standard drafting team minutes. In the errata, NERC also replaced the VRFs and VSLs in the February 10, 2011 petition with new proposed VRFs and VSLs.9

9. Reliability Standard CIP–002–4 requires each responsible entity to use the bright line criteria as a “checklist” to identify Critical Assets, initially and in an annual review, replacing the risk-based assessment methodology developed and applied by each registered entity required under the currently-effective Version 3 CIP Reliability Standards. As in past versions, each responsible entity will then identify the Critical Cyber Assets associated with its updated list of Critical Assets. If application of the bright line criteria results in the identification of Critical Cyber Assets, such assets become subject to the remaining CIP Reliability Standards.

10. In the petition, NERC states that CIP–002–4 addresses some, but not all, of the directives in Order No. 706. NERC explained that the standard drafting team limited the scope of requirements in the development of Version 4 “as an interim step” limited to the concerns raised by the Commission regarding
a deadline of 6 months from the end of the third quarter of 2012 (i.e., March 31, 2013), to provide the ERO with time to address any unforeseen contingencies. In addition, the Commission directs the ERO to submit quarterly reports, at the beginning of each quarter, in which it is to both confirm that it is on track to meet the deadline and describe the status of its CIP Reliability Standards development efforts.

14. Below we discuss the Commission’s basis for approving Version 4 of the CIP Reliability Standards. In addition, we discuss comments regarding: (1) The bright line criteria used to identify Critical Assets that are contained in Attachment 1 of Reliability Standard CIP–002–4; (2) the identification of Critical Assets that fall outside the scope of Attachment 1 by registered entities, Regional Entities, or ERO; (3) the implementation plan for the Version 4 CIP Reliability Standards; (4) compliance with Order No. 706; (5) the deadline for submitting CIP Reliability Standards that fully comply with Order No. 706; and (6) the VRFs and VSLs.

A. The Commission Adopts the NOPR Proposal To Approve the Version 4 CIP Reliability Standards

NERC Petition

15. NERC states that CIP–002–4 establishes clear and uniform criteria for identifying Critical Assets on the Bulk-Power System.16 According to NERC, CIP–002–4 achieves a specified reliability goal by requiring the identification and documentation of Critical Cyber Assets associated with Critical Assets that support the reliable operation of the Bulk-Power System. NERC maintains that the Reliability Standard “improves reliability by establishing uniform criteria across all Responsible Entities for the identification of Critical Assets.”

Further, NERC states that CIP–002–4 contains a technically sound method to achieve its reliability goal by requiring the identification and documentation of Critical Assets through the application of the criteria set forth in Attachment 1 of CIP–002–4.

NOPR

16. In the NOPR, the Commission proposed to approve the Version 4 CIP Reliability Standards. Giving due weight to the ERO’s petition, the NOPR stated that the Version 4 CIP Standards will result in the identification of certain types of Critical Assets that may not be identified under Version 3.

FURTHER READING

13. As discussed below, the Commission approves the eight modified Version 4 CIP Reliability Standards, finding that they are just and reasonable, not unduly discriminatory or preferential and in the public interest. In addition, the Commission approves NERC’s proposed VRFs, VSLs with modifications, and its proposed implementation plan. The Commission has also determined that it is appropriate to impose a deadline for the ERO to achieve full compliance with Order No. 706. NERC commented that it anticipates filing the Version 5 CIP Reliability Standards by the third quarter of 2012.15 We therefore establish

15 NERC Petition at 6 (citing Order No. 706, 122 FERC ¶ 61,040 at P 236).
16 NERC Petition at 6.
19 NERC Reply Comments at 4.
20 NERC Petition at 38.
21 Id. at 4.
existing entity-defined risk-based assessment methodologies that, as applied, generally do not adequately identify Critical Assets; and provides a level of consistency and clarity regarding the identification of Critical Assets lacking under Version 3.

21. With respect to the objections raised by Hydro-Québec and NV Energy, we find them unpersuasive. Although NV Energy asserts that Version 4 will identify Critical Assets that do not require protection or whose protection only offers marginal benefits, as we stated in the NOPR, Version 4 will offer an increase in the overall protection for bulk electric system components that clearly require protection, including control centers. Recognizing that Version 4 is an “interim step,” our concern is that Version 4 does not provide enough protection to satisfy Order No. 706.

22. We also find unpersuasive Hydro-Québec and NV Energy’s claim that the bright line criteria are based on arbitrary values i.e., large amounts of megawatts and voltages) without assessing the impact on reliability, or otherwise lack a technical justification. As discussed later in this final rule, the Commission finds that NERC offered an acceptable technical justification for the bright line criteria used to identify Critical Assets in Version 4. As indicated in the NOPR, we believe that Version 4 is an interim step towards full compliance with Order No. 706 and that implementation of Version 4 and concurrent retirement of Version 3, as proposed in the petition and reaffirmed by the ERO in its comments, is a step towards full compliance with Order No. 706. For the same reason, we reject the G&T Cooperatives’ suggestion that Version 4 be approved for “guidance purposes only.” Nevertheless, we note that approval of the specific bright line approach to identifying Critical Assets adopted in Version 4 does not prejudge the manner in which cyber assets are identified for protection in Version 5 or subsequent revisions to the CIP Reliability Standards.

B. Bright Line Criteria for Identifying Critical Assets


The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP–002–4 Attachment 1—Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually.

Attachment 1 to Reliability Standard CIP–002–4 provides seventeen criteria to be used by all responsible entities for the identification of Critical Assets pursuant to Requirement R1. The thresholds apply to specific types of facilities such as generating units, transmission lines and control centers. Reliability Standard CIP–002–4, Requirement R2 then requires responsible entities to develop a list of Critical Cyber Assets associated with the Critical Assets identified pursuant to Requirement R1.

1. Generation/Transmission

NERC Petition

24. Several of the proposed criteria pertain to the identification of critical generation assets and critical transmission assets. Reliability Standard CIP–002–4, criterion 1.1 designates as Critical Assets: “Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.” Reliability Standard CIP–002–4, Requirement R2 qualifies criterion 1.1 by stating that: “For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.”

25. For transmission assets, criterion 1.6 designates as Critical Assets: “Transmission Facilities operated at 500 kV or higher.” Criterion 1.7 also designates as Critical Assets: “Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.”

26. Reliability Standard CIP–002–4, criterion 1.2 provides that “Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate not Reactive Power nameplate rating of 1000 MVAR or greater” shall be designated as a Critical Asset. Criterion 1.3 designates as Critical Assets: “Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.” Criterion 1.8 designates as Critical Assets: “Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.”

Comments

27. Hydro-Québec states that the term “group of generating units” used in criterion 1.1 is ambiguous because it could mean a generating station or a group of units sharing the same transformer. Hydro-Québec also believes that the 15-minute period, established by CIP–002–4, Requirement R2, which states that “the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1,” needs further explanation because it is unclear how to determine whether operation is not reliable after 15 minutes. Finally, Hydro-Québec contends that the term “Flexible AC Transmission System (FACTS)” in criterion 1.9 must be defined in the NERC Glossary of Terms.

28. NV Energy comments that the bright line criteria lack technical justification because they are primarily based on asset size (e.g., megawatts and voltage levels) to determine criticality. NV Energy maintains that size should not be dispositive to determining whether an asset is critical. NV Energy cites the 500 kV or higher size threshold for transmission facilities in criterion 1.6 as an example of a broad categorization that is likely to capture elements, such as NV Energy’s radial facilities, whose function are not essential to the reliable operation of the

---

23. NOPR, FERC Stats. & Regs. ¶ 32,679 at P 23 (“The number of control centers identified as Critical Assets increases from 425 under Version 3 to 553 under Version 4, the latter figure representing 74 percent of all control centers.”).
24. NERC Petition at 6.
bulk electric system. NV Energy also identifies the 300 kV or higher threshold for transmission facilities interconnected at 300 kV or higher with three or more other transmission stations or substations in criterion 1.7 as another example. NV Energy asserts that other parameters, beyond the number of interconnections, must be evaluated to determine criticality. Finally, NV Energy states that the 1500 MW threshold in criterion 1.1 lacks technical justification.

29. ISO/RTO Council states that responsibility for identifying critical generation should not be shifted from generation owners under criterion 1.3, which it maintains allows a planning coordinator or transmission planner to designate critical generation facilities. Likewise, MISO maintains that criteria 1.3, 1.8, and 1.9 place undue burden on transmission authorities/coordinators, and transmission planners by requiring them to designate facilities as Critical Assets. ISO/RTO Council and MISO believe that these authorities have insufficient guidance or data to designate facilities as Critical Assets. ISO/RTO Council and MISO are concerned that these entities should be entitled to shift compliance obligations from the entities to make designations does not provide clarifying notes on the intent and rationale of the criteria in CIP–002–4. It explains in its petition that “[i]n specifying a 15-minute qualification, Requirement R2 includes only those Cyber Assets that would have a real-time impact on the reliable operation of the Bulk Electric System.” Further, NERC explains that there may be generation facilities that, “while essential to the reliability and operability of the generation facility, may not have real-time operational impact within the specified real-time operations impact window of 15 minutes,” such as a cyber asset controlling the supply of coal fuel in a generation facility. We believe that NERC has provided adequate explanation and justification of this provision. To the extent that Hydro-Quebec seeks specific advice on how to implement the Requirement, Hydro-Quebec should raise the issue with the relevant Regional Entity or NERC.

34. With respect to Hydro-Quebec’s comment that the term “Flexible AC Transmission System (FACTS)” should be defined in the NERC Glossary of Terms, the Commission observes that the term is defined in the North American Energy Standards Board (NAESB) Wholesale Electric Industry Glossary, which is recognized in the NERC Rules of Procedure as a reference. Moreover, Hydro-Quebec’s comment does not suggest a lack of understanding of what the term means such that Hydro-Quebec could not apply criterion 1.9.

35. The Commission disagrees with NV Energy’s comments that the bright line criteria lack a technical justification because they are primarily based on asset size. While it is true that the standard establishes thresholds based on asset size, NERC articulated a basis for those values. For example, for the 1500 MW threshold in criterion 1.1, the petition states that the standard drafting team derived that number “from the most significant Contingency Reserves operated in various Balancing Authorities in all regions * * * [u]sing this number and data reported by the U.S. Energy Information Administration [], the team determined that approximately 146 generators in the United States would be classified as Critical Assets using this criterion.” This accounts for 29 percent of the installed generator capacity in the United States.” Moreover, as discussed above, the 15-minute trigger in CIP–002–4, Requirement R2, is a qualification to the asset size thresholds in criterion 1.1 and is meant to include only “Cyber Assets that would have a real-time impact on the reliable operation of the Bulk Electric System.” Considering the ERO’s pleadings and affording due weight to the ERO’s technical expertise, the

---

29 ISO/RTO Council at 6.
30 MISO Comments at 5.
31 Id. at 7.
32 Id. at 8.
33 ISO/RTO Council Comments at 13.
34 NERC Petition at 9 (citing Rationale and Implementation Reference Document, http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean_20101220.pdf), The Rationale and Implementation Reference Document, dated December 2010, was also submitted as part of the NERC filing. As found on the Commission’s eLibrary system in Docket No. RM11–11–00, the Rationale and Implementation Reference Document is found in Exhibit E (Development Record of the proposed CIP Reliability Standard and the associated Implementation Plans) beginning at page 2141 of the PDF electronic file submitted by NERC. This Final Rule refers to the page numbers used within the Rationale and Implementation Reference Document. The Rationale and Implementation Reference Document states that it “provides guidance for Responsible Entities in the application of the criteria in CIP–002–4, Attachment 1. It provides clarifying notes on the intent and rationale of the Standards Drafting Team. It is not meant to augment, modify, or nullify any compliance requirements in the standard.” Rationale and Implementation Reference Document at 1.
35 NERC Petition at 12.
36 Id.
37 NERC Petition at 15.
38 Id.
39 Available at www.naesb.org/pdf/ wg9_glossary072604v3.doc.
41 NERC Petition at 15.
42 Id. at 12.
Commission accepts the ERO’s justification for approval of the bright line criteria in Attachment 1.\(^{43}\)

36. The Commission disagrees with MISO’s and ISO/RTO Council’s comment that criteria 1.3, 1.8, and 1.9 require reliability coordinators, planning coordinators/authorities, and transmission planners to review a registered entity’s Critical Asset list or designate assets as Critical Assets. Instead, these criteria use the product of planning actions taken by reliability coordinators, planning coordinators/authorities, and transmission planners pursuant to other non-CIP Reliability Standards—these planning actions are, put simply, not made in conjunction with the application of CIP–002–4. The Commission also disagrees with MISO and ISO/RTO Council’s comments that reliability coordinators, planning coordinators, and transmission planners should have the same liability protection as an entity externally reviewing Critical Asset lists, as was discussed in Order No. 706–A.\(^{44}\)

37. Criteria 1.3, 1.8, and 1.9 require a responsible entity to identify generation and transmission facilities as Critical Assets when they have been determined as “nursery to avoid BES Adverse Reliability Impacts in the long-term planning horizon” (criterion 1.3) or “critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies” (criteria 1.8 and 1.9).

38. First, this is not a discretionary action based on what a reliability coordinator, planning coordinator/authority, or transmission planner subsequently considers “necessary” to avoid adverse impacts. Rather, reliability coordinators, planning coordinators/authorities, and transmission planners make these underlying determinations as part of their compliance obligations associated with other (non-CIP) Reliability Standards. NERC developed a Rationale and Implementation Reference Document that provides guidance on implementation of the Attachment 1 criteria and supports our finding. This reference document associates criterion 1.3 with Reliability Standards TPL–003 and TPL–004: “If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, such as due to a category C3 contingency as defined in TPL–003 or a category D contingency as defined in TPL–004, then that unit must be classified as a Critical Asset under criterion 1.3.”\(^{45}\) Similarly, the Rationale and Implementation Reference Document associates criteria 1.8 and 1.9 with Reliability Standard FAC–014–2: “Parts 1.8 and 1.9 include those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC–014–2, Establish and Communicate System Operating Limits, R3.1.1 and R3.1.3.”\(^{46}\)

39. Second, during development of the Version 4 CIP Reliability Standards, the standard drafting team addressed this issue in responding to a comment concerning criteria 1.3 that “[n]o entity should be able to simply ‘designate’ another as having critical assets.”\(^{47}\) The standard drafting team responded by stating that “[t]he burden for identifying Critical Assets is with the Responsible Entity that is the asset owner * * * [t]he Planning Authority and/or Transmission Planner are not designating the asset as critical for CIP purposes; they are determining the unit to be necessary to avoid Adverse Reliability Impacts based on other NERC reliability standards.”\(^{48}\)

40. Third, transmission planners and planning authorities/coordinators cannot have a compliance obligation to designate Critical Assets under Reliability Standard CIP–002–4 because they are not identified as Applicable Entities under the Reliability Standard.\(^{49}\)

41. In sum, under CIP–002–4, the responsible entity is required, and thus bears the compliance obligation, to apply the bright line criteria in Attachment 1 of CIP–002–4 to designate Critical Assets. We therefore reject the contention that reliability coordinators, planning coordinators/authorities, and transmission planners designate Critical Assets under the bright line criteria. We also disagree that CIP–002–4 imposes an undue burden on reliability coordinators, planning coordinators/authorities, and transmission planners because, as discussed above, determining whether an asset is “necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon” (criterion 1.3) or “critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies” (criteria 1.8 and 1.9) is true that those determinations will be used by responsible entities when applying the bright line criteria in CIP–002–4. However, as discussed above, the responsible entities, and not planning coordinators and transmission planners, are ultimately responsible for compliance with the CIP Reliability Standards. Accordingly, we reject MISO and ISO/RTO Council’s suggestion to direct NERC to develop an appeals process for determinations made by planning coordinators and transmission planners in the context of other Reliability Standards in this final rule approving the Version 4 CIP Reliability Standards.

2. Blackstart/Must Run Units

NERC Petition

42. Reliability Standard CIP–002–4, criterion 1.3 designates as a Critical Asset: “Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.” Reliability Standard CIP–002–4, criterion 1.4 designates as a Critical Asset: “Each Blackstart Resource identified in the Transmission Operator’s restoration plan.”

Comments

43. ISO/RTO Council comments that criterion 1.4 pertaining to blackstart resources appears to conflict with the NERC Statement of Registry Criteria. ISO/RTO Council observes that while criterion 1.4 identifies as a Critical Asset “[e]ach Blackstart Resource identified in the Transmission Operator’s restoration plan”...
plan.” The Registry Criteria provide for registration of “any generator, regardless of size, that is a blackstart unit material to and designated as part of a transmission operator entity’s restoration plan * * *.”

ISO/RTO Council suggests that “some Regional Entities may have determined that certain blackstart units are not material to the Transmission Operator’s restoration plan, and are therefore, presumably not covered” by the Reliability Standards. Thus, ISO/RTO Council seeks clarification whether criterion 1.4 is meant to apply to blackstart units “covered” by the Registry Criteria or all blackstart resources and, if the latter, whether a revision to the Registry Criteria is appropriate.

45. MISO comments that designating must run units as Critical Assets pursuant to criterion 1.3 may create an incentive for generation owners and generation operators to remove such units from service prior to their designation as Critical Assets. Commission Determination

46. With regard to ISO/RTO Council’s comments, we note that NERC developed the Registry Criteria to identify users, owners and operators of the bulk electric system that are candidates for compliance registration. NERC does not apply the Registry Criteria to register particular assets. Moreover, whether NERC should revise the Registry Criteria is beyond the scope of this proceeding.

47. That being said, it is not clear to us whether any substantive distinction is to be made between criterion 1.4, which implicates each blackstart resource identified in a restoration plan, and the Registry Criterion, which identifies as a candidate for registration the owner or operator of “a blackstart unit material to and designated as part of a * * * restoration plan.” We leave it to NERC to consider whether a blackstart unit identified in a transmission operator’s restoration plan could ever be considered immaterial to that plan and, if so, whether a clarification or revision to one or more documents is appropriate.

48. We disagree with MISO that designating a “must run” unit as a Critical Asset may create an incentive for generation owners and generation operators to remove units from service prior to their designation as Critical Assets. The Commission is willing to consider rate filings to address this concern. For example, the Commission conditionally accepted a proposal filed by PJM to allow generators to recover costs related to compliance with mandatory NERC CIP Reliability Standards. Specifically, the Commission conditionally approved PJM’s proposal in order to provide additional means for blackstart service providers to recover incremental costs associated with providing blackstart service. Finally, MISO can compensate “must run” generation units under System Support Agreements to prevent generators deemed as “must run” from being removed from service.

3. Control Centers/Control Systems

NERC Petition

48. Reliability Standard CIP–002–4, criteria 1.14–1.17 define the control centers and backup control centers that are treated as Critical Assets. Specifically, criterion 1.14 identifies as a bright line for Critical Assets “[e]ach control center or backup control center used to perform the functional obligations of the Reliability Coordinator.” Criterion 1.15 pertains to control centers or backup control centers used to control generation at multiple plant locations equal to or exceeding 1500 MW. Criteria 1.16 and 1.17 include as Critical Assets control centers or backup control centers used to perform the functional obligations of transmission operators and balancing authorities, respectively.

NPPR

49. In the NOPR, the Commission expressed concern, based on survey data supplied by NERC, that the Reliability Standard CIP–002–4 criteria would still leave a significant number of control centers unprotected.

Comments

50. Commenters hold diverging views on whether the Version 4 CIP Reliability Standards adequately protect control centers and control systems (i.e., control systems not housed in control centers). G&T Cooperatives believe that Version 4 goes too far, while SPP RE and, to a lesser extent, MISO believe that it does not go far enough. NERC, PG&E, and the Trade Associations acknowledge the NOPR’s concern that CIP Version 4 does not protect some control centers/common control systems, but they anticipate that a future Version 5 CIP Reliability Standards will protect more Critical Assets. G&T Cooperatives believe that the Version 4 bright line criteria need additional work, which is why they support allowing a future Version 5 to supersede Version 4 before it becomes effective. Specifically, G&T Cooperatives state that criteria 1.14, 1.16, and 1.17 “sweep in control centers and backup control centers, without regard to their size or potential impact on the [bulk electric system].” G&T Cooperatives maintain that the bright line criteria should be revisited to ensure that they capture only those assets that should be covered in order to protect bulk electric system reliability.

52. SPP RE states that criteria 1.14–1.17 are insufficient because they do not consider interconnectivity of control centers or address the possibility that a small network-connected control center not deemed a Critical Asset could be used to compromise larger control centers. SPP RE believes that, at a minimum, all balancing authority and transmission operator control centers should be declared Critical Assets. SPP RE also encourages the Commission to consider requiring NERC to modify the bright line criteria to classify a control center as a Critical Asset if it is network-connected to other control centers.

53. With respect to common control systems, SPP RE believes that individual resources that do not qualify as Critical Assets under the bright line criteria can still pose a reliability risk if they have a common control system. SPP RE notes that under Version 4, a registered entity must designate its control center or generation facility as a Critical Asset in order to bring an associated common control system into scope. SPP RE believes that the bright line criteria may not ensure that all common control systems are identified, however. Criterion 1.1 designates as Critical Assets groups of generating units at a single plant location with an aggregate highest rated net Real Power capability equal to or exceeding 1500 MW. Criterion 1.15 designates as Critical Assets: “Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of facilities.”
generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1,500 MW in a single Interconnection.” SPP RE states that criterion 1.1 adequately protects the common control systems of generating units at a single plant location with aggregate real power equal to or exceeding 1,500 MW. However, SPP RE believes that criterion 1.15 does not clearly apply to control centers and common control systems that control generation that equals or exceeds 1,500 MW in the aggregate regardless of the individual plant size requirements set forth in criterion 1.1.65

54. MISO expresses concern with Version 4’s treatment of control centers. MISO asks for clarification whether Version 4 intentionally omitted “data centers” associated with control centers from the bright line criteria and whether registered entities have the discretion to designate them as Critical Assets. Because control centers often work in tandem with an associated data center, MISO recommends allowing registered entities to designate data centers as Critical Assets.66

55. NERC and PG&E acknowledge the NOPR’s concern that Version 4 does not fully address the Order No. 706 directives pertaining to control centers. NERC and PG&E temper this concern, however, by pointing to the lack of an accepted definition of “control centers” and the fact that some control centers in the generation context only communicate with generators that fall below the NERC Registration Criteria for generators. NERC and PG&E suggest that cyber assets at these generator locations are unlikely to have a greater impact on reliability than much larger single-unit generators merely because the smaller units have a control center. In any case, NERC and PG&E explain that under a future Version 5 every control center will be protected and will receive a “medium” or “high” level of security under a new three-tiered structure. Further, NERC and PG&E state that several Version 5 requirements will apply to control centers regardless of whether they are classified as medium or high.67 NERC also states that “cyber misuse” will be a consideration under the classification process in CIP Version 5 and that the CIP Version 5 drafting team has proposed a definition of “control center.”68

56. The Trade Associations likewise recognize the NOPR’s concern regarding control centers but state that control centers and control systems are being considered in the Version 5 project. The Trade Associations also state that appropriate prioritization and tailored application of mandatory requirements will be needed in addressing control centers and control systems given the widely varying circumstances and configurations in which these facilities are used.69 Commission Determination

57. The Commission recognizes the diverging views among commenters regarding the protection of control centers and control systems afforded under the Version 4 CIP Reliability Standards. In Order No. 706, we stated that “it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a critical asset.”70 The Commission maintains this view. However, as we observed in the NOPR, the percentage of control centers to be identified as Critical Assets under Version 4 is 74 percent, which is an improvement over the number currently identified under Version 3.71 Therefore, it is reasonable to approve Version 4 because it will ensure that more control centers are identified as Critical Assets than are identified under Version 3. However, we continue to expect comprehensive protection of all control centers and control systems as NERC works to comply with the requirements of Order No. 706.

58. We agree with SPP RE that the CIP Reliability Standards should consider interconnectivity of control centers and the strategy of classifying a control center as a Critical Asset if it is network-connected to other control centers. The Commission also finds merit in MISO’s comment that responsible entities should be allowed to designate data centers as Critical Assets because of their inherent connectivity to the control centers or control systems they support. Therefore, we expect NERC to address these approaches as it works to comply with the requirements of Order No. 706.72

C. NOPR Questions on Critical Asset Identification

1. Flexibility To Identify Critical Assets That Fall Outside of the CIP Version 4 Bright Line Criteria

59. In the NOPR, the Commission stated that under the currently-effective Reliability Standard CIP–002–3, a responsible entity that applies its risk-based assessment methodology considers specific types of assets identified in Requirement R1, as well as “any additional assets that support the operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.”73 The Commission invited comment on whether a registered entity retains the same flexibility under Version 4 to identify assets that, although outside of the bright line criteria for identifying Critical Assets, are essential to Bulk-Power System reliability.

Comments

60. NERC states that, in developing Version 4, the drafting team considered adding criteria that would allow entities to identify additional facilities falling outside of the bright line criteria, but determined not to include the provision. However, NERC adds that “registered entities are permitted to apply any or all of the requirements in the CIP standards to assets that do not meet the bright-line thresholds.”74

61. The Trade Associations and FirstEnergy believe that registered entities do not have the flexibility to identify Critical Assets that fall outside the bright line criteria such that they would be subject to mandatory and enforceable compliance obligations and should not have such flexibility because it would detract from the consistency afforded by the bright line criteria.75 The Trade Associations, however, state that registered entities have the discretion to identify facilities as Critical Assets provided those facilities are not subject to compliance obligations.76

62. PG&E comments that appropriate flexibility exists under Version 4 to allow the identification of Critical Assets essential to the bulk electric system. In particular, PG&E cites to criterion 1.3, which would require a planning coordinator or transmission planner to identify a generation facility

---

65 Id. at 6–7.
66 MISO Comments at 10–11.
68 Id. at 15.
69 NERC Comments at 14–15; PG&E Comments at 13–14.
70 Order No. 706, 122 FERC ¶ 61,040 at P 280.
71 NOPR, FERC Stats. & Regs. ¶ 32,679 at P 23.
72 See, e.g., Order No. 706, 122 FERC ¶ 61,040 at PP 280–281.
74 NERC Comments at 4.
75 Trade Associations Comments at 4–5; FirstEnergy Comments at 2.
76 Trade Association Comments at 5.
as "critical" if "necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Likewise, PG&E believes that criterion 1.8 provides that a reliability coordinator, planning authority, and transmission planner has authority to designate certain transmission facilities critical to the derivation of IROGs as critical. PG&E also believes that industry should be encouraged to apply any or all of the CIP Reliability Standards to assets that do not meet the bright line criteria, "even beyond a compliance and audit program."76

63. SPP RE encourages the Commission to require NERC to restore the "other" criterion to the bright line criteria.77 MISO likewise believes that registered entities should have the flexibility to identify more Critical Assets because the bright line criteria create a minimum regulatory floor on which to build.78

2. NERC or Regional Entities’ Ability To Identify Critical Assets That Fall Outside of the CIP Version 4 Bright-Line Criteria

NERC Petition

64. In the NOPR, the Commission invited comment on whether NERC and/or Regional Entities would have the ability, either in an event-driven investigation or compliance audit, to identify specific assets that fall outside the bright-line criteria yet are still essential to Bulk-Power System reliability and should be subject prospectively to compliance with the CIP Reliability Standards, and if so, on what basis should that decision be made.79

Comments

65. NERC states that the Version 4 CIP Reliability Standards are an interim step and that the future Version 5 CIP Reliability Standards will refine the bright line criteria, with the intent of categorizing assets (to be termed "BES Cyber Systems") as low, medium or high impact to Bulk-Power System reliability. NERC states that, in the interim, it has the authority under Section 810 of the NERC Rules of Procedure to issue an Alert to recommend specific actions. According to NERC, it can use the Alerts "as a tool to address assets that NERC and Regional Entities later determine should be treated as critical but to not fall into the CIP Version 4 criteria."80

66. The Trade Associations, Dominion, FirstEnergy and other commenters oppose identification of Critical Assets outside of the bright line process by NERC or Regional Entities as detracting from the clarity afforded by the bright line criteria. The Trade Associations and Tallahassee opine that the Commission should not undermine the bright line criteria by granting Regional Entities discretion to designate Critical Assets that are otherwise excluded by application of the bright line criteria.81 SPP RE states that it is not appropriate to apply arbitrarily criteria not found in the CIP Reliability Standards to require additional cyber systems to be subject to the CIP Reliability Standards.82 Dominion states that if such a mechanism is necessary, it should not be done in the compliance audit context.83

67. MISO supports review of Critical Asset designations by NERC and Regional Entities, given its belief that criteria 1.3, 1.8, and 1.9 require reliability coordinators, planning authorities/authorities and transmission planners to identify certain Critical Assets. MISO maintains that the lack of guidance for applying these criteria leaves room for substantial discretion, which may undermine the consistent identification of Critical Assets absent Regional Entity or NERC review.84

Commission Determination

68. We agree with NERC and others that registered entities can voluntarily apply any or all of the requirements in the CIP Reliability Standards to assets that fall outside the bright line criteria.85 As MISO described it, Version 4’s bright line criteria establish a “regulatory floor” for cybersecurity, which must be followed by all registered entities.86 Nothing in Version 4 prevents registered entities from applying the protections required by the CIP Reliability Standards to additional assets that they deem critical. At the same time, we agree that assets not identified by the bright line criteria are not subject to a compliance obligation or to addition by the Commission, NERC, or a Regional Entity. We are persuaded that the clarity and addition of Critical Assets effected by the bright line criteria render Version 4 an improvement over Version 3.

69. We expect NERC to continue to work towards a version of the CIP Reliability Standards that will largely eliminate the risk of gaps in the identification of Critical Assets.87 In Section E of this Final Rule, we discuss the directive in Order No. 706 regarding external review in an effort to provide the ERO with guidance in developing future versions of the CIP Reliability Standards.

D. Implementation Plan

NERC Petition

70. NERC proposed an implementation plan for existing Critical Assets and an implementation plan for newly identified Critical Assets and newly registered entities. For existing Critical Assets, NERC proposed an effective date for full compliance with the Version 4 CIP Standards of the first day of the eighth calendar quarter after applicable regulatory approvals have been received. The implementation plan for newly identified Critical Assets and newly registered entities specifies how responsible entities are to handle newly identified Critical Cyber Assets, as well as how newly registered entities are to implement the CIP Reliability Standards after the effective date for Version 4.

NOPR

71. In the NOPR, the Commission proposed to approve both the effective date and the implementation plan for CIP-002–4 based upon a belief that the proposed implementation plan establishes reasonable deadlines for industry compliance.88

Comments

72. Comments varied regarding NERC’s proposed implementation plan. NERC, PG&E and Exelon support the CIP Version 4 implementation plan. PG&E comments that the two year time frame, commencing from Commission approval, is reasonable. The Trade Associations support the implementation plan. However, they also urge the Commission to avoid a “one size fits all” approach, explaining that there are “complexities” of implementing “[CIP Versions] 3 to 4 to 5.”89 According to the Trade Associations, some entities may face significant challenges as the result of approval of Version 4 potentially followed so closely in time by the approval of Version 5.

---

73 PG&E Comments at 5.
74 Id.
75 SPP RE Comments at 5.
76 MISO Comments at 11.
77 NOPR, FERC Stats. & Regs. ¶ 32,679 at P 31.
78 SPP RE Comments at 5.
79 MISO Comments at 11.
80 NERC Comments at 4–7.
81 Trade Association Comments at 5–6; Tallahassee Comments at 4–5.
82 SPP RE Comments at 4.
83 Dominion Comments at 4–5.
84 MISO Comments at 4.
85 NERC Comments at 4.
86 MISO Comments at 4.
87 NERC Petition at 4.
89 Trade Associations’ Comments at 13.
Associations ask for coordination among NERC, the regions and registered entities to achieve compliance in an efficient and orderly manner. NERC and Exelon acknowledge that there could be concerns with implementing CIP Version 5 soon after Version 4 becomes effective, but note that CIP Version 5-related implementation issues could be revisited after CIP Version 5 is filed.\footnote{NERC Comments at 10; Exelon Comments at 3.}

73. G&T Cooperatives, ISO/RTO Council, SPP RE, ITC, Dominion, and FirstEnergy oppose and/or recommend modifying the CIP Version 4 implementation plan in anticipation of a future CIP Version 5 filing. G&T Cooperatives state that CIP Version 4 should be approved for “guidance purposes” only, thus delaying implementation, so that it may be superseded by CIP Version 5.\footnote{G&T Cooperatives Comments at 10.} G&T Cooperatives believe that CIP Version 5 should become effective on the date that CIP Version 4 would otherwise become effective. Therefore, G&T Cooperatives believe that NERC no longer intends that CIP Version 4 should go into effect in advance of CIP Version 5.

74. ISO/RTO Council asks that the Commission provide guidance to NERC on how to exercise discretion on enforcement and implementation issues given the potential overlap and possible conflict with CIP Version 5.\footnote{ISO/RTO Council Comments at 15.} SPP RE suggests that the Commission allow entities to “early adopt” CIP Version 5.\footnote{SPP RE Comments at 7.} ITC recommends keeping CIP Version 4 in effect for at least three years so registered entities can collect a full three-year audit cycle’s worth of data, which would avoid “frequent and abrupt changes” and could help later when implementing CIP Version 5.\footnote{ITC Comments at 4.}

94. In its reply comments, NERC reiterates that it supports implementation of CIP Version 4 as filed. NERC rejects the G&T Cooperatives’ suggestion that NERC no longer intends that CIP Version 4 should go into effect in advance of CIP Version 5. NERC states that it recognizes the concerns raised by industry regarding the interplay between CIP Version 4 and CIP Version 5. However, NERC states that “until CIP Version 5 and an appropriate implementation plan is fully vetted and approved by the industry, the NERC Board of Trustees, and FERC, there is no basis to determine at this juncture that the CIP Version 4 standards should not be implemented.”\footnote{NERC Reply Comments at 3.}

Commission Determination

76. The Commission adopts the NOPR proposal and approves both the effective date and the implementation plan for CIP–002–4 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. The comments opposing NERC’s proposed implementation plan for CIP–002–4 are all based upon concerns that the approval of CIP Version 4 may be followed very closely in time by a future Version 5 of the CIP Reliability Standards. We understand the commenters’ interest in careful coordination, so that the industry can achieve compliance in an efficient and orderly manner as the industry moves from Version 3 to Version 5, via the interim Version 4. These concerns, however, do not provide a basis on which to reject the NOPR proposal.

77. While G&T Cooperatives, ISO/RTO Council, SPP RE, ITC, Dominion, and FirstEnergy outline various proposed solutions to a potential overlap between CIP Version 4 and a future Version 5 of the CIP Reliability Standards, the commenters ignore one critical fact—the only version of the CIP Reliability Standards at issue in this proceeding is Version 4. There is no proposed Version 5 of the CIP Reliability Standards before the Commission at this time, so any concerns raised about implementation of Version 5 are beyond the scope of this proceeding. To the extent that the development of Version 5 raises actual implementation concerns, such concerns should be raised when NERC submits Version 5 for approval. This proceeding is not the appropriate forum to determine how to coordinate the implementation of the CIP Version 4 Reliability Standards with possible future versions of the CIP Reliability Standards that have not yet been developed or submitted for approval to the Commission.

E. Compliance With Order No. 706

78. In the petition, NERC stated that the standard drafting team “limited the scope of requirements in the development of CIP–002–4 through CIP–009–4 as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236.”\footnote{NERC Petition at 6.} NERC further stated that the standard drafting team is continuing its effort to address the remaining outstanding Order No. 706 directives. NERC explained that its phased approach to meeting the Order No. 706 directives has “consistently built upon prior versions of the CIP–002 through CIP–009 standards to enhance the reliability of the Bulk Electric System.”\footnote{Id.} In that light, the Commission discussed certain outstanding Order No. 706 directives in the NOPR and proposed giving guidance to aid in the development of the next version of the CIP Reliability Standards.

79. In their comments, the Trade Associations seek clarification as to whether the issues discussed in Section B of the NOPR (i.e., connectivity, control centers, and NERC and Regional Entity review of Critical Asset lists) should be viewed merely as encouragement to address those issues in CIP Version 5 or as new directives beyond what was required in Order No. 706.\footnote{Trade Association Comments at 10.} The Trade Associations explain that it is their expectation that the final rule will not include any further directives. Instead, the Trade Associations encourage the Commission to allow development of CIP Version 5 to move forward without introducing any new uncertainties in a final rule on CIP Version 4. Based on the comments in response to the NOPR, we determine not to issue new directives at this time beyond what is required to comply with Order No. 706. Consistent with the NOPR proposal, we provide guidance for future versions of the CIP Reliability Standards regarding the issues of connectivity, application of the National Institute of Standards and Technology (NIST) Framework, and provision of a regional perspective.

1. Connectivity

NOPR

80. In the NOPR, the Commission stated that:

In light of recent cybersecurity vulnerabilities, threats and attacks that have exploited the interconnectedness of cyber systems, the Commission seeks comments regarding the method of identification of Critical Cyber Assets to ensure sufficiency and accuracy. The Commission recognizes that control systems that support Bulk-Power System reliability are “only as secure as their weakest link,” and that a single vulnerability opens the computer network and all other networks with which it is interconnected to potential malicious activity. Accordingly, the Commission believes that any criteria adopted for the
purposes of identifying a Critical Cyber Asset under CIP–002 should be based upon a Cyber Asset’s connectivity and its potential to compromise the reliable operation of the Bulk-Power System, rather than focusing on the operation of any specific Critical Asset(s). [Footnotes omitted.] 108

The Commission invited comment on this approach.

Comments

81. NERC comments that, while it does not believe that the connectivity issue was raised in Order No. 706, the CIP Version 5 standards drafting team recognizes the importance of the matter and is considering it in the development of Version 5. 101 However, NERC does not believe that connectivity can be addressed in CIP Version 5 by the time it is submitted to the NERC Board of Trustees for approval. 102 NERC notes that CIP Version 5 will eliminate the blanket exemption for non-routably connected cyber systems, “and instead mov[e] the connectivity attribute to specific requirements.” 103 NERC adds that the CIP Version 5 drafting team has proposed to apply electronic security perimeter protections “of some form” to include all bulk electric system Cyber Systems. 104

82. SPP RE states that neither CIP Version 4 nor CIP Version 5 consider all possible communication paths between a given cyber asset and any assets that support a reliability function. According to SPP RE, the Version 4 standards define bright line criteria based on size of the asset, and the draft Version 5 standards would rate cyber systems based on their span of control, but fail to consider interconnectivity and the potential for a small system to be used as a vector of attack against other systems. 105 SPP RE explains that control center cyber systems routinely exchange data with reliability coordinators, over wide area networks. 106

83. ISO/RTO Council states that the Commission’s concerns with connectivity could be addressed by requiring certain asset owners and operators to take a “mutual distrust” posture. 107 MISO supports considering the connectivity issue but also encourages the Commission to evaluate the costs and benefits of this approach.

84. PG&E states that issues pertaining to connectivity are being addressed in

CIP Version 5. 108 The Trade Associations state that they understand the Commission’s concerns regarding connectivity. But taken together with the NOPR’s “weakest link” statements, the Trade Associations are concerned these views could imply that everything needs to be protected. 109 The Trade Associations believe that the “weakest link” concept articulated in the NOPR needs to be fleshed out in more detail and that Commission staff should work with the CIP Version 5 standard drafting team to discuss these issues. The Trade Associations also maintain that the CIP Version 5 standard drafting team is currently working on addressing the Commission’s directives in Order No. 706 and that no further directives regarding connectivity, or otherwise, should be made in the final rule approving CIP Version 4. According to the Trade Associations, any directives in the final rule would serve to prejudge CIP Version 5.

Commission Determination

85. The Commission appreciates the comments on whether cyber connectivity should be a basis for the identification of Critical Cyber Assets, or their equivalent, in future versions of the CIP Reliability Standards. We have raised concerns relating to the use of cyber connectivity as a basis for applying the CIP Reliability Standards during and since the approval of Version 1. For example, in Order No. 706, we stated that “[NERC’s compliance with the CIP Reliability Standards] is necessary in light of its interconnectivity with other entities that own and operate critical assets.” 110 Similarly, in finding that an “N minus 1” criterion is not an appropriate risk-based assessment methodology for identifying Critical Assets, we noted that a cyber attack can strike multiple assets simultaneously. 111 The cyber connectivity of Bulk-Power System assets increases the risk of a multiple asset cyber attack. The CIP Reliability Standards should reflect this risk. 86. In that light, we support the elimination of the blanket exemption for non-routably connected cyber systems as highlighted in NERC’s comments. 112 A continued blanket exemption in Version 5 would not adequately address risk.

87. In addition, we support the concept of applying electronic security perimeter protections “of some form” to all bulk electric system cyber systems. 113 Because electronic communications between functional entities and their associated systems are essential to the operation of the Bulk-Power System, it is important for each distinct system to be protected at its boundary by an electronic security perimeter. The use of electronic security perimeters, as required under the CIP Reliability Standards, is commonly referred to as zoned security in the information security industry. 114 Security zones are established to ensure that a compromise in one security zone does not lead to a compromise in another security zone across a security perimeter. 115 The Commission is encouraged by NERC’s comments that its standard drafting team is considering ways to address connectivity issues and electronic perimeter protections surrounding all BES Cyber Systems. 88. We also agree with SPP RE that the CIP Reliability Standards should consider communication paths between a given cyber asset and other assets that support a reliability function. 116 As noted by SPP RE, “control center BES Cyber Systems routinely exchange operational data with each other as required by NERC Reliability Standard TOP–005–1.” 117 As further noted by SPP RE, “connectivity is important to address because of the required communications from control centers to and between reliability coordinators under the Interconnection Reliability Operations and Coordination Standards.” 118 The Commission agrees that cyber connectivity is important to address

100 NOPR, FERC Stats. & Regs. ¶ 32,679 at P 43.
101 NERC Comments at 11.
102 Id.
103 Id.
104 Id.
105 Id.
106 Id. at 3–5.
107 ISO/RTO Council Comments at 17.
108 PG&E Comments at 9.
109 Trade Associations Comments at 18.
110 Order No. 706, 122 FERC ¶ 61,040 at P 47.
111 Id. P 256.
112 NERC Comments at 11.
113 Id.
115 A “security perimeter” is defined by the ISA99 Committee on Industrial Automation and Control Systems Security as a “boundary (logical or physical) of the domain in which a security policy or security architecture applies, i.e. the boundary of the space in which security services protect system resources.” Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, ISA–99.00.01–2007.
116 SPP RE Comments at 3–4.
117 Id.
118 Id.
119 Id.
when developing future versions of the CIP Reliability Standards. That being said, we acknowledge the concern of Trade Associations that the “connectivity” and “weakest link” concepts could possess different meanings to various stakeholders.\textsuperscript{120} Thus, addressing connectivity should include reaching a common understanding of the term. Further, we understand and agree with the Trade Associations’ concern that protection should be applied in a reasonable manner.\textsuperscript{121}

89. Recognizing the importance of addressing cyber connectivity in future versions of the CIP Reliability Standards, we encourage NERC to consider the benefits of a “mutual distrust” posture, or similar strategies, put forth by the ISO/RTO Council\textsuperscript{122} and as directed by the Commission in Order No. 706.\textsuperscript{123} In Order No. 706, the Commission used the term “mutual distrust” to denote how “outside world” systems are treated by those inside the control system.\textsuperscript{124} Specifically, a mutual distrust posture requires each responsible entity that has identified critical cyber assets to protect itself and not trust any communication crossing an electronic security perimeter, regardless of where that communication originates.\textsuperscript{125}

90. Applying electronic security perimeter protections “of some form” to bulk electric system cyber systems covered by the CIP Reliability Standards will support the adoption of a “mutual distrust” posture. This posture will encourage asset owners and operators to employ sound network architectural design, thus segmenting their systems into distinct security zones protected by managed interfaces that will allow only trusted access. The managed interfaces, or electronic security perimeter access points, are intended to restrict or prohibit network access and information flow to bulk electric system cyber systems covered by the CIP Reliability Standards from unidentified, unauthenticated, and unauthorized connectivity to ensure security. Multiple electronic security perimeters can be established to protect cyber assets and adopted as part of a defense in depth strategy to limit the propagation of a threat.\textsuperscript{126}

91. Having considered the feedback to our question on cyber connectivity, we continue to believe that criteria adopted for the purpose of identifying Critical Cyber Assets under CIP–002 should include a cyber asset’s “connectivity” and its potential to compromise the reliable operation of the Bulk-Power System. Therefore, we expect Version 5 to address these issues.

2. Application of NIST Framework NOPR

92. In the NOPR, the Commission elaborated on the Order No. 706 guidance regarding the consideration of the NIST Framework when developing CIP Reliability Standards.\textsuperscript{127} The NOPR explained that the NIST Framework recognizes that all connected assets require a baseline level of protection to prevent attackers from gaining a foothold to launch further, even more devastating attacks on other critical systems.\textsuperscript{128} The Commission invited comment on this approach.

Comments

93. NERC, PG&E, SPP RE, and MISO support applying aspects of the NIST Framework to the CIP Reliability Standards, which could lead to more bulk electric system components being protected, though at different levels depending on their criticality. NERC and PG&E state that the CIP Version 5 standard drafting team has incorporated four key features of the NIST Framework into the CIP Version 5.\textsuperscript{129} NERC states, however, that the NIST standards/guidelines should not be adopted in total because elements of the NIST standards/guidelines, which are meant to be applied in all federal agencies to manage risks to their information systems in support of their unique missions, are inapplicable to the power sector.\textsuperscript{130} NERC and MISO point out that the NIST Framework allows for applicable NIST concepts to be tailored and incorporated into the CIP Reliability Standards, which has been the approach of the standard drafting team in developing CIP Version 5.

Commission Determination

94. The Commission finds the feedback provided on the potential application of the NIST Framework to the CIP Reliability Standards to be useful. We agree with the commenters that support applying applicable features of the NIST Framework to Version 5 of the CIP Reliability Standards. As stated in the NOPR, we believe that the NIST Framework could provide beneficial input into the CIP Reliability Standards.\textsuperscript{131} In its comments, NERC states that a standards drafting team is incorporating four key features of the NIST Framework into the Version 5 CIP Reliability Standards: (1) Ensuring that all BES Cyber Systems associated with the Bulk-Power System, based on their function and impact, receive some level of protection; (2) customizing protection to the mission of the cyber systems subject to protection; (3) applying a tiered approach to security controls that specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk-Power System; and (4) using the concept of the BES Cyber System.\textsuperscript{132} We view the approach of incorporating these applicable features of the NIST Framework into the CIP Reliability Standards as a positive step in improving cyber security for the Bulk-Power System.

95. NIST standards are used by industry generally as a reference and can be applied by the ERO to the Bulk-Power System.\textsuperscript{133} Therefore, we

\textsuperscript{120}Trade Associations Comments at 18.
\textsuperscript{121}Id.
\textsuperscript{122}ISO/RTO Council Comments at 17.
\textsuperscript{123}Order No. 706, 122 FERC ¶ 61,040 at P 412 (“The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity’s control system from the outside world.”).
\textsuperscript{124}Id. P 33.
\textsuperscript{125}Id. n.24.
\textsuperscript{126}“Defense in depth” is defined by the ISA99 Committee on Industrial Automation and Control Systems Security as the “provision of multiple security provisions, especially in layers, with the intent to delay if not prevent an attack. NOTE: Defense in depth implies layers of security and detection, even on single systems, and provides the following features: attackers are faced with breaking through or bypassing each layer without being detected; a flaw in one layer can be mitigated by capabilities in other layers; system security becomes a set of layers within the overall network security.” Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, ISA-99.00.01–2007.
\textsuperscript{127}Id.
\textsuperscript{128}NOPR, FERC Stats. & Regs. ¶ 32.679 at P 46–52.
\textsuperscript{129}Id. P 51.
\textsuperscript{130}NERC Comments at 13; PG&E Comments at 11–12.
\textsuperscript{131}Id. P 52.
\textsuperscript{132}NERC Comments at 12–13.
\textsuperscript{133}NOPR, FERC Stats. & Regs. ¶ 32.679 at P 46.
\textsuperscript{134}Id. Comments at 13–14. NERC comments that the next version of the CIP Reliability Standards replaces the identification of “Critical Assets” with the categorization of “BES Cyber Systems.” Specifically, NERC states that “BES Cyber Systems will be characterized as ‘High Impact,’ ‘Medium Impact,’ or ‘Low Impact’ based on the impact of the cyber system to the reliable operation of the bulk power system * * * [t]his characterization makes use of a bright-line concept similar to Version 4, but requires responsible entities to determine the impact of loss, compromise or misuse of a given BES Cyber System using a bright-line impact filter.” NERC Comments at 7.
\textsuperscript{135}For example, NIST SP800–82 provides a detailed Guide to Industrial Control Systems Security that is relevant to the electric power industry. Specifically, NIST SP800–82 includes recommendations to assist in the protection of Supervisory Control and Data Acquisition systems, Distributed Control Systems, and other control system configurations such as Programmable Logic

Continued
continue to encourage NERC and industry to include aspects of the NIST Framework and standards into subsequent versions of the CIP Reliability Standards to better protect the Bulk-Power System. Similar to our approach in Order No. 706, we continue to urge NERC to look to relevant NIST standards for guidance in developing effective cybersecurity standards for the electric industry.134

3. Regional Perspective

NORP

96. In the NORP, the Commission highlighted the Order No. 706 directive for NERC to “develop a process of external review and approval of critical asset lists based on a regional perspective.”135 The NORP explained the Commission’s concern that a lack of a regional review of a registered entity’s identification of cyber assets might result in a reliability gap. In addition, the Commission discussed concerns regarding cyber systems spanning multiple regions:

“This problem may be exacerbated by any future revisions to the CIP Reliability Standards that opt to reserve a high level of independent authority to the registered entity to categorize and prioritize its cyber assets. Looking forward, it will be essential for NERC and the Regional Entities to actively review the designation of cyber assets that are subject to the CIP Reliability Standards, including those which span regions, in order to determine whether additional cyber assets should be protected.136

Comments

97. NERC states that the bright line criteria adopted under Version 4 of the CIP Reliability Standards provide certainty and clarity as to the assets that should be identified as critical. NERC explains that the CIP Reliability Standard drafting team is further refining the bright line criteria and anticipates that the next version of the CIP Reliability Standards will characterize “BES Cyber Systems” (in lieu of cyber assets) with “high,” “medium,” or “low” impact on Bulk-Power System reliability. According to NERC, “[t]his characterization makes use of a bright line concept similar to Version 4, but requires responsible entities to determine the impact of loss, compromise or misuse of a given BES Cyber System using a bright line impact filter.” 137

98. The Trade Associations state that they cannot support the NORP proposal on redesignation of assets based on a “regional view” without specific information about the mechanics of the proposal or the nature of the perceived reliability gap. According to the Trade Associations, registered entities are in the best position to determine which of their cyber assets are critical to the operation of Critical Assets and therefore subject to CIP compliance. The Trade Associations contend that NERC and the Regional Entities have the opportunity to review a registered entity’s approach to developing its list of Critical Cyber Assets in the context of a compliance audit or other compliance monitoring process.

99. FirstEnergy states that the bright line criteria should be the sole methodology for identifying Critical Assets and that allowing the ERO or Regional Entities the ability to add assets that fall outside the bright line criteria undermines the purpose of the bright line criteria.138 Tallahassee states that the Commission should not undermine the value of the bright line criteria by granting the Regional Entities the discretion to designate assets as critical if the assets are not otherwise identified by the bright line criteria.139 SPP RE, for its part, states that it is not appropriate to apply arbitrarily criteria not listed in the CIP Reliability Standards to require additional cyber assets to be subject to the CIP Reliability Standards. SPP RE states that the appropriate way to address any concern that the bright line criteria do not capture all assets that should be protected is to modify the bright line criteria to address any deficiency.

 Commission Determination

101. In Order No. 706, the Commission explained the need for external review of the Critical Asset lists in the context of an earlier version of the CIP Reliability Standards that required registered entities to apply individualized risk-based methodologies to identify Critical Assets.130 Further, as indicated in the NORP in the immediate proceeding, the Commission’s concerns are “exacerbated by any future revisions to the CIP Reliability Standards that opt to reserve a high level of independent authority to the registered entity to categorize and prioritize its cyber assets.”140

102. We agree with commenters that the adoption of appropriate, bright line criteria for Critical Asset identification may obviate the need for an external review. We believe that there is less need for external review where application of bright line criteria results in an objective, consistently applied approach to the identification of cyber assets. As discussed above, NERC anticipates the development of tiered, bright line criteria in the next version of the CIP Reliability Standards. Whether this development ultimately eliminates the need for an external review process as directed in Order No. 706 will depend on the discretion allowed to individual registered entities in identifying and characterizing assets or systems.

103. However, even with the adoption of clear and objective criteria, we believe that there remains a need for an entity with a regional perspective, presumably the ERO or a Regional Entity, to have the opportunity to identify or adjust the characterization of cyber assets in some circumstances. For example, an event may reveal that a specific cyber asset has a greater impact than previously recognized. In such circumstance, an objective third party should have the opportunity to designate a cyber asset prospectively as critical or recharacterize the impact of a cyber asset for compliance purposes.141 Likewise, it is possible that a technological development or newly discovered vulnerability could justify a case-specific adjustment.

104. We agree with SPP RE that a modification of one or more of the bright line criteria is an appropriate response to a generic change in risk or impact of a category of cyber assets. Accordingly, as a reasonable application of the Order No. 706 directive that an entity with a regional approach have oversight of Critical Asset identification, NERC and the regions—or another designated third party—should have the authority in some circumstances, such as those discussed above, to designate a cyber asset as critical or adjust the

134 Order No. 706, 122 FERC ¶ 61,040 at P 233 (directing the ERO “to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and [to] report these findings to the Commission”).


136 Id. P 61.

137 NERC Comments at 7. NERC states in its comments that the CIP standard drafting team is considering the adoption of the term “BES Cyber Systems” in the next version of the CIP Reliability Standards. Our discussion below uses the term “cyber assets” to include any cyber asset or systems that the ERO eventually designates as needing cyber security protections under the CIP Reliability Standards.

138 FirstEnergy Comments at 2.

139 Order No. 706, 122 FERC ¶ 61,040 at PP 298, 322.

140 NORP, FERC Stats. & Regs. ¶ 32,679 at P 61.

141 Order No. 706, 122 FERC ¶ 61,040 at P 325.
“impact” characterization. In addressing the Order No. 706 directives, NERC should develop appropriate provisions to implement this limited opportunity for review.

F. Deadline for Addressing Order No. 706 Directives

NERC Petition

105. In the petition, NERC states that the standard drafting team is continuing to address the outstanding Order No. 706 directives.142 NERC notes that the next version of the CIP Reliability Standards “will build on the CIP–002–4 standards’ establishment of uniform criteria for the identification of Critical Assets.”143

NERC Petition at 6.

142 Id.

143 Id.

144 NOPR, FERC Stats. & Regs. ¶ 32,679 at P 67.

145 NERC Comments at 8–9.

146 PG&E Comments at 8.

147 ISO/RTCA Comments at 16.

developed through the normal NERC standard development process.148

109. The Trade Associations, AMP, Exelon, FirstEnergy, and KCP&L do not support a hard deadline for filing CIP Version 5.149 The Trade Associations, supported by FirstEnergy and KPC&L, and AMP believe that the development schedule for CIP Version 5 is aggressive and may need to be revised. The Trade Associations caution that an artificial deadline may increase the risk that some complex technical issues may not be fully resolved in Version 5. The Trade Associations and Exelon support a “realistic goal” or “target date” for filing CIP Version 5 coupled with periodic informational filings marking NERC’s progress.150 AMP supports requiring NERC to make periodic informational filings as well.151 The Trade Associations state that if the Commission deems a deadline necessary, it should be set for the first quarter of 2013.

Commission Determination

110. We adopt our NOPR proposal to establish a deadline for compliance with the outstanding Order No. 706 CIP directives. Given the lapse of time since the issuance of Order No. 706, we believe that it is appropriate to set a reasonable deadline for completion of the next version of the CIP Reliability Standards, which, according to NERC, is expected to address the outstanding Order No. 706 directives.152 The setting of a deadline responds to the finding in the January 2011 Audit Report of the Department of Energy’s Inspector General that “the CIP standards implementation approach and schedule approved by the Commission were not adequate to ensure that systems-related risks to the Nation’s power grid were mitigated or addressed in a timely manner.”153

111. We recognize, as numerous commenters discuss, that the current schedule for completing CIP Version 5 is aggressive. We also understand that the volume of industry discussion is high and we agree that industry input should not be artificially rushed or curtailed. In its reply comments, NERC indicated that it anticipates filing the Version 5 CIP Reliability Standards by the third quarter of 2012.154

Accordingly, to allow for sufficient time beyond what NERC estimates, we establish a deadline that is 6 months from the end of the third quarter of 2012 (i.e., March 31, 2013). NERC must also submit reports at the beginning of each quarter in which the ERO is to explain whether it is on track to meet the deadline and describe the status of its standard development efforts.

G. Violation Severity Levels and Violation Risk Factors

NERC Petition

112. As amended on April 12, 2011, the petition includes proposed VRFs and VSLs for each Requirement of the Version 4 CIP Reliability Standards, CIP–002–4 to CIP–009–4.

148 Dominion Comments at 4.

149 Trade Associations Comments at 13–14; AMP Comments at 4–5; Exelon Comments at 3–4; FirstEnergy Comments at 3–4; KCP&L Comments at 2.

150 Trade Associations Comments at 15.

151 AMP Comments at 5.

152 NOPR, FERC Stats. & Regs. ¶ 32,679 at P 65 n.45.


NOPR, FERC Stats. & Regs. ¶ 32,679 at pp. 35–36.

154 NERC Reply Comments at 4.

155 NOPR, FERC Stats. & Regs. ¶ 32,679 at pp. 35–36.
The Paperwork Reduction Act (PRA)\textsuperscript{159} requires each federal agency to seek and obtain OMB approval before undertaking a collection of information directed to ten or more persons, or where a Responsible Entity fails to identify or include one or more Critical Assets that fall within the Critical Asset criteria in Attachment 1 in its Critical Assets list pursuant to Requirement R1, or where a Responsible Entity fails to identify or include one or more Critical Cyber Assets in its Critical Cyber Asset list pursuant to Requirement R2.

III. Information Collection Statement

115. The Commission approves the VRFs and VSLs proposed by NERC subject to the modifications discussed above. As NERC now agrees, the Commission directs modifications to the “Severe VSL” for Requirements R1 and R2 to include the word “complete.” The modified VSLs will address situations where a responsible entity fails to identify or include one or more Critical Assets even if such list is null.” (emphasis added).

157 The VSL for Requirement R1, for example, would read: “The Responsible Entity did not include the list of its identified Critical Assets in its Critical Cyber Asset list, such assets become subject to the modifications discussed above.”

158 Upon approval of a collection(s) of information, OMB will assign an OMB control number and expiration date. Respondents subject to the filing requirement 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.

159 The Office of Management and Budget (OMB) regulations require approval of certain information collection requirements imposed by agency rules.\textsuperscript{158} Upon approval of a collection(s) of information, OMB will assign an OMB control number and expiration date. Respondents subject to the filing requirement 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.

159 The Paperwork Reduction Act (PRA)\textsuperscript{159} requires each federal agency to seek and obtain OMB approval before undertaking a collection of information directed to ten or more persons, or where a Responsible Entity fails to identify or include one or more Critical Assets that fall within the Critical Asset criteria in Attachment 1 in its Critical Assets list pursuant to Requirement R1, or where a Responsible Entity fails to identify or include one or more Critical Cyber Assets in its Critical Cyber Asset list pursuant to Requirement R2.

III. Information Collection Statement

116. The Office of Management and Budget (OMB) regulations require approval of certain information collection requirements imposed by agency rules.\textsuperscript{158} Upon approval of a collection(s) of information, OMB will assign an OMB control number and expiration date. Respondents subject to the filing requirement of this rule will not be penalized for failing to respond to these collections of information unless the collections of information display a valid OMB control number. The Paperwork Reduction Act (PRA)\textsuperscript{159} requires each federal agency to seek and obtain OMB approval before undertaking a collection of information directed to ten or more persons, or where a Responsible Entity fails to identify or include one or more Critical Assets that fall within the Critical Asset criteria in Attachment 1 in its Critical Assets list pursuant to Requirement R1, or where a Responsible Entity fails to identify or include one or more Critical Cyber Assets in its Critical Cyber Asset list pursuant to Requirement R2.

III. Information Collection Statement

117. The Commission is submitting these reporting and recordkeeping requirements to OMB for its review and approval under section 3507(d) of the PRA. The Commission solicited comments on the need for this information, whether the information will have practical utility, the accuracy of provided burden estimates, ways to enhance the quality, utility, and clarity of the information to be collected, and any suggested methods for minimizing the respondent’s burden, including the use of automated information techniques. The Commission received two comments regarding burden and cost estimates.

118. Hydro-Québec and NV Energy claim that the cost estimates included in the NOPR for Version 4 are inaccurate and incomplete.\textsuperscript{161} NV Energy states that the estimate does not include the significant burden of the additional security requirements that will be required by the identification of more Critical Assets and related Critical Cyber Assets. NV Energy comments that the cost estimate does not consider such matters as increased background checking, personnel risk assessments, cyber security training programs, and increased complexity of cyber security perimeters.

119. After a review of the comments on the Commission’s cost estimate, we maintain the cost estimate provided in the NOPR. While we recognize that implementing the Reliability Standards is not without cost, the benefits to reliability must be recognized. In response to Hydro-Québec and NV Energy’s concerns, we note that the estimate provided in the NOPR addresses the potential for an incremental increase in costs across the industry and does not address the full cost of implementing the CIP Reliability Standards by an entity. We anticipate that the savings associated with the change from the entity-specific risk-based assessment methodology, which had to be reviewed and updated each year, to a bright-line approach will offset some, if not all, of the incremental cost increase for entities that have previously identified a Critical Cyber Asset. With regards to NV Energy’s comments, we note that the proposed revisions to the Version 4 CIP Reliability Standards address the manner for the identification of Critical Assets, and do not revise current requirements pertaining to background checking, personnel risk assessments, cyber security training programs, and cyber security perimeters.

120. Burden Estimate: The principal differences in the existing information collection requirements and the burden imposed by the Reliability Standards in this Final Rule are triggered by the changes in Reliability Standard CIP–002–4. The previous risk-based assessment methodology for identifying Critical Assets is being replaced by 17 uniform “bright line” criteria for identifying Critical Assets (in CIP–002–4, Attachment 1, “Critical Asset Criteria”). Reliability Standard CIP–002–4 requires each responsible entity to use the bright line criteria as a “checklist” to identify Critical Assets, initially and in an annual review, instead of performing the more technical and individualized risk analysis involved in complying with the previously-effective CIP Reliability Standards. As in past versions of these Standards, each Responsible Entity will then identify the Critical Cyber Assets associated with its updated list of Critical Assets. If application of the bright line criteria results in the identification of new Critical Cyber Assets, such assets become subject to the remaining standards (approved CIP–003–4, CIP–004–4, CIP–005–4, CIP–006–4, CIP–007–4, CIP–008–4, and CIP–009–4), and the information collection requirements contained therein.

121. We estimate that the burden associated with the annual review of the assets (by the estimated 1,501 applicable entities) will be simplified by the “Critical Asset Criteria” in Reliability Standard CIP–002–4. Rather than each entity annually reviewing and updating a risk-based assessment methodology that frequently required technical analysis and judgment decisions, the bright line criteria will provide a straightforward checklist for all entities to use. Thus, we estimate that the revised Reliability Standard will reduce the burden associated with the annual review, as well as provide a consistent and clear set of criteria for all entities to follow.

122. The estimated changes to burden as contained in the Final Rule in RM11–11 follow.

\textsuperscript{156} NERC Comments at 7–8; PG&E Comments at 6–7.

\textsuperscript{157} The VSL for Requirement R1, for example, would read: “The Responsible Entity did not develop a complete list of its identified Critical Assets even if such list is null.” (emphasis added).

\textsuperscript{158} 5 CFR 1320.11.


\textsuperscript{161} Hydro-Québec Comments at 6; NV Energy Comments at 6–7.
The revisions to the cost estimates based on requirements of this Final Rule are:

1. Each entity that has identified Critical Cyber Assets has a reduction of 40 hours (345 entities × 40 hrs. = $1,324,800 reduction).

2. 12 Entities that formerly had not identified Critical Cyber Assets, but now have them, has

---

### Table: Burden Hours Per Respondent

<table>
<thead>
<tr>
<th>Number of Respondents</th>
<th>Average Number of Annual Responses Per Respondent</th>
<th>Average Number of Burden Hours Per Response</th>
<th>Effect of Final Rule in RM11–11, on Total Annual Hours</th>
<th>Annual Burden Hrs. upon Implementation of RM11–11</th>
</tr>
</thead>
<tbody>
<tr>
<td>345 [no change]</td>
<td>1</td>
<td>1,880 [reduction of 40 hours from 1,920 to 1,880 hours]</td>
<td>reduction of 13,800 hours.</td>
<td>648,600</td>
</tr>
<tr>
<td>1,144 [reduction of 12 entities from 1,156 to 1,144]</td>
<td>1</td>
<td>120 [no change]</td>
<td>reduction of 1,440 hours [for the 12 entities].</td>
<td>137,280</td>
</tr>
<tr>
<td>increase of 12 [formerly 0]</td>
<td>1</td>
<td>3,840</td>
<td>increase of 46,080 ....</td>
<td>46,080</td>
</tr>
<tr>
<td>Net Total</td>
<td>1,501</td>
<td></td>
<td>+30,840</td>
<td>831,960</td>
</tr>
</tbody>
</table>

---

The revisions to the estimated number of entities that identified Critical Cyber Assets has a reduction of 120 hours and an increase of 3,840 hours (for a net increase of 3,720 annual hours), giving 12 entities × 3,720 hrs. @ $96/hour = $4,285,440.

Storage costs = 12 entities @ $15.25/entity = $183.

Total Net Annual Cost for the FERC–725B requirements contained in the Final Rule in RM11–11 = $2,960,823 ($4,285,440 + $183 − $1,324,800).

The estimated hourly rate of $96 is the average cost of legal services ($230 per hour), technical employees ($40 per hour) and administrative support ($18 per hour), based on hourly rates from the Bureau of Labor Statistics (BLS) and the 2009 Billing Rates and Practices Survey Report. The $15.25 per entity for storage costs is an estimate based on the average costs to service and store 1 GB of data to demonstrate compliance with the CIP Standards.

Title: Mandatory Reliability Standards, Version 4 Critical Infrastructure Protection Standards.

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. The Reliability Standards help ensure the reliable operation of the Bulk-Power System by providing a cybersecurity framework for the identification and protection of Critical Assets and associated Critical Cyber Assets. As discussed above, the Commission approves NERC’s proposed Version 4 CIP Standards pursuant to section 215(d)(2) of the FPA because they represent an improvement to the previously-effective 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.

123. Interested persons may obtain information on the reporting requirements by contacting the following: Federal Energy Regulatory Commission, 888 First Street NE., Washington, DC 20426 [Attention: Ellen Brown, Office of the Executive Director, email: DataClearance@ferc.gov, phone: (202) 395–7285; or via the Internet at http://www.ferc.gov].

124. Comments concerning this information collection can be sent 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) 395–4718, fax: (202) 273–0873].

IV. Environmental Analysis

125. 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. The Commission has
categorically excluded certain actions from this requirement as not having a
significant effect on the human environment. Included in the exclusion
are rules that are clarifying, corrective, or procedural or that do not
substantially change the effect of the regulations being amended. The
actions taken here fall within this
categorical exclusion in the
Commission’s regulations.

V. Regulatory Flexibility Act

126. The Regulatory Flexibility Act of
1980 (RFA) generally requires a
description and analysis of final rules
that will have significant economic
impact on a substantial number of small
entities. The RFA mandates
consideration of regulatory alternatives
that accomplish the stated objectives of
a proposed rule and that minimize any
significant economic impact on a
substantial number of small entities.
The Small Business Administration’s
(SBA) Office of Size Standards develops
the numerical definition of a small
business. The SBA has established a
size standard for electric utilities,
stating that a firm is small if, including
its affiliates, it is primarily engaged in
the transmission, generation and/or
distribution of electric energy for sale
and its total electric output for the
preceding twelve months did not exceed
four million megawatt hours.

127. This Final Rule may have a
significant economic impact on some
small entities. The Commission
estimates that 12 of the total small
to 5 p.m. Eastern time) at 888 First
Street NE., Room 2A, Washington, DC
20426.

131. From FERC’s Home Page on the
Internet, this information is available on
eLibrary. The full text of this document
is available on eLibrary in PDF and
Microsoft Word format for viewing,
printing, and/or downloading. To access
this document in eLibrary, type the
docket number excluding the last three
digits of this document in the docket
number field.

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

VII. Effective Date and Congressional
Notification

133. These regulations are effective
June 25, 2012. The Commission has
determined, with the concurrence of the
Administrator of the Office of
Information and Regulatory Affairs of
OMB, that this rule is not a “major rule”
as defined in section 351 of the Small
Business Regulatory Enforcement
Fairness Act of 1996.

List of Subjects in 18 CFR Part 40

Electric power, Electric utilities,
Reporting and recordkeeping
requirements.

By the Commission.
Nathaniel J. Davis, Sr.,
Deputy Secretary.

Appendix

<table>
<thead>
<tr>
<th>Commenters</th>
</tr>
</thead>
</table>

Abbreviation | Commenter |
-------------|-----------|
AMP .......... | American Municipal Power, Inc. |
Constellation .......... | Constellation Energy Group, Inc. (intervened w/o comment). |
Dominion .......... | Dominion Resources Services, Inc. |
Exelon .......... | Exelon Corporation. |
Hydro-Québec Cooperatives .......... | Hydro-Québec TransÉnergie. |
ITC .......... | International Transmission Company d/b/a ITCTransmission, Michigan Electric Company, LLC, ITC Midwest LLC and ITC Great Plains LLC. |

171 13 CFR 121.101.
Withholding by Government Entities

Removal of Regulations Requiring 3% Withholding by Government Entities

AGENCY: Internal Revenue Service (IRS), Treasury.

ACTION: Final regulations.

SUMMARY: This document provides a Treasury decision that removes the final regulations contained in TD 9524 relating to withholding by government entities on payments to persons providing property or services, and makes conforming amendments to regulations to reflect the removal of these regulations. The final regulations are removed because the 3% Withholding Repeal and Job Creation Act repealed the provision of the Internal Revenue Code underlying the final regulations before the provision became effective. The guidance affects government entities that would have been required to withhold and report tax from payments to persons providing property or services and also affects the persons receiving payments for property or services from these government entities.

DATES: Effective Date: These regulations are effective on April 25, 2012.

Applicability Date: For dates of applicability, see §§ 31.6011(a)–4(d) and 31.6302–1(n).

FOR FURTHER INFORMATION CONTACT: A. G. Kelley, (202) 622–6040 (not a toll-free number).

SUPPLEMENTARY INFORMATION:

Background

This document contains amendments to 26 CFR part 31 under section 3402(t) of the Internal Revenue Code (Code), relating to three percent withholding by government entities on payments for property or services. Section 3402(t) of the Code was added by section 511 of the Tax Increase Prevention and Reconciliation Act of 2005, Public Law 109–222 (TIPRA), 120 Stat. 345, which was enacted on May 17, 2006. The Treasury Department and the IRS issued final regulations under sections 3402(t), 3406, 6011, 6051, 6071, and 6302 of the Code that were published in the Federal Register on May 9, 2011 (TD 9524, 76 FR 26583, 2011–23 IRB 843) (the May 2011 final regulations). Those regulations were issued to implement the requirements of section 3402(t) and conform existing regulations to section 3402(t).

Section 102 of the 3% Withholding Repeal and Job Creation Act (Pub. L. 112–56, 125 Stat. 711), which was enacted on November 21, 2011, repealed section 3402(t) of the Code. Section 3402(t) was repealed before it became effective.

This document, therefore, removes the regulatory provisions issued under section 3402(t) and related sections, and makes conforming amendments to certain regulations to reflect the removal of the section 3402(t) regulations.

At the same time as the issuance of the May 2011 final regulations, the Treasury Department and the IRS also issued proposed regulations under section 3402(t), published in the Federal Register on May 9, 2011 (REG–151687–10, 76 FR 26678, 2011–23 IRB 867). A related document withdraws those proposed regulations in light of the repeal of section 3402(t). See REG–151687–10.

Special Analyses

It has been determined that this Treasury decision is not a significant regulatory action as defined in Executive Order 12866, as supplemented by Executive Order 13563. Therefore, a regulatory assessment is not required. It also has been determined that section 553(b) of the Administrative Procedure Act (5 U.S.C. chapter 5) does not apply to this regulation, and because no notice of proposed rule making is required for this rule, the Regulatory Flexibility Act (5 U.S.C. chapter 6) does not apply.

Drafting Information

The principal author of these final regulations is A. G. Kelley, Office of the Division Counsel/Associate Chief Counsel (Tax Exempt and Government Entities). However, other personnel from the IRS and the Treasury Department participated in their development.

List of Subjects in 26 CFR Part 31

Employment taxes, Fishing vessels, Gambling, Income taxes, Penalties, Pensions, Railroad retirement, Reporting and recordkeeping requirements, Social Security, Unemployment compensation.

A 102 of the 3% Withholding Repeal and Job Creation Act (Pub. L. 112–56, 125 Stat. 711), which was enacted on November 21, 2011, repealed section 3402(t) of the Code. Section 3402(t) was repealed before it became effective. This document, therefore, removes the regulatory provisions issued under section 3402(t) and related sections, and makes conforming amendments to certain regulations to reflect the removal of the section 3402(t) regulations.

At the same time as the issuance of the May 2011 final regulations, the Treasury Department and the IRS also issued proposed regulations under section 3402(t), published in the Federal Register on May 9, 2011 (REG–151687–10, 76 FR 26678, 2011–23 IRB 867). A related document withdraws those proposed regulations in light of the repeal of section 3402(t). See REG–151687–10.

Special Analyses

It has been determined that this Treasury decision is not a significant regulatory action as defined in Executive Order 12866, as supplemented by Executive Order 13563. Therefore, a regulatory assessment is not required. It also has been determined that section 553(b) of the Administrative Procedure Act (5 U.S.C. chapter 5) does not apply to this regulation, and because no notice of proposed rule making is required for this rule, the Regulatory Flexibility Act (5 U.S.C. chapter 6) does not apply.

Drafting Information

The principal author of these final regulations is A. G. Kelley, Office of the Division Counsel/Associate Chief Counsel (Tax Exempt and Government Entities). However, other personnel from the IRS and the Treasury Department participated in their development.

List of Subjects in 26 CFR Part 31

Employment taxes, Fishing vessels, Gambling, Income taxes, Penalties, Pensions, Railroad retirement, Reporting and recordkeeping requirements, Social Security, Unemployment compensation.

A 102 of the 3% Withholding Repeal and Job Creation Act (Pub. L. 112–56, 125 Stat. 711), which was enacted on November 21, 2011, repealed section 3402(t) of the Code. Section 3402(t) was repealed before it became effective. This document, therefore, removes the regulatory provisions issued under section 3402(t) and related sections, and makes conforming amendments to certain regulations to reflect the removal of the section 3402(t) regulations.

At the same time as the issuance of the May 2011 final regulations, the Treasury Department and the IRS also issued proposed regulations under section 3402(t), published in the Federal Register on May 9, 2011 (REG–151687–10, 76 FR 26678, 2011–23 IRB 867). A related document withdraws those proposed regulations in light of the repeal of section 3402(t). See REG–151687–10.

Special Analyses

It has been determined that this Treasury decision is not a significant regulatory action as defined in Executive Order 12866, as supplemented by Executive Order 13563. Therefore, a regulatory assessment is not required. It also has been determined that section 553(b) of the Administrative Procedure Act (5 U.S.C. chapter 5) does not apply to this regulation, and because no notice of proposed rule making is required for this rule, the Regulatory Flexibility Act (5 U.S.C. chapter 6) does not apply.