DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

18 CFR Part 40

[Docket No. RM06–22–000; Order No. 706]

Mandatory Reliability Standards for Critical Infrastructure Protection

Issued January 18, 2008.

AGENCY: Federal Energy Regulatory Commission, Department of Energy.

ACTION: Final Rule.

SUMMARY: Pursuant to section 215 of the Federal Power Act (FPA), the Commission approves eight Critical Infrastructure Protection (CIP) Reliability Standards submitted to the Commission for approval by the North American Electric Reliability Corporation (NERC). The CIP Reliability Standards require certain users, owners, and operators of the Bulk-Power System to comply with specific requirements to safeguard critical cyber assets. In addition, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to the CIP Reliability Standards to address specific concerns.

DATES: *Effective Date:* This rule will become effective April 7, 2008.

FOR FURTHER INFORMATION CONTACT:

Gary Cohen (Legal Information), Office of the General Counsel, Federal Energy Regulatory Commission, 888 First Street, NE., Washington, DC 20426, (202) 502–8321.

Christy Walsh (Legal Information), Office of the General Counsel, Federal Energy Regulatory Commission, 888 First Street, NE., Washington, DC 20426, (202) 502–6523.

Regis Binder (Technical Issues), Office of Electric Reliability, Federal Energy Regulatory Commission, 888 First Street, NE., Washington, DC 20426, (202) 502–6460.

Jan Bargen (Technical Issues), Office of Electric Reliability, Federal Energy Regulatory Commission, 888 First Street, NE., Washington, DC 20426, (202) 502–6333.

SUPPLEMENTARY INFORMATION:

TABLE OF CONTENTS

Before Commissioners: Joseph T. Kelliher, Chairman; Suedeen G. Kelly, Marc Spitzer, Philip D. Moeller, and Jon Wellinghoff.

Final Rule

1. Pursuant to section 215 of the Federal Power Act (FPA),[1] the Commission approves eight Critical Infrastructure Protection (CIP) Reliability Standards submitted to the Commission for approval by the North American Electric Reliability Corporation (NERC). The CIP Reliability Standards require certain users, owners, and operators of the Bulk-Power System to comply with specific requirements to safeguard critical cyber assets.[2] In addition, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications to the CIP Reliability Standards to address specific concerns identified by the Commission.

I. Background

2. Section 215 of the FPA requires a Commission-certified Electric Reliability Organization (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 the Commission can independently enforce Reliability Standards.[3]

3. Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO[4] and, subsequently, certified NERC as the ERO.[5] On April 4, 2006, as modified on August 28, 2006, NERC submitted to the Commission a petition seeking approval of 107 proposed Reliability Standards. On March 16, 2007, the Commission issued a Final Rule, Order No. 693, approving 83 of these 107 Reliability Standards and directing other related actions.[6] In addition, pursuant to section 215(d)(5) of the FPA, the Commission directed NERC to develop modifications to 56 of the 83 approved Reliability Standards.[7]

4. In April 2007, the Commission approved delegation agreements between NERC and each of the eight Regional Entities.[8] Pursuant to the delegation agreements, the ERO has delegated responsibility to the Regional Entities to carry out compliance monitoring and enforcement of the mandatory Reliability Standards.

5. Prior to being certified by the Commission as the ERO, NERC had developed a cyber security standard for the electric industry on a voluntary basis. This voluntary standard, Urgent Action 1200, was adopted in 2003, and remained in effect on a voluntary basis until June 1, 2006, at which time the eight CIP Reliability Standards that are the subject of the current rulemaking replaced the Urgent Action 1200 standard.

6. On August 28, 2006, NERC submitted to the Commission for approval the following eight CIP Reliability Standards:[9]

CIP–002–1—Cyber Security—Critical Cyber Asset Identification: Requires a responsible entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology.

CIP–003–1—Cyber Security—Security Management Controls: Requires a responsible entity to develop and implement security management controls to protect critical cyber assets identified pursuant to CIP–002–1.

CIP–004–1—Cyber Security—Personnel & Training: Requires personnel with access to critical cyber assets to have identity verification and a criminal check. It also requires employee training.

CIP–005–1—Cyber Security—Electronic Security Perimeters: Requires the identification and protection of an electronic security perimeter and access points. The electronic security perimeter is to encompass the critical cyber assets identified pursuant to the methodology required by CIP–002–1.

CIP–006–1—Cyber Security—Physical Security of Critical Cyber Assets: Requires a responsible entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.

CIP–007–1—Cyber Security—Systems Security Management: Requires a responsible entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.

CIP–008–1—Cyber Security—Incident Reporting and Response Planning: Requires a responsible entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets.

CIP–009–1—Cyber Security—Recovery Plans for Critical Cyber Assets: Requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

7. NERC states that these CIP Reliability Standards provide a comprehensive set of requirements to protect the Bulk-Power System from malicious cyber attacks. They require Bulk-Power System users, owners, and operators to establish a risk-based vulnerability assessment methodology to identify and prioritize critical assets and critical cyber assets. Once the critical cyber assets are identified, the CIP Reliability Standards require, among other things, that the responsible entities establish plans, protocols, and controls to safeguard physical and electronic access, to train personnel on security matters, to report security incidents, and to be prepared for recovery actions. Further, NERC developed an implementation plan that provides for a three-year phase-in to achieve full compliance with all requirements.

8. Each CIP Reliability Standard uses a common organizational format that includes five sections, as follows: (A) Introduction, which includes ''Purpose'' and ''Applicability'' sub-sections; (B) Requirements; (C) Measures; (D) Compliance; and (E) Regional Differences. In this Final Rule, these section titles are capitalized when referencing a designated provision of a Reliability Standard.

9. In a separate filing, NERC submitted 162 Violation Risk Factors that correspond to Requirements of the proposed CIP Reliability Standards.[10] Violation Risk Factors delineate the relative risk to the Bulk-Power System associated with the violation of each Requirement and are used by NERC and the Regional Entities to determine financial penalties for violating a Reliability Standard.

10. On December 11, 2006, the Commission released a ''Staff

[1] 16 U.S.C. 824o (2000 & Supp. V 2005).

[2] In the context of the CIP Reliability Standards, cyber assets are programmable electronic devices and communication networks including hardware, software, and data. *See Mandatory Reliability Standards for Critical Infrastructure Protection,* Notice of Proposed Rulemaking, 72 FR 43970 (Aug. 6, 2007), FERC Stats & Regs. ¶ 32,620 at P 1 (Jul. 20, 2007) (CIP NOPR).

[3] 16 U.S.C. 824o(e)(3) (2000 & Supp. V 2005).

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

[5] *North American Electric Reliability Corp.,* 116 FERC ¶ 61,062 (ERO Certification Order), *order on reh'g & compliance,* 117 FERC ¶ 61,126 (ERO Rehearing Order) (2006), *appeal docket sub nom. Alcoa, Inc.* v. *FERC,* No. 06–1426 (D.C. Cir. Dec. 29, 2006).

[6] *Mandatory Reliability Standards for the Bulk-Power System,* Order No. 693, FERC Stats. & Regs. ¶ 31,242 (2007); Order No. 693–A, *reh'g denied,* 120 FERC ¶ 61,053 (2007).

[7] Section 215(d)(5) provides ''The Commission . . . may order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section.''

[8] *See North American Electric Reliability Corp.,* 119 FERC ¶ 61,060, *order on reh'g,* 120 FERC ¶ 61,260 (2007).

[9] The CIP Reliability Standards are not codified in the CFR and are not attached to the Final Rule. They are, however, available on the Commission's eLibrary document retrieval system in Docket No. RM06–22–000 and are available on the ERO's Web site, *http://www.nerc.com.*

[10] *See* NERC's March 23, 2007 filing in Docket No. RR07–10–000, Exh. A.

Preliminary Assessment of the North American Electric Reliability Corporation's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection'' prepared by the Commission's staff (CIP Assessment). The CIP Assessment identified staff's preliminary observations and concerns regarding the eight proposed CIP Reliability Standards, describing issues common to a number of the proposed CIP Reliability Standards, and discussing various issues raised by individual CIP Reliability Standards. While discussing the issues, the CIP Assessment did not make specific recommendations on the appropriate action to be taken by the Commission on particular proposals.[11]

11. On July 20, 2007, the Commission issued the CIP NOPR, which proposed to approve the eight CIP Reliability Standards submitted to the Commission for approval by NERC. In addition, the Commission proposed to direct NERC to develop modifications to the CIP Reliability Standards to address specific concerns identified by the Commission.

12. In response to the CIP NOPR, comments were filed by about 70 interested persons. In the discussion below, we will address the issues raised by these comments. Appendix A to this Final Rule lists the entities that filed comments on the CIP NOPR. Five comments were filed after the time prescribed in the CIP NOPR. Nevertheless, the Commission will consider these comments, as they will neither prejudice the other commenters, nor delay the proceeding.

II. Discussion

A. Overview

13. In the Final Rule, the Commission approves the eight CIP Reliability Standards, finding that they are just and reasonable, not unduly discriminatory or preferential and in the public interest. Further, the Commission approves NERC's implementation plan that sets milestones for responsible entities to achieve full compliance with the CIP Reliability Standards. The Commission also directs NERC to develop modifications to the CIP Reliability Standards through its Reliability Standards development process to address specific concerns identified by the Commission. Similar to our approach in Order No. 693, we view such directives as a separate action from approval, consistent with our authority in section 215(d)(5) of the FPA to direct the ERO to develop a modification to a Reliability Standard. As discussed below, such modification should not affect the current implementation plan. Rather, NERC is directed to develop a timetable for development of the modifications to the CIP Reliability Standards and, if warranted, to develop and file with the Commission for approval, a second implementation plan.

14. Other determinations in the Final Rule include:

A directive that the ERO must develop modifications to the CIP Reliability Standards to remove the ''reasonable business judgment'' language.

The ERO must also develop modifications to remove ''acceptance of risk'' exceptions from the CIP Reliability Standards.

The ERO is directed to develop specific conditions that a responsible entity must satisfy to invoke the ''technical feasibility'' exception. This structure for use of the technical feasibility exception allows flexibility and customization of implementation of the CIP Reliability Standards in a controlled manner.

The Commission directs the ERO to provide additional guidance regarding the development of a risk-based assessment methodology for the identification of critical assets pursuant to CIP–002–1. Further, external review of critical asset lists is required.

The Commission directs the ERO to make specific revisions to its Violation Risk Factor designations.

B. Approval of NERC's Proposed CIP Reliability Standards

1. NOPR Proposal

15. In the CIP NOPR, the Commission proposed to approve NERC's eight proposed CIP Reliability Standards as mandatory and enforceable. As a separate action, pursuant to section 215(d)(5) of the FPA, the Commission proposed to direct NERC to modify certain provisions of the CIP Reliability Standards.

2. Comments

16. Most commenters strongly support the Commission's proposal to approve the CIP Reliability Standards as mandatory and enforceable.[12] For example, EEI states that the CIP Reliability Standards are technically sound and well designed to achieve the specified reliability goal, namely cyber security for electric industry critical assets. EEI adds that the CIP Reliability Standards are designed to serve the interest of preserving grid reliability by seeking to prevent unauthorized access to control systems and other critical cyber assets, whether by physical or electronic means. EEI believes that the CIP Reliability Standards strike the appropriate balance in providing reasonable flexibility in an environment where systems vary greatly in architecture, technology, and risk profile.[13]

17. By contrast, ABB argues that the Commission should defer action so that equipment vendors and the standard-setting organizations such as the Institute of Electrical and Electronics Engineers can coordinate electric power system cyber security initiatives. Applied Control Solutions argues that the proposals in the CIP NOPR do not go far enough, and that the Commission should go further and immediately adopt the National Institute of Standards and Technology (NIST) Security Risk Management Framework in place of the CIP Reliability Standards.

18. NIST itself argues that the Commission should adopt the NERC proposed CIP Reliability Standards, as appropriately enhanced based on the Commission's proposed directives in the CIP NOPR, as an interim measure. NIST advocates that the Commission prescribe plans for a two to three year transition to cyber security standards that are identical to, consistent with, or based on SP 800–53 and related NIST standards and guidelines.

19. WIRAB supports NERC's CIP Reliability Standards and states that they represent a significant advancement for cyber security and Bulk-Power System reliability. Yet, WIRAB recommends that the Commission remand the CIP Reliability Standards to NERC with guidance as to the types of changes the Commission would like to see, but without direction to make any specific change. WIRAB expresses concern that the CIP NOPR proposes numerous detailed directives to modify the CIP Reliability Standards and goes beyond providing guidance to NERC. WIRAB states that a remand would allow the Reliability Standards development process to work as anticipated and, in doing so, would avoid problems with different Reliability Standards or different levels of enforcement on different sides of the international border.

20. In response to our proposal to modify certain CIP Reliability Standards, some commenters maintain that the Commission's proposals were

[11] The CIP Assessment is available on the Commission's webpage at *http://www.ferc.fed.us/industries/electric/indus-act/reliability.asp.*

[12] *E.g.,* Alliant, Arizona Public Service, Bonneville, California Commission, Duke, EEI, Idaho Power, ISO/RTO Council, Juniper, KCPL, Luminant, Manitoba, NERC, New York Commission, Northeast Utilities, Ontario IESO, Ontario Power, PG&E, PSEG Companies, Progress, Puget Sound, ReliabilityFirst, SDG&E, Southern, Tampa Electric, Teltone and Xcel.

[13] Alliant, KCPL, PG&E, Puget Sound, PSEG Companies and Southern support EEI's views.

overly prescriptive.[14] Others state that any prescriptive elements of the CIP NOPR should be replaced with directions that NERC use its Commission-approved Reliability Standards development process to address any necessary changes identified by the Commission.[15] PG&E adds that the measures agreed on in the NERC stakeholder process and included in the CIP Reliability Standards represent a reasonable balance between aggressive Reliability Standards and measures that are feasible and sustainable. EEI argues that the Commission needs to be careful when it provides guidance that it does not usurp NERC's authority as ERO by dictating a specific or exclusive outcome from this process.

21. Commenters also express concern that the Commission might intend to sidestep the NERC stakeholder process and have NERC simply revise the CIP Reliability Standards in accordance with the Commission's proposals without providing NERC stakeholders an opportunity to participate in this process.[16] In this regard, EEI urges that the Final Rule make clear that any improvements to the CIP Reliability Standards should be considered in the NERC Reliability Standards development process before being mandated.

22. KCPL supports the Commission's proposal to direct NERC to develop modifications to the CIP Reliability Standards to address potential improvements using the Reliability Standards development process. KCPL believes that the Commission has authority to direct the ERO to modify the CIP Reliability Standards and to provide sufficient guidance to the direction that grid reliability should take so as to fulfill its obligations under the Energy Policy Act of 2005. However, KCPL too is concerned that several of the Commission's proposed requirement directives are overly prescriptive.

23. The New York Commission opposes the Commission placing any conditions on its approval of the CIP Reliability Standards, such as requiring NERC to rewrite them as a condition for their approval.

[14] *E.g.,* CEA, EEI, FirstEnergy, PSEG Companies, SDG&E and Tampa Electric.

[15] *E.g.,* Georgia Operators, Idaho Power, Muscatine Power, NERC, Northern California, NRECA, TAPS and Xcel.

[16] *See, e.g.*, Allegheny, Alliant, Arizona Public Service, Duke, EEI, Entergy, FirstEnergy, FPL Group, Iowa Municipals, KCPL, Luminant, PG&E, Progress, PSEG Companies, Tampa Electric and TAPS.

3. Commission Determination

24. The Commission approves the eight CIP Reliability Standards pursuant to section 215(d) of the FPA, as discussed below. In approving the CIP Reliability Standards, the Commission concludes that they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. These CIP Reliability Standards, together, provide baseline requirements for the protection of critical cyber assets that support the nation's Bulk-Power System. Thus, the CIP Reliability Standards serve an important reliability goal.[17] Further, as discussed below, the CIP Reliability Standards clearly identify the entities to which they apply, apply throughout the interconnected Bulk-Power System, and provide a reasonable timetable for implementation.[18]

25. The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP–002–1 through CIP–009–1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework.

26. With regard to WIRAB's recommendation, we share the ongoing concern of promoting coordinated action on Reliability Standards on an international basis. However, in this instance, we do not believe a remand to NERC, which would result in significant delays in having mandatory and enforceable cyber security requirements in effect in the United States, is justified or would further such coordination. The implementation schedule provided by NERC, which applies continent-wide, requires applicable entities to achieve ''auditable compliance'' no earlier than mid-2009. This should provide adequate time for entities responsible for compliance with the CIP Reliability Standards in the United States, Canada and Mexico to achieve compliance on a common timetable. As discussed later, future modifications to the CIP Reliability Standards developed pursuant to the direction provided in the Final Rule would not overlap with the NERC implementation plan. Accordingly, the Commission concludes that this is not a satisfactory reason for remanding the CIP Reliability Standards.

27. In approving the CIP Reliability Standards and directing the ERO to modify them, the Commission is taking two independent actions and does not condition our approval on the ERO modifying the CIP Reliability Standards. First, we are exercising our authority to approve a proposed Reliability Standard. Second, we are directing the ERO to submit a modification of the Reliability Standards to address specific issues or concerns.[19] Accordingly, New York Commission's concerns about the Commission placing any conditions on its approval of the CIP Reliability Standards are unnecessary.

28. With regard to the concerns raised by some commenters about the prescriptive nature of the Commission's proposed modifications, the Commission agrees that a direction for modification should not be so overly prescriptive as to preclude the consideration of viable alternatives in the ERO's Reliability Standards development process. However, in identifying a specific matter to be addressed in a modification to a CIP Reliability Standard, it is important that the Commission provide sufficient guidance so that the ERO has an understanding of the Commission's concerns and an appropriate, but not necessarily exclusive, outcome to address those concerns. Without such direction and guidance, a Commission proposal to modify a CIP Reliability Standard might be so vague that the ERO would not know how to adequately respond.[20]

29. Thus, in some instances, while we provide specific details regarding the Commission's expectations, we intend by doing so to provide useful guidance to assist in the Reliability Standards development process, not to impede it. We find that this is consistent with statutory language that authorizes the Commission to order the ERO to submit a modification ''that addresses a specific matter'' if the Commission considers it appropriate to carry out section 215 of the FPA. In the Final Rule, we have considered commenters' concerns and, where a directive for modification appears to be determinative of the outcome, the Commission provides flexibility by directing the ERO to

[17] *See* Order No. 672 at P 321.

[18] *Id.* P 322–35.

[19] 16 U.S.C. 824o(d)(5) (''[t]he Commission . . . may order the Electric Reliability Organization to submit to the Commission a proposed Reliability Standard or modification to a Reliability Standard that addresses a specific matter if the Commission considers such a new or modified Reliability Standard appropriate to carry out this section.'').

[20] *See* Order No. 693 at P 185–87.

address the underlying issue through the Reliability Standards development process without mandating a specific change to the CIP Reliability Standard. Further, the Commission clarifies that, where the Final Rule identifies a concern and offers a specific approach to address that concern, we will consider an equivalent alternative approach provided that the ERO demonstrates that the alternative will adequately address the Commission's underlying concern or goal as efficiently and effectively as the Commission's proposal.

30. Consistent with section 215 of the FPA, our regulations, and Order No. 693, any modification to a Reliability Standard, including a modification that addresses a Commission directive, must be developed and fully vetted through NERC's Reliability Standard development process. Until the Commission approves NERC's proposed modification to a Reliability Standard, the preexisting Reliability Standard will remain in effect.

C. Applicability

31. The Applicability section of each proposed CIP Reliability Standard identifies the following 11 categories of responsible entities that must comply with the CIP Reliability Standard: Reliability coordinators, balancing authorities, interchange authorities,[21] transmission service providers, transmission owners, transmission operators, generator owners, generator operators, load serving entities, NERC, and Regional Reliability Organizations.

1. NOPR Proposal

32. The CIP NOPR explained that, with regard to the applicability of the CIP Reliability Standards to the ERO, NERC has modified its Rules of Procedure to provide that the ERO will comply with each Reliability Standard that identifies the ERO as an applicable entity.[22] Further, the delegation agreements between NERC and each of the eight Regional Entities expressly state that the Regional Entity is committed to comply with approved Reliability Standards. The Commission stated its belief that, while it is likely that NERC and the Regional Entities are not directly subject to mandatory Reliability Standards as users, owners or operators of the Bulk-Power System, their adherence to the CIP Reliability Standards pursuant to the NERC Rules of Procedure and the delegation agreements suffices.

33. The Commission also indicated in the CIP NOPR that it would rely on the NERC registration process to determine applicability with the CIP Reliability Standards.[23] While expressing concern about small entities becoming a gateway for cyber attacks, the Commission indicated that it was prepared to rely on the registration process based in part on the expectation that industry will use the ''mutual distrust'' posture.[24] The Commission also explained that it would rely on the NERC registration process to include all critical assets and associated critical cyber assets, and listed examples. Further, we noted that because, as an initial compliance step, each entity that is responsible for compliance with the CIP Reliability Standards must first identify critical assets through the application of a risk-based assessment, CIP–002–1 acts as a filter, determining a subset of entities that must comply with the remaining CIP requirements (i.e., CIP–003–1 through CIP–009–1).

34. The Commission also raised concerns regarding operation of critical cyber assets by out-sourced entities.[25] The CIP NOPR noted that, on occasion, NERC negotiates contracts with third-party vendors, and the products developed by the vendors are then used by responsible entities that, as owners of the critical cyber assets, are ultimately responsible for their cyber security protection under the CIP Reliability Standards. The Commission solicited comment on whether and how out-sourced entities should be contractually obligated to comply with the CIP Reliability Standards while satisfying their other contractual obligations.

2. Comments

35. Most commenters that address the issue support the Commission's approach to assuring NERC and Regional Entity compliance with the CIP Reliability Standards. Commenters also support the Commission's reliance on the NERC registration process to identify appropriate entities. Numerous commenters address the issue of third-party vendors, indicating that such third parties are not subject to mandatory Reliability Standards and that responsible entities need to address the matter through contractual provisions with their vendors.

a. Applicability to NERC and Regional Entities

36. EEI supports the Commission's conclusion that NERC's modifications to its Rules of Procedure and the delegation agreements between NERC and each of the eight Regional Entities with respect to compliance with approved Reliability Standards is sufficient and does not require any additional measures or revisions at this time. EEI expects that the Commission will provide oversight with respect to compliance by NERC and a Regional Entity. However, unlike responsible entities, the ERO and Regional Entities are not subject to penalties under the FPA. Therefore, in considering what level of oversight to provide for these entities, EEI urges the Commission to consider that these entities do not have the same incentive as responsible entities to comply with the CIP Reliability Standards.

37. Progress believes that the CIP Reliability Standards must apply to the ERO and the Regional Entities since they have access to critical data of many electric systems and may be perceived as more strategic targets than other registered entities. California Commission, Northern Indiana and Northeast Utilities also assert that the CIP Reliability Standards should apply to NERC and the Regional Entities. Northern Indiana states that subjecting NERC to the CIP Reliability Standards would obviate Northern Indiana's concern with providing NERC personnel with access to information they may need when reviewing and evaluating Northern Indiana's compliance measures.

38. California Commission comments that the CIP NOPR properly recognized the ERO as an applicable entity. It also states that the delegation agreements between NERC and the Regional Entities mandate that the Regional Entities will be subject to the CIP Reliability Standards. California Commission states that, if the ERO or Regional Entities do not adhere to the CIP Reliability Standards, they could become the weak link whose failure could harm the Bulk-Power System.

[21] *See* Docket No. RR08–3–000 wherein, on November 11, 2007, NERC filed an amendment to its Statement of Compliance Registry Criteria to add Interchange Authority to the list of functional entities that are required to comply with certain Reliability Standards.

[22] *See* CIP NOPR at P 21–31; NERC Rules of Procedure, section 100.

[23] *Id.* P 27. The CIP NOPR also affirmed the statement in Order No. 693 that the Commission intends to further examine applicability issues under section 215 of the FPA in a future proceeding. Order No. 693 at P 77.

[24] *Id.* P 28. The term ''mutual distrust '' is used to denote how ''outside world'' systems are treated by those inside the control system. 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. This concept is discussed further in the context of CIP–003–1.

[25] CIP NOPR at P 31.

b. Reliance on NERC Registration Process

39. NRECA, MEAG Power and other commenters support the Commission's reliance on the NERC registration process to identify appropriate entities and also share the concern that entities not registered could become a weakness in the security of the Bulk-Power System.[26] NRECA states that the Commission's proposed approach is appropriate and consistent with the Commission's prior orders, the statute, and the ERO's Statement of Registry Criteria. EEI suggests that proper registration, combined with a strong ERO audit program, would assure that all critical assets are covered by the CIP Reliability Standards. EEI also asks the Commission to clarify that the NERC registration process would identify responsible entities, but not critical assets.

40. EEI and ISO/RTO Council agree with the statement in the CIP NOPR that demand side aggregators might also need to be included in the NERC registration process if their load shedding capacity would affect the reliability or operability of the Bulk-Power System. EEI comments that demand side aggregators do not fit into any of the current registry categories and their inclusion would likely require the development of a definition of ''demand response'' and ''direct load control,'' as well as size thresholds, which are best addressed in the NERC Reliability Standards development process.

41. California Commission comments that small entities can become a weak link whose failure could harm Bulk-Power System reliability. It is concerned that an entity that should be registered may slip through the identification process. Accordingly, California Commission suggests that any entity connected to the Bulk-Power System, regardless of size, must comply with the CIP Reliability Standards irrespective of their registration status.

c. Third-Party Vendors

42. The majority of commenters contend that neither the ERO, nor the Commission, have authority to extend the applicability of the CIP Reliability Standards to third-party vendors.[27] NRECA, for example, argues that this conclusion is dictated by statute, as section 215 of the FPA only applies to users, owners and operators of the Bulk-Power System and does not confer jurisdiction over third-party vendors. Accordingly, commenters claim that the relationship between registered entities and their outsourced providers is necessarily one of contract, and the regulatory compliance obligation falls solely on the registered entity.

43. EEI agrees with the CIP NOPR statement that responsible entities, as owners of critical assets, are ultimately accountable for their cyber security protection under the Reliability Standards. EEI also comments that it is reasonable that responsible entities may wish to provide their vendors with incentives to comply with CIP Reliability Standards while satisfying their other contractual obligations.[28] According to ReliabilityFirst, outsourced products developed for the exchange of data integral to reliability must be developed in compliance with the CIP Reliability Standards. It believes the responsible entity should contractually obligate vendors of such products to comply with appropriate requirements of the CIP Reliability Standards.

44. ISO/RTO Council comments that, when an application is developed and maintained by an outsourced provider, that provider manages access to the environment on which the application runs and therefore must be contractually obligated by the responsible entity to comply with the CIP Reliability Standards. While not in NERC's registry, such third parties must perform the services and operate the applications in a manner consistent with the CIP Reliability Standards. According to ISO/RTO Council, the responsible entity should be charged with incorporating contractual terms and conditions into its agreements with the third-party provider that obligates the provider to comply with the requirements of the CIP Reliability Standards. Responsibility for non-compliance by the third-party vendor should be borne by the responsible entity that made the business decision to outsource the application.

45. Other commenters contend that the CIP Reliability Standards must apply to vendors and contractors as well as responsible entities. For example, California Commission suggests that the CIP Reliability Standards should apply to every entity that has a cyber connection to the Bulk-Power System. However, in California Commission's view, some special rules must be developed on CIP Reliability Standards applicability for entities that are not responsible entities but that have entered contracts obligating them to comply with the CIP Reliability Standards. Consumers claims that vendors and contactors with access (remote and on-site) to the critical cyber assets should be required to comply with the CIP Reliability Standards' personnel risk assessment guidelines. Consumers also advocates that vendor companies should have a personnel risk assessment policy, i.e., background check, for all new personnel and all systems (software applications and hardware devices) should be tested for quality and reliability.

46. Northern Indiana comments that third-party vendors working for NERC must comply with the CIP Reliability Standards, e.g., background checks, just as Northern Indiana's third-party vendors must. Otherwise, NERC's vendors should not be given access to critical cyber assets.

3. Commission Determination

47. The Commission adopts the CIP NOPR approach regarding NERC and Regional Entity compliance with the CIP Reliability Standards. The Commission maintains its belief that NERC's compliance is necessary in light of its interconnectivity with other entities that own and operate critical assets. Further, we conclude that NERC's Rules of Procedure, which state that the ERO will comply with each Reliability Standard that identifies the ERO as an applicable entity, provide an adequate means to assure that NERC is obligated to comply with the CIP Reliability Standards. Likewise, the delegation agreements between NERC and each Regional Entity expressly state that the Regional Entity is committed to comply with approved Reliability Standards.[29] Based on these provisions, we find that the Commission has authority to oversee the compliance of NERC and the Regional Entities with the CIP Reliability Standards.

48. With regard to EEI's concerns about NERC's incentives to comply with the CIP Reliability Standards, we believe that NERC's position as overseer of Bulk-Power System reliability provides a level of assurance that it will take compliance seriously. Moreover, section 215(e)(5) of the FPA provides that the Commission may take such action as is necessary or appropriate against the ERO or a Regional Entity to

[26] *E.g.*, Duke, EEI, Energy Producers, Northeast Utilities and Reliant.

[27] *See, e.g.*, Alliant, Mr. Brown, Duke, EEI, ISO/RTO Council, NRECA, PG&E, SDG&E and Tampa Electric.

[28] Alliant, Mr. Brown, PG&E, SDG&E and Tampa Electric agree with EEI's position.

[29] In Order No. 693, at P 157, the Commission directed NERC to remove each reference to the Regional Reliability Organization and replace it with a reference to the Regional Entity. This directive applies to the CIP Reliability Standards as well.

ensure compliance with a Reliability Standard or Commission order.[30]

49. The Commission also adopts its CIP NOPR approach and concludes that reliance on the NERC registration process at this time is an appropriate means of identifying the entities that must comply with the CIP Reliability Standards.[31] We are concerned, like the California Commission, that some small entities that are not identified in the NERC registry may become gateways for cyber attacks. However, we are not prepared to adopt California Commission's suggested approach of requiring that any entity connected to the Bulk-Power System, regardless of size, must comply with the CIP Reliability Standards irrespective of the NERC registry. We believe this approach is overly-expansive and may raise jurisdictional issues. Rather, we rely on NERC and the Regional Entities to be vigilant in assuring that all appropriate entities are registered to ensure the security of the Bulk-Power System.

50. With regard to EEI's request for clarification, the NERC registry process is designed to identify and register entities for compliance with Reliability Standards, and not identify lists of assets. In the CIP NOPR, the Commission explained that it would expect NERC to register the owner or operator of an important asset, such as a blackstart unit, even though the facility may be relatively small or connected at low voltage.[32] While the facility would not be registered or listed through the registration process, NERC's or a Regional Entity's awareness of the critical asset may reasonably result in the registration of the owner or operator of the facility.

51. Likewise, we believe that NERC should register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk-Power System. EEI and ISO/RTO Council concur that the need for the registration of demand side aggregators may arise, but state that it is not clear whether aggregators fit any of the current registration categories defined by NERC. We agree with EEI and ISO/RTO Council that NERC should consider whether there is a current need to register demand side aggregators and, if so, to address any related issues and develop criteria for their registration.

52. The Commission agrees with the many commenters that suggest that the responsibility of a third-party vendor for compliance with the CIP Reliability Standards is a matter that should be addressed in contracts between the registered entity that is responsible for mandatory compliance with the Standards and its vendor. To the extent that the responsible entity makes a business decision to hire an outside contractor to perform services for it, the responsible entity remains responsible for compliance with the relevant Reliability Standards. Thus, it is incumbent upon the responsible entity to assure that its third-party vendor acts in compliance with the CIP Reliability Standards. We agree with ISO/RTO Council's characterization of the matter:

> . . . when an application is developed and maintained by an outsourced provider, that outsourced provider manages physical and cyber access to the environment on which the application runs and therefore must be contractually obligated to the Responsible Entity to comply with the Reliability Standards.
>
> While such providers are not registered entities subject to the Reliability Standards, they must perform the services and operate the applications in a manner consistent with the Reliability Standards . . . the Responsible Entity should be charged with incorporating contractual terms and conditions into agreements with third-party service providers that obligate the providers to comply with the requirements of the Reliability Standards. In that regard, if a Responsible Entity determines that it is necessary to outsource a service that is essential to the reliable operation of a Critical Asset, Critical Cyber Asset, or the bulk electric system, it is clear that the Responsible Entity must be held responsible and accountable for compliance with the Reliability Standards.[33]

53. Further, it is incumbent upon a responsible entity to conduct vigorous oversight of the activities and procedures followed by the vendors they employ. Thus, we expect a responsible entity to address in its security policy under CIP–003–1 its policies regarding its oversight of third-party vendors.

D. Compliance Measured by Outcome

1. Performance-Based Standards

a. NOPR Proposal

54. The CIP NOPR expressed concern that the lack of specificity within the proposed CIP Reliability Standards could result in inadequate implementation efforts and inconsistent results.[34] In addressing the appropriate amount of specificity, the Commission stated that ''performance-based standards may not always be appropriate, for example, in situations where the 'how' may be inextricably linked to the Reliability Standard and may need to be specified to ensure the enforceability of the standard.'' [35] Thus, the Commission indicated that it may be appropriate to direct NERC in specific instances to develop modifications to the CIP Reliability Standards to address the ''how.''

55. The CIP NOPR also noted that the CIP Reliability Standards do not provide a mechanism to measure performance. The Commission identified three strategies for monitoring performance: (1) Internal and external oversight of a responsible entity's activities; (2) documenting, monitoring and revisiting a responsible entity's exercise of flexibility in a way that excepts it from a Requirement; and (3) reporting certain wide-area information and analysis to the Commission.

b. Comments

56. NERC and others comment that the CIP Reliability Standards should prescribe what outcome must be accomplished, but should not prescribe how that outcome is accomplished.[36] These commenters contend that discussion on how to implement a Requirement should be provided in a separate reference document such as guidelines or white papers, but not included in the CIP Reliability Standards themselves. This approach would allow responsible entities to retain the flexibility to implement a solution that best meets their needs.[37] According to NERC, including ''how'' language in the CIP Reliability Standards would dictate the only acceptable manner of implementation and thwart other acceptable, and possibly superior, methods of satisfying the Reliability Standards. In contrast, a guidance document allows more flexibility and is more easily updated as technology advances.

57. In addition, NERC expresses concern that including acceptable solutions as part of the CIP Reliability Standards could introduce common vulnerabilities based on all industry participants using a nearly identical solution to a given vulnerability.[38] PSEG Companies share this concern, adding that identifying the technology

[30] Section 39.9 of the Commission's regulations provides similar language to that of the statute. In Order No. 672, the Commission discussed its authority to take action against the ERO or a Regional Entity and the types of actions that are available. *See* Order No. 672 at P 761–62.

[31] CIP NOPR at P 26–30.

[32] *Id.* P 29.

[33] ISO/RTO Council comments at 21–22.

[34] CIP NOPR at P 32, citing CIP Assessment at 3.

[35] *Id.* at P 33, quoting Order No. 672 at P 260.

[36] *E.g.*, EEI, Alliant, Arizona Public Service, Mr. Brown, FirstEnergy, ISO/RTO Council, Luminant, Northeast Utilities, Ontario Power, PSEG Companies, Puget Sound and Southern.

[37] *E.g.*, NERC, ReliabilityFirst and Mr. Brown.

[38] Ontario Power and ReliabilityFirst raise similar concerns.

to be used to combat vulnerabilities creates vulnerabilities and allows hackers to focus their efforts on disrupting those systems. NERC and ReliabilityFirst also argue that guidance to address every contingency would be voluminous and difficult to write.

58. A number of commenters also provide comment regarding performance measurement and the Commission's proposal for internal and external oversight. NERC contends that much of the proposed additional oversight is in place in the existing ERO and regional compliance and audit programs. NERC explains that these programs are being updated based on the Requirements of the CIP Reliability Standards.

59. Other commenters, such as EEI, ISO/RTO Council and Puget Sound, suggest that the determination of whether a responsible entity meets or fails to meet the requirements of a CIP Reliability Standard should be determined in an audit based on the specific facts and circumstances of its use, ownership or operation of the Bulk-Power System. EEI argues that a strong auditing requirement serves to ensure quality control, and will result in consistency in the implementation of the CIP Reliability Standards. KCPL states that the information technology associated with cyber security provides a unique challenge for the audit function and auditors must have a significant amount of experience with both the industry and the cyber security needs to ensure that the obligations to the CIP Reliability Standards are properly evaluated during an audit. SERC–CIPC adds that the distinction between mandatory requirements and non-binding guidance should be made clear to auditors, noting that these differences could be subtle.

60. With regard to external oversight, Northern Indiana believes that certain independent entities' employees ''such as [those performing] the internal audit function'' can provide a wide-area view. Northern Indiana requests clarification on what the Commission means by the term ''external oversight.''

c. Commission Determination

61. The Commission received comments on both sides of the issue of specificity. Some commenters caution against the CIP Reliability Standards being too specific, while others request more guidance to help them comply. In general, the Commission believes it is appropriate to provide sufficient guidance to explain Requirements so that responsible entities have a high degree of certainty that they understand what is necessary to comply with a Requirement. More guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and effectively. Additional guidance need not be included in a specific Requirement, but could be in the form of examples. The Commission is not directing that the ERO establish a specific end result. Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by-case basis. Therefore, in several instances throughout this Final Rule, the Commission gives the ERO direction to provide additional guidance. In some cases, we require that the guidance be placed in modifications to the CIP Reliability Standards. In other cases, we note that some or all of the additional guidance could be placed in a reference document separate from the CIP Reliability Standards.

62. Some of the more specific directives in this Final Rule pertain to issues that the Commission considers necessary to carry out its statutory responsibilities. Examples of this include areas of oversight, exceptions to Requirements, and reports to the Commission. In developing these directives, we have tried to strike a balance between our needs to implement the statute and the concerns expressed by commenters.

63. We agree in general with commenters who point out that compliance issues should be determined in audits and that a strong auditing process will help to ensure quality control and consistency in the implementation of the CIP Reliability Standards. However, we point out that audits are only one aspect of the ERO's compliance monitoring and enforcement process. All aspects of that process must function well. In addition, we note compliance audits are conducted after-the-fact and do not diminish the necessity for internal and external reviews of compliance efforts, including the identification of critical assets and critical cyber assets.

64. In response to Northern Indiana, we explain ''external oversight'' in our discussions and determinations of specific Requirements in the Final Rule.

2. Adequacy of Outcomes

a. NOPR Proposal

65. The CIP NOPR noted that many of the Requirements of the CIP Reliability Standards consist of broad directives, with corresponding Measures and Compliance provisions focusing largely on proper documentation.[39] The Commission asserted that documentation by itself does not satisfy the Requirements of a Reliability Standard and, rather, implementation of the substance of the Requirements is most important in determining compliance.

66. The Commission also noted that, while certain Requirements of the CIP Reliability Standards obligate a responsible entity to develop and maintain a plan, policy or procedure, the Requirements do not always explicitly require implementation of the plan, policy or procedure. The Commission proposed to interpret such provisions to include an implicit implementation requirement.

b. Comments

i. Documentation

67. SPP and ReliabilityFirst agree with the Commission that adequate documentation does not substitute for substantive compliance with the responsibilities set forth in the requirements of the CIP Reliability Standards. However, they express concern that not relying on objective documentation requirements to demonstrate compliance could result in subjective variations in the audit process and uneven application of the Requirements of a Reliability Standard. ReliabilityFirst states that, while it is reasonable to apply subjective reasoning as part of a readiness assessment, any audit that could result in financial sanctions for non-compliance must rely solely upon clearly defined objective measures. To remedy the concern that documentation may not assure compliance with a CIP Reliability Standard, SPP suggests that the Requirements and Measures prescribed in a CIP Reliability Standard be enhanced to define the minimum acceptable documentation content.

68. In the context of measuring performance, Northern Indiana states that it generally supports the Commission's desire to clarify the CIP Reliability Standards but cautions the Commission from prescribing modifications that would limit a responsible entity's discretion. Northern Indiana comments that, while in some instances (such as testing vulnerabilities on a real-time, active system basis) documentation should suffice to demonstrate compliance, in other situations documentation does not suffice. In these instances, even though the responsible entity's documentation may comply with the CIP Reliability

[39] CIP NOPR at P 35–41.

Standards, the responsible entity must nevertheless demonstrate actual compliance. In these cases, Northern Indiana suggests that compliance can be verified in a subsequent audit.

69. Xcel notes that, in the CIP NOPR, the Commission indicated that ''compliance will in all cases be measured by whether a party met or failed to meet the Requirement given the specific facts and circumstances.'' [40] Xcel agrees that the Requirements contain the substantive obligations of a CIP Reliability Standard. Xcel asks the Commission to clarify whether an entity that complies with the substance of the Requirements but violates the documentation provisions of the Measures or Levels of Non-Compliance may be assessed a penalty. Xcel suggests that penalties are not warranted in this circumstance.

ii. Obligation to Implement Plans, Policies and Procedures

70. EEI, FirstEnergy, ISO/RTO Council, Northeast Utilities and PG&E agree that certain CIP requirements do not explicitly require implementation of a plan, policy or procedure that the responsible entity is required to develop and maintain. Thus, they support directing NERC, in the course of its scheduled industry Reliability Standards development process, to consider making explicit that a responsible entity must implement a plan, policy or procedure that it is required to develop.

71. Xcel asks the Commission to clarify what it means to implement a plan, policy or procedure. Specifically, Xcel asks the Commission to clarify that ''this does not mean that an entity has to follow every aspect of its plans, policies or procedures to the letter or be in violation * * *.'' [41] Xcel comments that following every feature of a plan in all cases would hinder the flexibility that an entity needs to respond effectively to a particular situation. Further, according to Xcel, the Commission's proposal would make each plan, policy and procedure tantamount to an enforceable Reliability Standard. Xcel claims that this would give entities an incentive to include fewer details in their plans, policies and procedures.

c. Commission Determination

i. Documentation

72. While the Commission agrees with commenters that relying on an objective determination such as whether a document exists would facilitate the compliance audit process, we do not believe such a cursory approach is the best way to ensure the protection of the Bulk-Power System. We adopt our proposal in the CIP NOPR that responsible entities must comply with the substance of a Requirement. In this way we affirm the Commission's position established in Order No. 693 that, ''while Measures and Levels of Non-Compliance provide useful guidance to the industry, compliance will in all cases be measured by determining whether a party met or failed to meet the Requirement given the specific facts and circumstance of its use, ownership or operation of the Bulk-Power System.'' [42] While we agree with Northern Indiana that, depending on the Requirement in question, in some instances (such as active system testing) documentation would suffice to demonstrate compliance, even in these cases auditors should look at the content of the documentation to determine if the substance of the Requirement has been met.

73. Xcel seeks clarification regarding responsible entities that comply with the substance of a Requirement but violate the documentation provisions. In Order No. 693, in response to a similar request by Xcel, the Commission explained that, ''[w]hile the Commission generally agrees that it is a violation of the Requirements that is subject to a penalty, we recognize that because Measures are intended to gauge or document compliance, failure to meet a Measure is almost always going to result in a violation of a Requirement.'' [43] We add that a responsible entity's failure to maintain documentation (as set forth in a Measure) that obstructs the ability of the ERO, Regional Entity or Commission to determine compliance with the substance of a Requirement may warrant a penalty.

ii. Obligation To Implement Plans, Policies and Procedures

74. In the CIP NOPR, the Commission also noted that, while certain Requirements of the CIP Reliability Standards obligate a responsible entity to develop and maintain a plan, policy or procedure, the Requirements do not always explicitly require implementation of the plan, policy or procedure. The Commission proposed to interpret such provisions to include an implicit implementation requirement.

75. Consistent with that proposal, the Commission concludes that, where the CIP Reliability Standards obligate a responsible entity to develop and maintain a plan, policy or procedure, there should be a corresponding obligation to implement the plan, policy or procedure. However, while the CIP NOPR proposed to interpret the CIP Reliability Standards as including an implicit obligation to implement plans, policies and procedures, we are persuaded by the commenters that a better approach is for the ERO to develop modifications to the CIP Reliability Standards that contain appropriate implementation language. Accordingly, we direct the ERO to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards.

76. As to Xcel's argument that, at times, the proper course is to deviate from a plan, we agree that the details of such plans are not equivalent to Requirements of a CIP Reliability Standard. However, the responsible entity's plan should be followed unless a deliberate decision is made for good reason not to follow it. Such reason should be documented and available for compliance auditors to review. Merely ignoring plan provisions is equivalent to not having a plan. For clarity, we note that a decision not to follow a particular plan provision due to circumstances will not except a responsible entity from a related Requirement in a CIP Reliability Standard. As discussed below, we find that any exception to a CIP Reliability Standard must comply with the required conditions for a technical feasibility exception.

E. Implementation Plan

77. In the CIP NOPR, the Commission explained that, because the CIP Reliability Standards are new and require applicable entities in many cases to develop new cyber security systems and procedures, NERC developed an implementation plan based on a schedule that provides for implementation of the CIP Reliability Standards over a three-year period.[44] The implementation plan sets out a proposed schedule for accomplishing the various tasks associated with compliance with the CIP Reliability Standards. The schedule gives a timeline by calendar quarters for completing various tasks and prescribes

[40] Xcel comments at 5, quoting CIP NOPR at P 39 (in turn quoting Order No. 693 at P 253).

[41] Xcel comments at 7.

[42] Order No. 693 at P 253.

[43] *Id.* P 256.

[44] CIP NOPR at P 42. *See also* NERC August 28, 2006 Filing, Exhibit B ''Implementation Plan for Cyber Security Standards'' (implementation plan).

milestones for when a responsible entity must: (1) ''Begin work''; (2) ''be substantially compliant'' with a Requirement; (3) ''be compliant'' with a Requirement; and (4) ''be auditably compliant'' with a Requirement. According to the implementation plan, ''auditably compliant'' must be achieved in 2009 for certain Requirements by certain responsible entities, and in 2010 for others.

1. Commission Approval of Implementation Plan

a. NOPR Proposal

78. The Commission proposed to approve NERC's implementation plan, including the proposed timelines for achieving compliance.[45] The Commission stated its belief that the timetable proposed by NERC sets reasonable deadlines for industry compliance, recognizing the broad industry input to its development, and the tasks that many responsible entities face to purchase and install new equipment and software to achieve compliance.

b. Comments

79. Numerous commenters urge the Commission to accept NERC's proposed implementation plan and the proposed timeline for achieving compliance with the CIP Reliability Standards.[46] For example, Applied Control Solutions comments that, due to real cyber vulnerabilities to the grid, there is an urgent need to move forward with the effective dates without delay and not allow any extension of those dates. KCPL states that the implementation plan has been developed based on input from industry stakeholders and the timetables and processes agreed upon in that process represent prudent steps toward the implementation of the CIP Reliability Standards.

80. Many of these same commenters express concern about how the Commission's proposal in the CIP NOPR to direct that NERC develop certain modifications to the CIP Reliability Standards would affect the implementation schedule. NERC explains that the implementation plan and time frame are for the existing CIP Reliability Standards as submitted to the Commission. NERC states that any changes to the CIP Reliability Standards resulting from the Final Rule will potentially impact the implementation plan and time frame, and a new schedule will need to be developed during the Reliability Standards development process associated with those changes.[47]

81. Similarly, EEI and Entergy advocate that the Final Rule make clear that modifications developed pursuant to the Reliability Standards development process should not be implemented until the conclusion of the NERC implementation plan.[48] PSEG Companies add that responsible entities have already developed budgets and implementation plans in reliance on the existing CIP Reliability Standards. PSEG Companies indicate that, although they may ultimately support some of the changes proposed in the CIP NOPR, they cannot support modifying the current CIP Reliability Standards before the 2009 compliance deadline. EEI and Alliant claim that, if the Commission directs the NERC Reliability Standards development process to consider potential changes to the CIP Reliability Standards before the conclusion of the implementation plan, responsible entities will be significantly discouraged from performing any further work until these changes are finalized. Thus, implementation work may slow or come to a stop because responsible entities will have an incentive to wait for the final outcome of this Commission-imposed revision process.

82. Manitoba Hydro comments that the Commission should reject NERC's proposed implementation schedule because it is based on the unrealistic expectation that the CIP Reliability Standards would be approved without the need for any revisions. Muscatine Power & Water argues that if the Commission requires utilities to base their risk-based assessments on formal guidelines provided by NERC, then the implementation schedule must be extended to allow additional time for compliance.

83. APPA/LPPC suggest the implementation plan may need adjustment if the Regional Entities or some other region-wide institutions supplement a responsible entity's list of critical assets. In such cases, APPA/LPPC request that the Commission direct NERC to develop a reasonable schedule for determining the timeline for being auditably compliant with respect to the newly designated assets.

84. Entergy characterizes the CIP NOPR as proposing to ''remand'' CIP–002–1, which according to Energy would leave unresolved the basic issue of which assets are subject to the CIP Reliability Standards. Entergy contends that without knowledge of which assets the CIP Reliability Standards apply, the proposed timeline is unworkable.

85. SPP maintains that there is no table prescribing a schedule in which an existing registered entity can bring a newly identified critical asset and its critical cyber assets into compliance. While not expected to change frequently, the critical asset list can change for any number of valid reasons, and the registered entity needs an appropriate period of time in which to achieve compliance for that asset. In the absence of a compliance schedule, no guidance is available to either the registered entity or the auditor. SPP recommends that a new table be developed defining a compliance schedule for newly identified critical assets and based upon the date of the risk-based assessment. SPP argues that the table should include milestones for tasks already completed and milestones for tasks yet to be done that will require additional resources and time to comply.

c. Commission Determination

86. The Commission adopts its CIP NOPR proposal and approves NERC's implementation plan and time frames for responsible entities to achieve auditable compliance. Responsible entities require a reasonable period of time to purchase and install new cyber software and equipment and develop new programs and procedures to achieve compliance. Commenters indicate that the implementation plan provides that reasonable period of time. Further, we agree with commenters that there is an urgent need to move forward without any delays. Accordingly, we approve NERC's implementation plan.

87. Commenters raise concerns regarding the impact on the implementation plan of the Commission's directives for modifications to the CIP Reliability Standards. As explained above, the Commission is not modifying the CIP Reliability Standards in this Final Rule. Rather, pursuant to section 215(d)(5) of the FPA, the Commission in the Final Rule directs the ERO to develop certain modifications to the CIP Reliability Standards pursuant to the NERC Reliability Standards development process. Even though the development of such modifications will take time, this does not present a reason for delay or revision to the NERC implementation plan for implementing the CIP

[45] *Id.* P 47.

[46] *E.g.,* NERC, Applied Control Solutions, EEI, FirstEnergy, KCPL, PG&E and Progress.

[47] *See also* Allegheny, Alliant, Detroit Edison, Duke, EEI, Entergy, FPL Group, Idaho Power, KCPL, Manitoba Hydro, MidAmerican, National Grid, OGE, Ontario IESO, PG&E, PSEG Companies, Southern, Teltone and Xcel.

[48] EEI at 6. Elsewhere, EEI states that the Commission should not direct NERC to consider changes to the CIP Reliability Standards before the conclusion of the NERC implementation plan. EEI at 7–8.

Reliability Standards approved in this Final Rule.

88. The Commission believes that the modifications to the CIP Reliability Standards developed by the NERC Reliability Standards development process should not be audited prior to the conclusion of the approved implementation plan. EEI and other commenters claim that commencing the development of such modifications prior to the conclusion of the implementation plan would be discouraging to industry. The Commission, however, finds that it is unacceptable to delay the development of the modifications directed in this Final Rule until after the conclusion of the implementation plan. Since it is uncertain how long it will take to develop revised CIP Reliability Standards, we believe it is not reasonable to wait until the 2009–2010 time period for the process to start. Features such as enhanced conditions on technical feasibility exceptions and oversight of critical asset determinations are too important to the protection of the Bulk-Power System to wait that long.

89. While we are both sympathetic and concerned about straining industry resources, the Commission and the electric industry must do their best to protect the electric infrastructure that is essential to the health and safety of the nation. Therefore, we direct the ERO to submit a work plan for Commission approval for developing and filing for approval the modifications to the CIP Reliability Standards that we are directing in this Final Rule. As suggested by NERC, the Commission will consider a second implementation plan for achieving compliance with the forthcoming revised CIP Reliability Standards.

90. The Commission did not propose to remand CIP–002–1 as argued by Entergy. Nonetheless, Entergy raises a valid concern since the Commission's directive, discussed below, that the ERO develop modifications to CIP–002–1 could affect a responsible entity's identification of critical assets. We share Entergy's concern that there are threshold issues regarding CIP–002–1 that must be addressed before responsible entities can have certainty regarding which assets must be protected according to the CIP Reliability Standards. We also believe that responsible entities need certainty regarding the conditions for a technical feasibility exception to inform their decisions about how to comply with the CIP Reliability Standards, even in their current form. Therefore, we direct the ERO, in its development of a work plan, to consider developing modifications to CIP–002–1 and the provisions regarding technical feasibility exceptions as a first priority, before developing other modifications required by the Final Rule.

2. Self-Certification

a. NOPR Proposal

91. In the CIP NOPR, the Commission expressed concern over whether responsible entities will be fully prepared for compliance upon reaching the implementation deadline and will take reasonable action to protect the Bulk-Power System during the interim period.[49] The Commission stated that NERC's plans to require self-certification during the interim period are helpful and proposed that, to allow adequate monitoring of progress, the ERO develop a self-certification process with certifications more frequent than once per year. The CIP NOPR suggested that self-certification be tied either to target dates in the schedule or perhaps quarterly or semi-annual certifications. The Commission indicated that, while an entity should not be subject to a monetary penalty if it is unable to certify that it is on schedule, such an entity should explain to the ERO the reason it is unable to self-certify. The ERO and the Regional Entities should then work with such an entity either informally or, if appropriate, by requiring a remedial plan, to assist such an entity in achieving full compliance in a timely manner. We also stated that the ERO and the Regional Entities should provide informational guidance, upon request, to assist a responsible entity in assessing its progress in reaching ''auditably compliant'' status.

b. Comments

92. Many commenters oppose directing NERC to consider a self-certification process with more frequent self-certifications than on an annual basis.[50] In this regard, EEI argues that a more frequent self-certification requirement is likely to impose undue burdens without commensurate benefits. KCPL claims that there are sufficient processes already in place in order to evaluate and monitor CIP Reliability Standards compliance and additional requirements for self-certification provide no significant support or benefit to tracking a Responsible Entity's obligations to the CIP Reliability Standards and are unneeded.

93. Other commenters, such as APPA/LPPC, MidAmerican, Northern Indiana and SDG&E either support or do not object to more frequent self-certifications. APPA/LPPC support NERC's proposed self-certification process as a reasonable means of tracking the progress made by responsible entities toward full, auditable compliance. Nor do they object to the Commission's proposal that such certification be rendered quarterly or semi-annually. Northern Indiana supports semi-annual self-certification during the transition until the implementation plan is completed. Northern Indiana contends that more frequent self-certification would be unduly burdensome.

94. METC–ITC also support quarterly or semi-annual self-certifications because the certifications will properly pressure entities to take timely steps to achieve compliance by the deadline for auditable compliance. METC–ITC are concerned, however, that having NERC monitor progress toward compliance with the CIP Reliability Standards via self-certifications, may place a burden on the ERO and the Regional Entities that their current staffs may be unable to properly administer. Thus, METC–ITC propose that the Commission require the ERO to file plans addressing how it will satisfy the new requirements for providing assistance to responsible entities and further assessing CIP implementation as part of its readiness reviews.

95. SDG&E supports semi-annual certifications, but comments that quarterly certifications would be distracting to the main goal, as well as burdensome, time consuming and paper intensive. It agrees with the Commission that an entity should not be penalized if it cannot certify that it is on schedule. SDG&E does not object to the Commission's proposal that the ERO and the Regional Entities should work with such an entity to achieving full compliance, provided that the Commission clarify that this means ''getting back'' on schedule and not accelerating compliance.

c. Commission Determination

96. While the Commission is sensitive to concerns that more frequent self-certifications may be burdensome, it is important that the ERO and the Commission know whether industry, or segments of industry, are having difficulty implementing the CIP Reliability Standards. Therefore, we direct the ERO to require more frequent, semi-annual, self-certifications prior to

[49] CIP NOPR at P 48.

[50] *E.g.*, Alliant, Bonneville, Entergy, EEI, ISO–NE, KCPL, National Grid, Northeast Utilities, PG&E, Portland General, Progress, Puget Sound and Southern.

the date by which full compliance is required. Such additional self-certifications may be a ''stream-lined'' version, but must be useful for the ERO and the Commission to assess industry's progress toward achieving compliance with the CIP Reliability Standards.

97. Further, we adopt our CIP NOPR proposals that, while an entity should not be subject to a monetary penalty if it is unable to certify that it is on schedule, such an entity should explain to the ERO the reason it is unable to self-certify. The ERO and the Regional Entities should then work with such an entity either informally or, if appropriate, by requiring a remedial plan to assist such an entity in achieving full compliance in a timely manner. Further, we expect the ERO and the Regional Entities to provide informational guidance, upon request, to assist a responsible entity in assessing its progress in reaching ''auditably compliant'' status.

98. With regard to METC–ITC's comment, we will not require NERC and the Regional Entities to submit plans describing how it will undertake these responsibilities. Rather, the ERO and Regional Entities can address any need for additional resources in the ERO's annual budget filing. If necessary to fulfill their statutory obligations, the ERO and Regional Entities may file a request for additional funding to supplement their Commission approved budgets.

99. With regard to SDG&E's comment, we clarify that the goal of a Regional Entity working with a responsible entity that is unable to self-certify is to assist the entity in meeting the NERC time frames for auditable compliance, and not to accelerate compliance ahead of schedule.

3. Adding a Cyber Security Assessment to NERC's Readiness Reviews

a. NOPR Proposal

100. To further address the Commission's concerns about the period prior to when responsible entities achieve full compliance with the CIP Reliability Standards, the CIP NOPR also proposed that the ERO add a cyber security assessment to NERC's existing readiness reviews.[51] The Commission explained that the assessment should identify best practices and deficiencies of the reviewed entities to assist them in preparing for implementation of the CIP Reliability Standards and help the Commission evaluate the potential effectiveness of the Standards before full implementation.

[51] CIP NOPR at P 49.

b. Comments

101. NERC and other commenters oppose the addition of a cyber security assessment to NERC's existing readiness reviews.[52] NERC requests that the Commission allow the existing oversight framework to work without adding new or different requirements specific to the CIP Reliability Standards. EEI points out that, because readiness reviews are not conducted on an annual basis, the review would not occur early enough in the implementation process to assist responsible entities' implementation of the CIP Reliability Standards or assist the Commission in assessing the status of compliance efforts. EEI also asserts that the most likely result of adding a cyber security assessment to NERC's readiness reviews would be to unnecessarily distract responsible entities from performing the actual implementation of the CIP Reliability Standards. Southern adds that such assessments would merely duplicate the self-certifications.

102. Northeast Utilities asks the Commission to reconsider its proposal prior to the 2009 deadline for full compliance with the CIP Reliability Standards. According to Northeast Utilities, readiness reviews are performed by industry peer volunteers under Regional Entity guidance to identify best practices and ensure that system operators have the tools, processes and procedures in place to operate reliably. It contends that, given the limited industry experience with cyber security, the readiness review process will not produce the benefits the Commission expects.

103. In contrast, MidAmerican and SDG&E agree with the Commission that adding a cyber component to the readiness audit process would be beneficial, provided an exception is made for publication of any weaknesses found during a typical readiness audit. They submit that any areas of concern uncovered by the audit should be considered sensitive and confidential with appropriate safeguards developed and in place to protect this information. MidAmerican also recommends that the Commission consider including a cyber security assessment within the ERO's existing readiness reviews.

104. Xcel asks the Commission to clarify that the CIP NOPR, in proposing that NERC add cyber security assessments to its existing schedule of reliability readiness reviews, did not intend for NERC to revise its schedule of reviews but, rather, add a new element to the previously-scheduled reviews.

[52] *E.g.,* Alliant, Bonneville, EEI, ISO–NE, Luminant, Northeast Utilities, Southern and Tampa Electric.

c. Commission Determination

105. The Commission is persuaded by comments regarding the limited reach of readiness reviews and the questionable utility of such reviews prior to the date by which entities are to be compliant; thus, adding the CIP Reliability Standards to the readiness reviews at this time will delay industry's compliance efforts. Therefore, the Commission will not require that the CIP Reliability Standards be added to the readiness reviews at this time.

F. Issues Presented by Terminology

106. The CIP NOPR discussed specific terminology used in the CIP Reliability Standards that, while providing flexibility for a responsible entity in achieving compliance, also raise concerns regarding enforceability of the Standards. Specifically, the Commission raised concerns regarding the terms ''reasonable business judgment,'' ''acceptance of risk,'' and ''technical feasibility.'' As discussed below, the Commission adopts the CIP NOPR proposals and directs NERC to modify the CIP Reliability Standards through the Reliability Standards development process to remove the first two terms, and develop specific conditions that a responsible entity must satisfy to invoke the ''technical feasibility'' exception. Moreover, in response to concerns raised by commenters, the Commission has changed certain conditions for invoking the technical feasibility exception.

1. Reasonable Business Judgment

a. NOPR Proposal

107. As we stated in the CIP NOPR,[53] each of the proposed CIP Reliability Standards incorporates the concept of ''reasonable business judgment'' as a guide for determining what constitutes appropriate compliance with those Reliability Standards. The Purpose statement of Reliability Standard CIP–002–1 provides that:

> These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible entities should interpret and apply Standards CIP–002 through CIP–009 using reasonable business judgment.

108. In addition, each of the subsequent CIP Reliability Standards (*i.e.*, CIP Reliability Standards CIP–003–1 through CIP–009–1) includes a

[53] CIP NOPR at P 50.

statement that ''Responsible Entities should interpret and apply the Reliability Standard using reasonable business judgment.''

109. The Commission pointed out in the CIP NOPR that NERC's Glossary of Terms Used in Reliability Standards (NERC Glossary) does not define reasonable business judgment, and the CIP Reliability Standards do not otherwise suggest how the term is to be interpreted. NERC's Frequently Asked Questions (FAQ) document that accompanies the CIP Reliability Standards provides the only available guidance on the issue.[54] It states that the phrase is meant ''to reflect—and to inform—any regulatory body or ultimate judicial arbiter of disputes regarding interpretation of these Standards—that responsible entities have a significant degree of flexibility in implementing these Standards.'' The FAQ document notes that there is a long history of judicial interpretation of the business judgment rule and states that ''[c]ourts generally hold that the phrase indicates reviewing tribunals should not substitute their own judgment for that of the entity under review other than in extreme circumstances.''

110. The Commission proposed, in the CIP NOPR, to direct the ERO to modify the CIP Reliability Standards to remove references to the ''reasonable business judgment'' language before compliance audits start in 2009.[55] In the CIP NOPR, the Commission discussed the history of the reasonable business judgment concept and the meaning attached to that concept by the courts in the corporate context.[56] The Commission pointed out that, if this term is applied to the CIP Reliability Standards, it could easily be understood to have the same meaning as in the corporate context.

111. The Commission noted that flexibility and discretion are essential in implementing the CIP Reliability Standards and that implementing those Reliability Standards must be done on the basis of the specific facts and circumstances applicable in the individual case at hand. Cyber security problems do not lend themselves to one-size-fits-all solutions. In addition, the Commission acknowledged that cost can be a valid consideration in implementing the CIP Reliability Standards. However, the Commission concluded that the traditional concept of reasonable business judgment is ill suited to the task of implementing an appropriate program of cyber security pursuant to section 215 of the FPA.

112. That concept was developed specifically to address the issue of how courts should approach business decisions made by a company's officers or directors, and the answer it provides is based on certain assumptions about how our economic system operates and who is most likely to have the knowledge and expertise needed to make appropriate business decisions. However, the concept of reasonable business judgment takes on a very different meaning when removed from its original context and applied to a different factual situation where very different assumptions apply.

113. The Commission noted in the CIP NOPR that cyber security standards are essential to protecting the Bulk-Power System against attacks by terrorists and others seeking to damage the grid. Because of the interconnected nature of the grid, an attack on one system can affect the entire grid. It is therefore unreasonable to allow each user, owner or operator to determine compliance with the CIP Reliability Standards based on its own ''business interests.'' Business convenience cannot excuse compliance with mandatory Reliability Standards. The Commission also noted that the explanation of reasonable business judgment found in the FAQ document closely tracks the treatment of the concept in the corporate law context.

114. The Commission stated that this test is fundamentally incompatible with Congress' decision to adopt a regime of mandatory Reliability Standards. The Commission explained that the issue under section 215 of the FPA is not whether the management of a business is acting in the interest of its own shareholders, but rather whether an entity is taking appropriate action to avert risks that could threaten the entire grid. Finally, the Commission noted that in the corporate governance context, the business judgment rule is invoked only in extreme circumstances, generally when an officer or director is found to have acted fraudulently, in bad faith, or with gross or culpable negligence. For all these reasons, the Commission proposed in the CIP NOPR that the ERO remove references to the ''reasonable business judgment'' language from the CIP Reliability Standards.

b. Comments

115. NERC and numerous parties, including California Commission, Texas Commission, ISO–NE and ReliabilityFirst, agree that references to reasonable business judgment should be removed from the CIP Reliability Standards. National Grid concurs to the extent that this language adds confusion by incorporating a business law concept into the CIP Reliability Standards or could be construed to allow responsible entities to avoid liability for violations unilaterally and subjectively. APPA/LPPC state that use of reasonable business judgment overstates the appropriate amount of discretion to the extent that term was intended to incorporate a body of law developed in the corporate governance context. NRECA agrees that the term would give responsible entities too much latitude in essence to exempt themselves from the CIP Reliability Standards. Xcel states that reasonable business judgment has developed an exculpatory meaning in corporate law that is not applicable to compliance with the CIP Reliability Standards. ISO–NE states that the term provides no measurable value to any of the Requirements and appears to be an open-ended caveat that is susceptible to abuse.

116. Texas Commission states that, in reviewing costs associated with upgrades for physical and cyber security for prudence, it applies a more rigorous criterion than reasonable business judgment. It argues that a looser criterion in the CIP Reliability Standards could require a company to purchase more equipment or software than would later be compensated for in their rates. Texas Commission states that reasonable business judgment does not relieve an entity from showing that any expenditures it made were just and reasonable as required in Texas Commission rate cases. Texas Commission concludes that it is in the best interest of regulated entities either to remove the term or to replace it with a more narrowly focused term with a clearly defined statutory basis.

117. Numerous commenters argue that use of the term reasonable business judgment was never intended to import corporate law concepts into the CIP Reliability Standards but rather to ensure that Responsible Entities have sufficient flexibility when implementing them.[57] EEI states that the term was intended to allow flexible but objective decision-making in determining an approach to compliance. It was not intended to provide flexibility on whether to comply, only on how to comply.

118. Mr. Brown states that neither the CIP Reliability Standards nor the FAQ document state that the use of

[54] NERC included the FAQ document in its August 28, 2006 filing. The FAQ document is also available at *ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Revised_CIP-002-009_FAQs_06Mar06.pdf.*

[55] CIP NORP at P 58.

[56] *Id.* P 59, 61.

[57] *E.g.*, Alliant, Arizona Public Service, EEI, PSE&G, SoCal Edison and Xcel.

reasonable business judgment would have the effects that the Commission suggests and that the Commission's description of the language and its potential effect is an effort to set up a ''straw man'' rather than address the clear intent of the language. He maintains that the Commission's analysis of the language is speculative and hyper-legalistic.

119. A number of commenters either oppose removal of reasonable business judgment from the CIP Reliability Standards or express serious concern about removing it. Tampa Electric argues that the term should be retained or at the very least replaced with language that ensures flexibility. SDG&E disagrees with wholesale elimination of the business judgment rule and instead urges that parameters or guidelines be adopted that determine when and how to apply the concept. MidAmerican suggests that it can be retained if accompanied by a mitigation plan with a sunset clause. Northern Indiana supports retaining the language, explaining that the CIP Reliability Standards are new, and the development of best practices regarding them continues to evolve. Responsible entities thus must have the flexibility to exercise discretion and make the appropriate strategic decisions when implementing the Reliability Standards.

120. A number of commenters argue that use of reasonable business judgment makes it clear that cost is a relevant factor. EEI states that a responsible entity is expected to weigh cyber security options in light of the risk to reliability in the same manner as similarly situated entities. Reasonable business judgment does not imply that it is acceptable to make purely economic choices to avoid protecting a critical cyber asset and thus to jeopardize grid reliability. Evaluating whether an asset is critical requires considering the asset's role, its cost, and the impact of the asset being compromised, as well as the costs of potential protection strategies, consistent with good business practice in the electric industry. EEI states that even with the inclusion of this language, the other requirements in the CIP Reliability Standards, such as documentation of decision-making and rigorous auditing, will prevent unfettered discretion in identifying and securing critical cyber assets.

121. Ontario Power states that outright removal will render the CIP Reliability Standards too rigid and that removal could be interpreted by some to mean that compliance is required regardless of the cost, the impact on production systems, or the risk to the Bulk-Power System. Tampa Electric argues that without the leeway afforded by reasonable business judgment, responsible entities could be forced into cost-prohibitive controls that do not add value in terms of security simply to satisfy an external requirement that is ill-fitted to the particular circumstances. SDG&E states that because the cost should not exceed the security benefit, certain security investments require business judgment. There must be latitude to develop a reasonable business case for determining the costs and benefits of investing in or implementing a security control based on key risk and investment factors specific to an entity.

122. A number of commenters defend the use of reasonable business judgment in terms that focus more on the issue of liability than simple flexibility or economic considerations. AMP-Ohio states that the plain language of the proposed CIP Reliability Standards could create a strict liability environment if there is no exception for ''good faith'' or ''reasonable judgment.'' Mr. Brown states that the proposal to remove the reasonable business judgment language appears to hold utilities, and perhaps individual managers, officers and directors, directly responsible for any adverse impact of decisions based upon their inherently imperfect knowledge and information regardless of whether they acted in good faith and made reasonably well-informed decisions. Entergy states that the industry must have reasonable assurance that the actions they are implementing meet the CIP Reliability Standards and Requirements if they acted in good faith, performed the proper evaluation, and took actions consistent with their evaluation.

123. Mr. Brown maintains that there are 200 years of legal precedent for determining what constitutes prudent behavior, and nothing in the legislative history of section 215 of the FPA suggests that Congress intended to depart from that precedent in this case. He states that the Commission should proceed with great caution when it proposes to depart from this precedent for determining prudent behavior without a clear, express mandate from Congress to do so.

124. EEI and other commenters argue that if the reasonable business judgment language is removed from the CIP Reliability Standards, it should be replaced with alternative language developed in the Reliability Standards development process.[58] They argue that such language is necessary to ensure necessary flexibility. National Grid states that the Commission should allow the ERO to develop suitable replacement language to allow for the reasonable flexibility that the Commission acknowledges that the industry requires in addressing critical infrastructure protection issues.

125. APPA/LPPC suggest that phrases such as ''reasonable judgment'' or ''judgment consistent with Good Utility Practice'' as substitutes for reasonable business judgment. A number of commenters, including NIPSCO and Georgia Operators, point to the phrase ''good utility practice'' in the pro forma OATT as a model or starting point for alternative language.

126. A number of commenters, including Manitoba Hydro and NRECA, criticize the proposal to remove references to reasonable business judgment as overly prescriptive. Manitoba Hydro states that the proposal appears to preclude the consideration of alternative wording. These commenters stress the importance of reliance on the Reliability Standards development process.

127. Southwest TDUs state that, while the Commission correctly proposes to eliminate the so-called business judgment rule, the CIP NOPR does not address the dichotomy in application of the CIP Reliability Standards between public and private entities. While the Commission correctly concludes that flexibility and discretion in implementation are necessary, there is no discussion of what that means for a public body, nor is there any recognition that a public body may be governed by state requirements and possibly by local ordinances.

c. Commission Determination

128. Consistent with the CIP NOPR, the Commission concludes that the concept of reasonable business judgment is inappropriate in the context of mandatory CIP Reliability Standards. Accordingly, the Commission directs the ERO to develop modifications to the CIP Reliability Standards that do not include this term. We note that many commenters, including NERC, agree that the reasonable business judgment language should be removed based largely on the rationale articulated by the Commission in the CIP NOPR.

129. While there may have been no intention to import corporate law concepts into the CIP Reliability Standards, it is difficult to draw any other conclusion on the basis of the

[58] *E.g.*, Arizona Public Service, Mr. Brown, Georgia Operators, KCPL, NRECA, Northern California, NIPSCO, Northeast Utilities, OGE, PG&E, SoCal Edison, Tampa Electric and Xcel.

documents provided. We note that the only guidance on reasonable business judgment that emerged from the Reliability Standards development process and that was supplied to the Commission is found in the FAQ document, and that document appears to invoke the traditional corporate law business judgment rule. The FAQ document specifically references existing court precedent on the rule, and it sets forth the elements of reasonable business judgment in what is essentially a restatement of classic formulations of the business judgment rule.[59] Moreover, the FAQ document specifically references one of the most objectionable aspects of the business judgment rule in the cyber security context, the requirement that the courts defer to the decisions of company officers and directors in all but the most extreme circumstances.

130. In short, the only explanation of reasonable business judgment in the documentation responsible entities would rely on focuses on corporate law concepts. We thus reject Mr. Brown's claim what we are being hyper-legalistic and constructing straw men rather than addressing the clear intent of the language. Mr. Brown fails to identify where some intent other than to adopt the traditional business judgment rule is clearly stated, and his references to 200 years of legal precedent only serve to reinforce our conclusion. We are unaware of any such extensive body of precedent on reasonable business judgment other than that developed in the corporate law context.

131. The most common argument raised in favor of reasonable business judgment is that it ensures flexibility. The Commission, however, acknowledged the importance of flexibility and discretion in the CIP NOPR.[60] The CIP Reliability Standards consist for the most part of quite general Requirements that must be implemented in a wide variety of circumstances. As drafted, they do not provide one-size-fits-all solutions and, rather, require responsible entities to assess their individual situations and devise solutions appropriate to their circumstances. We therefore disagree with Ontario Power that outright removal of all references to reasonable business judgment would render the CIP Reliability Standards too rigid. It will still be necessary for responsible entities to choose between available alternatives to arrive at cyber security solutions that best fit their situation. In short, the CIP Reliability Standards do not simply allow flexibility, they require it.

132. Many commenters suggest that the issue is not simply flexibility, but rather the flexibility to balance costs against other factors when implementing the CIP Reliability Standards. Many of the arguments about cost have been raised in connection with the problem of technical feasibility as it relates to long-life legacy equipment. We will address that issue below and note here simply that cost is a relevant consideration for those purposes, and recourse to reasonable business judgment is unnecessary to confirm that or to address the problem appropriately. Beyond that we disagree that deleting references to reasonable business judgment will lead to overly burdensome requirements or counterproductive results. For example, we disagree with Tampa Electric that without the leeway afforded by reasonable business judgment responsible entities would be forced into cost-prohibitive controls that do not add value in terms of security. No explanation was provided as to how this might occur. The Commission acknowledged the validity of cost considerations in the CIP NOPR and reaffirms that position here. The funds available for cyber security will not be infinite and, therefore, a responsible entity will need to make careful judgments to ensure that available funds are spent effectively. We do not see how the absence of references to reasonable business judgment will prevent this from happening.

133. Finally, some commenters link the need for flexibility with the problem of liability. We are keenly aware that unlike many other aspects of Bulk-Power System operations, cyber security represents a new and rapidly developing field. In other areas, the substance of appropriate practices is well established and well understood, but there can be considerably more uncertainty in the cyber security realm. Responsible entities therefore quite understandably wish to have, in Entergy's words, assurances that their actions meet the CIP Reliability Standards and Requirements if they act in good faith, perform the proper evaluation, and act consistent with their evaluation. We agree that they should have such assurances, but we disagree that references to reasonable business judgment are an appropriate way to provide such assurances. The real issue is whether responsible entities take reasonable and prudent actions based on an informed understanding of the current state of cyber security practice and how it applies to their situation. The Commission, therefore, disagrees with AMP-Ohio and Mr. Brown that the absence of references to reasonable business judgment will lead to a strict liability enforcement regime.

134. We disagree with Mr. Brown's claim that removal of reasonable business judgment could lead to liability for individual managers under section 215 of the FPA. That section applies to users, owners, and operators of the Bulk-Power System, and any liability arising under section 215 applies to them, not their employees.

135. Although we disagree with National Grid and others that alternative language is necessary to ensure necessary flexibility, we agree that the ERO and the participants in the Reliability Standards development process may choose to develop alternative language to replace reasonable business judgment and propose it for Commission approval. Such language would need to be adapted to the issues involved in forming judgments on proper cyber security measures and embody an objective standard focused on conduct that promotes the interests of Bulk-Power System security and reliability. Such language would also need to take into consideration our finding discussed below that a responsible entity cannot excuse itself from compliance with a requirement of the CIP Reliability Standards.

136. In response to the Southwest TDUs, we note that the CIP Reliability Standards apply in the same way to both public and private users, owners, and operators of the Bulk-Power System. Any specific issues that Southwest TDUs have with the Reliability Standards should be raised in the Reliability Standards development process.

137. Finally, we reject arguments that we are being overly prescriptive in directing the ERO to remove all references to reasonable business judgment from the CIP Reliability Standards. We discuss that general issue elsewhere in this Final Rule and will not repeat that discussion here. It is, however, important to note that such objections are inapposite in this instance for an additional reason that involves the specific nature of the issue raised. The concept of reasonable business judgment speaks to a general legal standard of conduct proposed to apply under a statute that Congress has directed the Commission to administer. It does not involve matters specific to

[59] *See, e.g., Cramer* v. *General Telephone and Electronics Corp.*, 582 F.2d 259 (3d Cir. 1978); *Joy* v. *North*, 692 F.2d 880 (2d Cir. 1982); *In Re Bal Harbour Club, Inc.*, 316 F.3d 1192 (11th Cir. 2003); *Froelich* v. *Senior Campus Living LLC*, 355 F.3d 802 (4th Cir. 2004); *Poth* v. *Rassey*, 281 F. Supp. 2d (E.D. Va. 2003).

[60] *See* CIP NOPR at P 17, 59.

reliability but rather is bound up with the problem of legal enforceability. The Commission has a particular duty to see that the laws it administers can be enforced effectively. We are not being overly prescriptive when acting to ensure that this will be the case.

138. Based on the above discussion, as well as our lengthy analysis in the CIP NOPR, the Commission directs the ERO to modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin.

2. Acceptance of Risk

a. NOPR Proposal

139. The Commission explained in the CIP NOPR that some Requirements in the CIP Reliability Standards permit an entity not to take the actions specified in the Requirement if they ''document compensating measures applied to mitigate risk exposure or an acceptance of risk.'' [61] The CIP NOPR explained that the CIP Reliability Standards do not provide explicit guidance on the circumstances in which it is appropriate to accept the risk of non-compliance. The Commission further explained that the phrase ''acceptance of risk'' essentially allows a Responsible Entity to opt out of certain provisions of a mandatory Reliability Standard at its discretion.[62] The Commission stated its belief that the acceptance of risk language does not serve any justifiable purpose and proposed to direct that the ERO remove this language from the CIP Reliability Standards.

b. Comments

140. Numerous commenters, including NERC, support the removal of acceptance of risk language, provided that this is accomplished using NERC's Reliability Standards development process.[63] Texas Commission believes that removing the term is warranted and states that one entity's acceptance of risk may have an adverse impact on the Bulk-Power System. ISO–NE argues that the term provides no measurable value to any of the Requirements and appears to be an open-ended caveat that is susceptible to abuse.

141. EEI, FirstEnergy, Manitoba Hydro and others contend that the proposal to remove the acceptance of risk language from the CIP Reliability Standards mandates a specific outcome and fails to allow for consideration of alternatives to address the Commission's concerns in the NERC Reliability Standards development process. FPL recommends directing the ERO to consider the issue and either (1) make the appropriate modifications based on the Commission's concerns or (2) provide justification for an acceptance of risk provision. EEI states that the Commission's concerns regarding this language are valid, but should be reasonably tempered by the Commission's expectation that industry will use the mutual distrust posture.

142. Some commenters suggest alternate language to replace the term ''acceptance of risk.'' [64] SDG&E states it does not disagree with the Commission's rationale but proposes, rather than eliminating the concept entirely, to substitute the term ''risk-based.'' Similarly, Xcel acknowledges that acceptance of risk may be a poor choice of words, but that alternate language should be considered. Xcel explains that the phrase ''acceptance of risk'' recognizes that an exception may be appropriate under some circumstances. For example, Requirement R2.3 of CIP–007–1 allows an entity to determine that an unused port does not need to be disabled and accept the risk of not doing so if it determines that the port is insignificant. METC–ITC state that the Commission should consider alternate language that promotes the quantification, documentation and justification of the risk that an entity proposes to accept.

143. A number of other commenters, including Tampa Electric, note that it is not possible to eliminate all risks and state that the goal should be to minimize risks to an acceptable level that still allows business processes to function. Idaho Power states that all businesses carry and accept some level of risk, and it is not appropriate to shift the burden to the company, ratepayer or shareholder to develop systems that may remove all risk. A company can perform an analysis of risk to determine a risk level that delivers an adequate level of security for the company, neighboring utilities and consumers, while remaining manageable to the company from a cost standpoint.

144. APPA/LPPC agree that the CIP Reliability Standards cannot be ignored simply because a company deems a risk acceptable, but believe that the intent of this language was to provide a degree of discretion where compliance is perceived to pose a greater risk to critical asset availability than non-compliance. They envision situations where it is reasonable to conclude that compliance poses a significant risk in the specific instances where acceptance of risk language appears. For example, with respect to Requirement R3.2 of CIP 007–1 (security patch management), inadequately tested patches can pose a risk of system failure, and an entity must weigh the risk of using software with a known flaw against the risk that the vendor's patch will introduce even greater risk.

145. Tampa Electric maintains that the impact of risk to the grid should be weighed before disallowing acceptance of risk. References to acceptance of risk should not be removed because, when a measure is not technically feasible, an effective compensatory control or mitigation, short of replacing the system, is not always possible. In addition, acceptance of risk is not always based on cost reasons. A compensatory step could cause safety issues or some other process problem that makes it highly undesirable.

146. Mr. Brown states that acceptance of risk does not permit an entity simply to decline compliance. The intent was to require explanation, mitigation efforts, evaluation of the potential ramifications of accepting the risk, or other accountability to demonstrate how the CIP Reliability Standards are being complied with in essence. Mr. Brown states that greater transparency is welcome, but removing the language does not mean that such decisions will no longer be made. Rather it will result in such decisions being kept out of sight.

147. FPL Group states that the CIP Reliability Standards provide guidance that allows documentation of measures taken to mitigate risk exposure or an acceptance of risk. This guidance is reasonable and based on control system best practices. It allows responsible entities to evaluate the value of the mitigation with regard to operability and reliability of the Bulk-Power System in comparison to overall feasibility. Responsible entities should not have to bear unreasonable burdens for mitigation that yields only limited benefit. Responsible entities can make the determination to accept the risk-based on reasonable technical judgment insofar as there is no material negative impact to the Bulk-Power System.

148. Entergy opposes eliminating acceptance of risk. It argues that acceptance of risk by senior management is a long-established practice and predates the CIP Reliability Standards. Because of legacy technology, removing this option would require expenditure of significant

[61] *Id.* P 70. *See also* CIP–007–1, Requirements R2.3, R3.2, and R4.1.

[62] *Id.* P 83.

[63] *See also* California Commission, CEA, Texas Commission, ISO–NE and ReliabilityFirst.

[64] *E.g.*, METC–ITC, SDG&E and Xcel.

additional time and money to secure equipment. Associated countermeasures would in many cases be of limited relevance and effectiveness due to the vintage of these legacy controls.

149. With regard to CIP–007–1, MidAmerican supports the proposal to eliminate acceptance of risk from Requirement R2.3 but believes the term should remain in Requirement R3 if accompanied by a mitigation plan and sunset provision. MidAmerican argues that, by requiring a mitigation plan and a time frame for compliance, the CIP Reliability Standard would provide needed flexibility while maintaining the certainty of a committed end-date.

c. Commission Determination

150. The Commission continues to view the term ''acceptance of risk'' as representing an uncontrolled exception from compliance that creates unnecessary uncertainty about the existence of potential vulnerabilities. Responsible entities should not be able to opt out of compliance with mandatory Reliability Standards. The Commission, therefore, directs the ERO to remove acceptance of risk language from the CIP Reliability Standards.

151. In response to concerns raised by NERC, EEI and others, we agree that this action should occur through the Reliability Standards development process. In response to the concerns of many commenters who argue that it should be possible to propose alternative language, we note that this is consistent with the Reliability Standards development process. However, any alternative language that provides a similar opportunity for a responsible entity to opt out of compliance would be subject to remand. Rather, the Commission believes that alternative language that deals with such issues in terms of technical feasibility is preferable. To that end, we have adapted the concept of technical exceptions to encompass a broader range of valid justifications. Elsewhere in this Final Rule we address the criticism that our actions are overly prescriptive and those remarks apply equally here.

152. Expanding the use of the technical feasibility conditions would address the desire for flexibility expressed by some commenters while providing the control that the Commission finds to be necessary. It would provide for documentation, reporting and approval of how responsible entities have elected to comply with the CIP Reliability Standards and thus would permit the ERO and Regional Entities to assess the significance of any possible vulnerability. As to the argument by METC–ITC that a technical feasibility exception may not be possible in all cases, we note that we have found that technical feasibility should not be limited simply to whether something is technically possible but also whether it is technically safe and operationally reasonable. Thus, this approach addresses the issue of inadequately tested patches raised by APPA/LPPC, and similar general concerns raised by Tampa Electric.

153. In response to Entergy, we note that a long-established practice of risk acceptance by senior management does not mean that a continuation of this practice is appropriate under a new system of mandatory cyber security Reliability Standards. We have addressed Entergy's concerns about costs-related legacy equipment in connection with technical feasibility.

154. Many commenters defend retention of the acceptance of risk language by pointing out that it is impossible to eliminate all risk. While likely true, it is beside the point. The acceptance of risk language in the CIP Reliability Standards fails to acknowledge that the real issue is whether the nature and level of inevitable risk is acceptable from a system-wide perspective. Within a system of CIP Reliability Standards intended to protect the Bulk-Power System as a whole, that problem can be addressed by a system that documents and reports the risks in question and ultimately subjects them to approval by the ERO or Regional Entities. The Commission's concern in the CIP NOPR was with the lack of appropriate controls, and eliminating references to acceptance of risk does not imply that all risk can be eliminated.

155. We disagree with Mr. Brown that mutual distrust means that risks accepted by one entity do not affect others on an interconnected control system. A mutual distrust approach is a good security posture. However, its value depends on how well it is implemented. There will likely be a variety of levels of sophistication applied to implementing mutual distrust. It is not a basis for allowing other responsible entities to ignore their obligations under mandatory CIP Reliability Standards.

156. Accordingly, the Commission directs the ERO to develop through its Reliability Standards development process revised CIP Reliability Standards that eliminate references to acceptance of risk.

3. Technical Feasibility

a. NOPR Proposal

157. As the Commission explained in the CIP NOPR, two proposed CIP Reliability Standards provide exceptions from compliance with Requirements based on ''technical feasibility.'' [65] The NERC Glossary does not define the term ''technically feasible,'' nor do the CIP Reliability Standards themselves specify how an entity is to determine whether an action is technically feasible. NERC's FAQ document provides the following guidance on the meaning of the phrase ''where technically feasible: ''

> Technical feasibility refers only to engineering possibility and is expected to be a ''can/cannot'' determination in every circumstance. It is also intended to be determined in light of the equipment and facilities already owned by the responsible entity. The responsible entity is not required to replace any equipment in order to achieve compliance with the Cyber Security Standards. When existing equipment is replaced, however, the responsible entity is expected to use reasonable business judgment to evaluate the need to upgrade the equipment so that the new equipment can perform a particular specified technical function in order to meet the requirements of these standards.[66]

158. Based on these concerns, the Commission proposed in the CIP NOPR to allow, in the near term, exceptions from compliance based on the concept of ''technical feasibility'' in a limited set of circumstances, but also stated that responsible entities should not be permitted to invoke technical feasibility on the basis of ''reasonable business judgment.'' In addition, a responsible entity should not be able to except itself unilaterally from a Requirement of a mandatory CIP Reliability Standard with no oversight.

159. Thus, the Commission proposed in the CIP NOPR to direct that the ERO establish a structure to require accountability from those who rely on ''technical feasibility'' as the basis for an exception. The CIP NOPR described such a structure as requiring a responsible entity to: (1) Develop and implement interim mitigation steps to address the vulnerabilities associated with each exception; (2) develop and implement a remediation plan to eliminate the exception, including interim milestones and a reasonable completion date; and (3) obtain written

[65] CIP NOPR at P 68–69. The ''technically feasible'' phrase is found in CIP–005–1, Requirements R2.4, R2.6, R3.1, R3.2 and CIP–007–1, Requirements R4, R5.3, R6, R6.3. Additionally, CIP–007, Requirement R2.3 uses ''technical limitations'' to similar effect.

[66] FAQ document at 1.

approval of these steps by the senior manager assigned with overall responsibility for leading and managing the entity's implementation of, and adherence to, the CIP Reliability Standards as provided in CIP–003–1, Requirement R2.[67]

160. The Commission stated in the CIP NOPR that this proposed structure should include a review by senior management of the expediency and effectiveness of the manner in which a responsible entity has addressed each of these three proposed conditions. In addition, the Commission proposed to require a responsible entity to report and justify to the ERO and the Regional Entity for approval each exception and its expected duration. In situations where any of the proposed conditions are not satisfied, the Commission proposed that the ERO or the Regional Entity would inform the responsible entity that its claim to an exception based on technical feasibility is insufficient and therefore not approved. Failure to timely rectify the deficiency would invalidate the exception for compliance purposes.

161. The Commission stated its belief that it is important that the ERO, Regional Entities and the Commission understand the circumstances and manner in which responsible entities invoke the technical feasibility provision as well as other provisions that function as exceptions to the CIP Reliability Standards. The Commission, therefore, proposed to direct the ERO to submit an annual report that would include, at a minimum, the frequency of the use of such provisions, the circumstances or justifications that prompt their use, the interim mitigation measures used to address the vulnerabilities, and the milestone schedule to eliminate them and to bring the entities into compliance to eliminate future reliance on the exception.

162. The Commission sought comment on additional categories of information that should be included in the content of this report that would be useful for the Commission, as well as the ERO and Regional Entities, in evaluating the invocation of technical feasibility and similar provisions, and the impact on protection of critical assets.

163. Finally, the Commission proposed to direct the ERO to consider making ''technically feasible,'' and derivative forms of that phrase as used in the CIP Reliability Standards, defined terms in the NERC Glossary, pursuant to the prior clarifications, without any reference to reasonable business judgment.

164. Below, we first address issues related to the general rationale underlying technical feasibility exceptions. We then address issues connected with documentation of exceptions and their remediation and mitigation. Finally, we address the approval of these exceptions.

b. Technical Feasibility Generally

i. Comments

165. Numerous commenters focused on the need for technical feasibility exceptions generally and their underlying rationale. Most support technical feasibility exceptions in some form.

166. Texas Commission expresses concern that technical feasibility could be used to justify inaction. It states that flexibility can be achieved by other means, but if reference to technical feasibility is retained, responsible entities should not be allowed to use it to avoid taking necessary action. Texas Commission comments that it is reasonable to develop a process under which entities with known vulnerabilities self-report to NERC and the Regional Entity and provide a timeline for correcting these deficiencies.

167. NERC states that the Commission properly recognized the appropriateness of an exception based on technical feasibility and suggests that it be designated an ''exemption for reliability.'' [68] NERC supports clarification of the Reliability Standards to ensure that an exemption is documented and justified in terms of its impact on Bulk-Power System reliability. ReliabilityFirst makes similar proposals.

168. NERC and others believe that the appropriate way to address the Commission's specific proposed directives is through the Commission-approved Reliability Standards development process.[69] Northern California supports the Commission's recommendation that the ERO re-examine and clarify the meaning of technical feasibility and provide guidance on the appropriate procedures for claiming an exemption based on it. Ontario IESO comments that, if the term reasonable business judgment is removed from the CIP Reliability Standards, industry and the ERO may find other areas where the concept of technical feasibility is applicable when revising the CIP Reliability Standards.

NRECA states that technical feasibility is a matter on which the Commission should defer to the ERO's technical expertise and not adhere to a one-size-fits-all approach.

169. NERC explains that the CIP Reliability Standards include references to technical feasibility to recognize that, in many cases, equipment in place in substation and generating plant environments was implemented with operational functions paramount to all other considerations, including security. This equipment is not at the end of its useful life and historically has not been designed with ready access to software updates and patches. Such software upgrades that could increase functionality without directly contributing to reliability generally have not been made. NERC states that modern replacement equipment is more readily compatible with an environment where updates and patches are more commonplace and security functionality is an understood necessity. Securable equipment will be used when equipment is replaced due to natural end-of-life or failure, but this modern equipment represents a very small percentage of the installed base of all cyber equipment in substations and generating plants.

170. Many commenters, including APPA/LPPC, Duke, Entergy, NRECA and ReliabilityFirst, concur with this explanation of rationale for the references to technical feasibility. Duke agrees that technical feasibility exceptions should be controlled, but it argues that replacing legacy equipment on an accelerated schedule could create industry-wide logistical problems and unwarranted ratepayer impacts. NRECA maintains that rapid replacement of equipment would mean costs for customers, could overwhelm the supply chain, and could lead to premature obsolescence of replacement equipment as security technology continues to improve. Consumers Energy states that technical feasibility exceptions are proposed as a last resort that is forced by the limitations of available technology, support and service limitations of existing technology, and as-built limitations.

171. Entergy maintains that the older equipment in question generally cannot be compromised through typical hacker techniques, and physical access to it is often required. This presents greater challenges for attackers and means that only local impact will result from a successful attack. Entergy recommends allowing industry three to five years to upgrade critical assets with modern cyber controls that will provide the needed operational efficiency

[67] CIP NOPR at P 79.

[68] NERC comments at 20–22.

[69] *E.g.,* Alliant, Manitoba Hydro, Northern California and NRECA.

improvements and that would be properly secured as a matter of course.

172. ReliabilityFirst notes that a very small percentage of the installed base of all cyber equipment in substations and power plants incorporates security functionality. Consumers Energy explains that older control systems can still be very reliable, but many assets identified as critical cyber assets do not have malware and virus protection, in some cases due to technology conflicts with virus and malware protection systems. In addition, managing updates on devices that are continuously online is a difficult task. Consumers Energy states that there are adequate alternate measures in such cases such as firewalls with content security functions that restrict any options for infecting systems with viruses and that implement intrusion detection for the perimeter with advanced content security services.

173. NERC states that the drafting team believed that cyber security standards should not unnecessarily impede the primary mission of maintaining reliable Bulk-Power System operations. NERC and ReliabilityFirst argue that changes must be carefully planned and tested to ensure that no unintended consequences occur. Technologies are constantly evolving, and it is impractical to think that equipment always can maintain a leading-edge cyber security posture without introducing operating issues.

174. Manitoba Hydro states that industry attempted to strike a balance for security at the various types of facilities while recognizing the large base of legacy systems at remote locations. The security framework focused on routable protocols and dial up access. The Commission's proposals to limit technical feasibility exceptions and implement a defense in depth measure in front of legacy systems would have a nominal impact on control centers but a significant impact on other facilities, systems and equipment, forcing unjustified early equipment replacement or installation of technology to provide mitigating controls. Manitoba Hydro argues that modifying the Reliability Standards on this point could add considerable work for responsible entities and require modifications to the implementation period.

175. Northern Indiana, Ontario Power and SoCal Edison support retaining the term technical feasibility. Ontario Power maintains that removing references to technical feasibility could be interpreted by some to mean that mandatory compliance is required, regardless of the cost, the impact on production systems, or the risk to the Bulk-Power System. Northern Indiana concurs with the Commission's proposal to treat instances of technical infeasibility as exceptions that require reporting and certain alternative courses of action. However, it disagrees with what it describes as the Commission's restrictive interpretation of the term and urges the Commission to acknowledge that technical infeasibility may apply to future assets as well. Northern Indiana advocates that the Commission instead direct NERC to interpret technical feasibility narrowly with regard to the technical characteristics of both existing and future assets. Northern Indiana states that the Commission should not assume technical infeasibility will exist only during the transition period and not afterwards, nor should it assume only one single means will exist, on a going forward basis, to comply with the Reliability Standards.

176. Mr. Brown states that technical feasibility has less to do with whether to comply than with how to comply. Whether or not something is technically feasible is purely an engineering issue. On the other hand, whether or when to replace equipment that cannot do something due to technical feasibility with equipment that can do so is purely a managerial decision. Mr. Brown states that in light of his interpretation of reasonable business judgment, the Commission should have much less concern about the interplay between technical feasibility and reasonable business judgment.

177. Teltone states that it is now easy to incorporate CIP-related features such as two-factor authentication (with unique user names and passwords) to both dial-up and Internet protocol devices without replacing them, upgrading their software, or taking them offline. Access and usage logging of legacy devices at substations is easily accomplished, something Teltone maintains should quell the problem of technical feasibility.

ii. Commission Determination

178. The Commission adopts the CIP NOPR proposal and directs the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards. We will modify some of our proposed criteria for that framework of accountability further below. We are persuaded by commenters that the proposed conditions for invoking the technical feasibility exception should allow for operational considerations. In response to Northern Indiana and other commenters, we note that the Commission did not propose to eliminate references to technical feasibility from the CIP Reliability Standards, only that the term be interpreted narrowly and without reference to considerations of business judgment.

179. In response to those commenters who argue that the Commission's concerns and directives should be addressed through the Reliability Standards development process, we agree that to the degree revisions to the Reliability Standards are necessary to address our concerns, they would be made through that process. We disagree, however, with the arguments that claim we are rewriting the CIP Reliability Standards or adhering to a one-size-fits-all approach. With respect to the latter point, we note that technical feasibility issues are by their nature something that must be dealt with on a case-by-case basis, as they only arise in specific circumstances. Our concern here is primarily with the framework within which decisions on technical feasibility are made and ensuring that this framework promotes sound decisions that lead to effective results. The oversight provisions we describe below are essential elements of such a framework.

180. We agree with NERC and other commenters on the underlying rationale for a technical feasibility exception, i.e., that there is long-life equipment in place that is not readily compatible with a modern environment where cyber security issues are an acknowledged concern. While equipment replacement will often be appropriate to comply with the CIP Reliability Standards, such as in instances where equipment is near the end of its useful life or when alternative or supplemental security measures are not possible, we acknowledge that the possibility of being required to replace equipment before the end of its useful life is a valid concern.

181. The Commission, however, disagrees with Northern Indiana that technical feasibility should be interpreted to apply to future assets also. The justification presented for technical feasibility exceptions is rooted in the problem of long-life legacy equipment and the economic considerations involved in the replacement of such equipment before the end of its useful life. We recognize that these considerations can be valid in some cases, but Northern Indiana has not explained why technical feasibility exceptions should apply to replacement equipment. The Commission neither assumes that technical infeasibility issues will be present only during the transition period, nor does it assume

that on a going forward basis there will be only one single means to comply with the CIP Reliability Standards. It does assume, however, that all responsible entities eventually will be able to achieve full compliance with the CIP Reliability Standards when the legacy equipment that creates the need for the exception is supplemented, upgraded or replaced.

182. The Commission agrees with various commenters that the implementation of the CIP Reliability Standards should not be permitted to have an adverse effect on reliability and that proper implementation requires that care be taken to avoid unintended consequences. We thus believe it is important to clarify that the meaning of ''technical feasibility'' should not be limited simply to whether something is technically possible but also whether it is technically safe and operationally reasonable.

183. We disagree with Mr. Brown's view that whether or when to replace equipment that cannot do something due to technical feasibility with equipment that can do so is purely a managerial decision, especially since he intertwines this proposition with the concept of reasonable business judgment. While we accept NERC's rationale for technical feasibility exceptions, as discussed below, an integral issue in individual cases where legacy equipment presents a technical feasibility issue is whether an alternative course of action protects the reliability of the Bulk-Power System to an equal or greater degree than compliance would. This is not a purely managerial decision involving reasonable business judgment, regardless of what meaning one imparts to that term.

184. While a number of commenters agree that it is important to clarify the meaning of technical feasibility, none appear to support defining the term in the NERC Glossary. Therefore, in light of the comments received generally and the specific guidance that we are providing to the ERO in connection with technical feasibility, we conclude that a definition of this type is unnecessary. A definition cannot substitute for a framework of conditions or criteria to provide accountability, and if those conditions or criteria are implemented, a definition is not needed. We do not agree with NERC that replacing the term technical feasibility with ''exemption for reliability'' would be helpful. We note, in particular, that an ''exemption'' normally is understood to be a release from an obligation whereas what is under discussion here is an exception that forms an alternative obligation.

185. While the Commission will not address the merits of any particular technology, we note that Teltone's comments raise an important general consideration when developing policy on technical feasibility. While technical limitations present real issues, and while one should not be overly optimistic that technological developments will resolve them sooner than expected, one should not be overly pessimistic either. Indeed, high standards should, if anything, encourage the development of technical solutions.

186. Based on the above considerations, the Commission adopts its proposal in the CIP NOPR that technical feasibility exceptions may be permitted if appropriate conditions are in place. The term technical feasibility should be interpreted narrowly to not include considerations of business judgment, but we agree with commenters that it should include operational and safety considerations.

c. Technical Feasibility Exception Mitigation and Remediation

187. As mentioned above, in the CIP NOPR, the Commission proposed a three step structure to require accountability when a responsible entity relies on technical feasibility as the basis for an exception. This proposed structure would require a responsible entity to: (1) Develop and implement interim mitigation steps to address the vulnerabilities associated with each exception; (2) develop and implement a remediation plan to eliminate the exception, including interim milestones and a reasonable completion date; and (3) obtain written approval of these steps by the senior manager assigned with overall responsibility for leading and managing the entity's implementation of, and adherence to, the CIP Reliability Standards, along with regional approval through the ERO.

i. Comments

188. NERC supports clarification of the CIP Reliability Standards to ensure that the use of a technical feasibility exemption must be documented and justified in terms of its impact on Bulk-Power System reliability. Duke also agrees with the proposal to require documentation, including appropriate mitigation and a senior management-approved remediation plan.

189. National Grid states that the Commission's mitigation proposal is reasonable and appropriate, but it maintains that the Commission should clarify that acceptable mitigation for older assets entails measures short of replacement, upgrades, or retrofits. A mitigation requirement otherwise would undermine any relief associated with an exception. Mitigation measures for vulnerabilities associated with older assets will need to be in place as long as those assets remain in service. National Grid states that the Commission's references to ''interim'' mitigation and remediation implementation milestones could suggest that older assets must be replaced before the end of their useful lives or that the mitigation measures would not be as effective as the solutions codified in the Reliability Standards. National Grid argues that mitigation measures should be as or more effective than compliance, and in the case of minor technical or administrative requirements, replacement of certain assets before the end of their useful lives would be wasteful and inefficient.

190. SPP believes it is reasonable to treat technical feasibility as a documented exception. Such exceptions should be reviewed and approved annually, but identifying a reasonable completion date for remediation may not always be possible. SPP states that to require remediation of a technical feasibility exception by a date certain is contrary to the Commission's acknowledgement that cost can be a prohibiting factor. Technical limitations may prohibit compliance with a requirement. The appropriate response in such cases is to mitigate the risk by implementing compensating measures. SPP questions the need for remediation where compensating measures are equally effective in reducing risk. It recommends that responsible entities be required initially to mitigate the risk and then evaluate and document whether further remediation is required and technically feasible as part of the exception approval process.

191. Northern Indiana believes a remediation plan should seek to eliminate the exception to the extent possible, but complete elimination may not be possible in all cases. Northern Indiana states that the Commission should consider the development and implementation of a remediation plan to eliminate the exception to the extent possible. Tampa Electric submits that it is unreasonable to require a remediation plan in every case. Sometimes there is no technology that would permit compliance with the letter of the CIP Reliability Standard.

ii. Commission Determination

192. With some minor refinements discussed below, the Commission adopts the CIP NOPR proposal for a

three step structure to require accountability when a responsible entity relies on technical feasibility as the basis for an exception. We address mitigation and remediation in this section and direct the ERO to develop: (1) A requirement that the responsible entity must develop, document and implement a mitigation plan that achieves a comparable level of security to the Requirement; and (2) a requirement that use of the technical feasibility exception by a responsible entity must be accompanied by a remediation plan and timeline for eliminating the use of the technical feasibility exception. While the CIP NOPR proposed that each remediation plan contain a reasonable completion date, the Commission is persuaded by the comments of National Grid and SPP that a date certain for remediation may not be possible in some instances. While we expect remediation by a date certain to be the norm, we will not require a date certain for remediation in every instance that a responsible entity invokes the technical feasibility exception. An entity must provide an explanation when it believes that it is not possible for a remediation plan to provide a reasonable completion date.

193. We also agree with Northern Indiana that in some instances remediation can be required only to the extent possible. For example, in some cases it may never be possible to enclose certain critical cyber assets within a six-sided physical boundary as required under CIP–006–1. However, such cases need to be sufficiently justified, the mitigation strategies must be ongoing and effective, and the justification must be subject to periodic review. We also are mindful that accelerated replacement of equipment can be economically wasteful where security is not otherwise compromised. We thus agree with National Grid that where mitigation measures are as or more effective than compliance, and in the case of minor technical or administrative requirements, replacement of certain assets before the end of their useful lives can be wasteful and inefficient. We also agree with SPP that remediation might not be necessary where compensating measures are equally effective in reducing risk. However, such cases must be subject to clear criteria and periodic review and, where necessary, updates.

194. However, in adopting this approach, we do not intend to suggest that it would never be necessary to replace equipment before the end of its useful life to achieve cyber security goals. Where equipment is near the end of its useful life or if insufficient mitigation measures are available, the equipment should be replaced. However, such situations must be dealt with on a case-by-case basis. We emphasize that responsible entities must protect assets that are critical to the reliable operation of the Bulk-Power System.

d. Approval and Control of Specific Exceptions

195. This section discusses the Commission's directions with regard to approval of a technical feasibility exception, the third component of our framework for allowing technical feasibility exceptions. As described above, the CIP NOPR proposed that NERC develop a requirement that a responsible entity relying on the technical feasibility exception must obtain written approval of a remediation plan by a senior manager.[70] The Commission also proposed that the responsible entity report and justify to the ERO and the Regional Entity for approval of each exception. In addition, the Commission proposed to direct that the ERO submit an annual report regarding industry use of the technical feasibility exception.

i. Comments

196. California Commission states that approval of technical feasibility exceptions by the ERO and the relevant Regional Entity is critical because it prevents attempts to manipulate the system and induces responsible action.

197. National Grid supports providing Regional Entities with notice of technical feasibility exceptions and audits of exceptions by Regional Entities. It states that a central clearinghouse that catalogs all technical feasibility exceptions would be helpful because of the interdependencies among the Bulk-Power System assets. This clearinghouse could verify whether reliance on exceptions (or the associated mitigation measures) adequately maintains reliability and does not create reliability issues for neighboring systems. ISO–NE states that reporting exceptions to Regional Entities would be useful in identifying CIP Reliability Standards and Requirements with frequent implementation issues that call for modifications.

198. In contrast, ISO/RTO Council, EEI and others do not believe that reporting and approval of technical feasibility exceptions is appropriate.[71] EEI states it does not believe that NERC or the Regional Entities have the technical expertise to make these types of determinations. ISO–NE states it is unlikely that either Regional Entities or the ERO will have the necessary skills to evaluate the broad spectrum of situations that the industry presents. MidAmerican states that requiring ERO and Regional Entity approval would burden those entities, create delays, and divert resources away from more urgent cyber security concerns. Tampa Electric states that the Commission should ensure that delays do not interfere with timely compliance by responsible entities. Idaho Power believes that the Commission's proposals on technical feasibility would place administrative burdens on both company and the Regional Entities that outweigh the benefits. Idaho Power sees little value in policing the use of the technical feasibility exception with such a burdensome administrative process that may, in the end, delay the resolution of legitimate technical feasibility issues.

199. ReliabilityFirst argues that a responsible entity's senior manager must already approve any exceptions, making reporting and approval unnecessary, and it will be very difficult for the ERO or Regional Entity staff to review a responsible entity's exceptions effectively and assess them realistically. SERC-CIPC recommends that the requirement to authorize and document exceptions remain with the entity's designated senior manager.

200. ISO/RTO Council argues that granting the Regional Entities authority to adjudicate exceptions along with the ability to apply sanctions for non-compliance creates a conflict of interest. Auditors should be independent, and an assessor should not be involved with review and approval of policy exceptions. ISO/RTO Council argues that instead of requiring that exceptions be reported and justified, the Commission should consider directing the ERO to detail the type of justifications and considerations that must be documented when invoking a technical feasibility exemption. Responsible entities would then be required to incorporate them into their analysis of possible exemptions.

201. EEI, OGE and SoCal Edison question how the ERO and Regional Entities would determine what is technically feasible for a particular model of equipment in a specific context. If there is to be external review and approval, there should be an appeals process, and that would delay implementation of future revisions to the CIP Reliability Standards. Alliant, EEI and Tampa Electric believe that NERC should require that decisions on technically feasible be subject to audits

[70] CIP NOPR at P 79.

[71] *E.g.,* FirstEnergy, ISO–NE, KCPL, SERC–CIPC and SoCal Edison.

that are ultimately reported to the Commission. Duke, KCPL and SoCal Edison maintain that evaluation of technical feasibility issues should be left to compliance audits.

202. Northern Indiana seeks clarification of the information that will be needed to justify an exception. It suggests that, similar to the Commission's proposed approach regarding self-certification, a responsible entity should have the opportunity to consult with the ERO and Regional Entities. Northern Indiana also advocates the waiver of monetary penalties during this time as well as within the timeframe of any remediation plan.

203. APPA/LPPC state that the Commission should clarify that when a Regional Entity or the ERO rejects a technical feasibility exception request, the responsible entity may rely on the exception until it has been ruled upon. In addition, the organization should be allowed a reasonable time to come into compliance.

204. Entergy states that there is no indication that the benefits of reporting exceptions would outweigh the detriments, but if further reporting is required, it recommends a single annual report from each registered entity that includes a summary description of the exceptions and actions taken or to be taken. The ERO could use this report to satisfy its annual reporting requirement.

205. A number of other commenters emphasize the sensitivity of information about technical feasibility exceptions. SPP states that an annual report must contain information that qualifies as Critical Energy Infrastructure Information (CEII) to be of any value. SERC–CIPC also recommends CEII treatment for this information. SPP is concerned that if the report is not treated as CEII, sensitive data could be inadvertently made public. To protect against disclosure, SPP proposes that the ERO could make exception documentation available for Commission staff inspection in the ERO offices as a possible alternative to a report. National Grid states that information about exceptions should be subject to adequate information protection controls to avoid disclosure and misuse.

206. Duke opposes an annual report by the ERO to the Commission because, even if it does not contain CEII, it will compromise security by publicly identifying problem areas for the industry and the mitigation measures being employed. If a report must be submitted, there must be stringent and enforceable confidentiality measures to prevent inadvertent or unauthorized disclosure. OGE believes reporting and approval for all exceptions is contrary to the purpose of the CIP Reliability Standards because information on exceptions sent to the ERO or Regional Entity could indicate weaknesses in security that could be compromised and exposed. These same concerns lead Xcel to urge that Regional Entities develop confidentiality protocols for such communications.

207. ISO–NE states that detailed technical descriptions of exceptions should not be passed to the Regional Entities or the ERO because the information would be potential vulnerability information that the responsible entity should protect as critical cyber asset information under CIP–003–1, Requirement R4. Tampa Electric states that, if the Commission decides to require ERO or Regional Entity review, it should also prescribe controls to ensure the confidentiality and security of the information under review.

208. Although not commenting specifically on reporting of technical feasibility issues, Bonneville notes that under the Freedom of Information Act (FOIA), release of information to an external party generally waives any privileges against disclosure with respect to subsequent requests to the federal agency for that same information. Bonneville is concerned that submission of critical asset information to the Regional Entity, particularly the vulnerability-related rationales for including and excluding various facilities on the critical asset list, may act as such a waiver.

ii. Commission Determination

209. For the reasons discussed below, the Commission concludes that technical feasibility exceptions should be reported and justified and subject to approval by the ERO or the relevant Regional Entity. The Commission thus adopts its CIP NOPR proposal that use and implementation of technical feasibility exceptions must be governed by a clear set of criteria. However, because we are persuaded by the commenters, we have modified certain elements of our original proposal, as discussed below.

210. Most objections to the CIP NOPR proposal regarding the review and approval of technical feasibility exceptions are not objections in principle but rather focus on practical issues of implementation, such as limited ERO and Regional Entity resources and sensitivity of the information in question. To the extent that objections in principle have been raised, we disagree. Thus, we disagree with ReliabilityFirst's argument that senior manager approval of exceptions is unnecessary because of the responsibilities already assigned to the senior manager by CIP–003–1. These technical feasibility exceptions implicate matters that go beyond the purview of individual responsible entities and must be subject to review and approval by those with a wider-area view and general responsibility for system reliability. We also disagree with the ISO/RTO Council that the Commission should simply direct the ERO to detail the type of justifications and considerations that must be documented when invoking a technical feasibility exemption. While such guidance could be useful, it cannot substitute for reporting, review, and approval, which is necessary to address concerns that extend beyond the reach of an individual responsible entity.

211. With regard to the senior management approval, we continue to believe that internal approval is an important component of an overall framework of accountability with regard to use of the technical feasibility exception. Therefore, we adopt this aspect of our CIP NIPR proposal and direct the ERO to include approval of the mitigation and remediation steps by the senior manager (identified pursuant to CIP–003–1) in the course of developing this framework of accountability.

212. However, the practical considerations pointed out by a number of the comments have convinced us to adopt an approach to the issue of external oversight different from the one originally proposed. We agree, in particular, with those commenters who argue that pre-approval could tax ERO and Regional Entity resources, delay implementation, and possibly create undue risks that sensitive information will be disclosed.

213. The Commission agrees with National Grid that Regional Entities should, in the first instance, receive and catalogue notices of technical feasibility exceptions that are claimed. Such notices must include estimates of the degree to which mitigation measures achieve the goals set by a CIP Reliability Standard and be in sufficient detail to allow verification of whether reliance on exceptions (or the associated mitigation measures) adequately maintains reliability and does not create reliability issues for neighboring systems. Initial submission of notices should be provided by responsible entities at least by the ''Compliant'' stage of implementation in order to allow Regional Entities to plan for

auditing exceptions, as described in more detail below.

214. The Commission also agrees with National Grid, EEI and others that actual evaluation and approval of technical feasibility exceptions should be performed in the first instance in the audit process. This would allow assessment of exceptions within their specific context and thus facilitate greater understanding in evaluating individual exceptions, as well as related mitigation steps and remediation plans. This also would increase the amount of sensitive information that remains on-site and reduces the risk of improper disclosure. In addition, it will allow the ERO and Regional Entities, informed by the initial notices discussed above, to include personnel in audit teams with sufficient expertise to judge the need for a technical feasibility exception and the sufficiency of preferred mitigation measures.[72]

215. Given the significance of technical feasibility exceptions, the Commission believes that initial audits of technical feasibility exceptions should be expedited, i.e., performed earlier than otherwise, including moving the audit to an earlier year. Also, in general, responsible entities claiming such exceptions should receive higher priority when determining which entities to audit, and the more exceptions an entity has, the higher the priority for audit should be. Further, NERC may provide an appeals process for the review of technical feasibility exceptions, if it determines that this is appropriate.

216. However, the Commission notes that the audit process is a Regional Entity and ERO process, and audit team findings regarding exceptions are subject to Regional Entity and ERO review. The Commission believes that the audit report should form the basis for ERO or Regional Entity approval of individual exceptions. Approval thus represents a determination on compliance with the applicable CIP Reliability Standards, and we disagree with the ISO/RTO Council that approval of technical feasibility exceptions raises any conflict of interest or due process concerns. The proposed procedures raise no special issues in this respect.

217. We agree with EEI and others that approvals and potential appeals should not be allowed to delay implementation, but we believe our revised proposal resolves this problem. We also agree with APPA/LPPC that responsible entities should be able to rely on a technical feasibility exception prior to formal approval. However, we disagree with Northern Indiana that penalties should be waived within the time when an approved remediation plan is being implemented, as proper implementation of the plan itself constitutes a necessary element of compliance.

218. In summary, on the issues pertaining to external approval of a responsible entity's use of the technical feasibility exception, rather than a pre-approval process, we direct the ERO to design and conduct an approval process through the Regional Entities and the compliance audit process. This process should require the ERO or a Regional Entity to approve any technical feasibility exception, taking into account whether the technical feasibility exception is needed and whether the mitigation and remediation steps are adequate to the circumstance.

219. We agree with comments emphasizing the importance of protecting sensitive information relating to technical feasibility exceptions. We agree with SPP and others that CEII treatment should be available for any such information. In response to Bonneville, we agree that a governmental entity subject to FOIA requirements should not be required to submit sensitive information about critical assets or critical cyber assets that could be deemed a waiver of FOIA protection that is otherwise available. Nonetheless, a governmental entity's decision to rely on a technical feasibility exception should also be subject to appropriate oversight and accountability. Thus, we direct NERC, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities that are subject to Reliability Standards as users, owners or operators of the Bulk-Power System can safeguard sensitive information.

220. As stated in the CIP NOPR, the Commission believes that it is important that the ERO, Regional Entities and the Commission understand the circumstances and manner in which responsible entities invoke the technical feasibility exception.[73] Accordingly, we direct the ERO to submit an annual report to the Commission that provides a wide-area analysis regarding use of the technical feasibility exception and the effect on Bulk-Power System reliability. The annual report must address, at a minimum, the frequency of the use of such provisions, the circumstances or justifications that prompt their use, the interim mitigation measures used to address vulnerabilities, and efforts to eliminate future reliance on the exception.[74]

221. While we agree with commenters that the compilation of data for the annual report must not compromise the security of the Bulk-Power System, we disagree that this is a reason not to require the report. Rather, as we indicated in the CIP NOPR, the report should not provide a level of detail that divulges CEII data. Rather, the report should contain aggregated data with sufficient detail for the Commission to understand the frequency with which specific provisions are being invoked as well as high level data regarding mitigation and remediation plans over time and by region. Further, we direct the ERO to control and protect the data analysis to the extent necessary to ensure that sensitive information is not jeopardized by the act of submitting the report to the Commission.

e. Conclusion

222. In conclusion, pursuant to section 215(d)(5) of the FPA, we direct the ERO to develop a set of criteria to provide accountability when a responsible entity relies on the technical feasibility exceptions in specific Requirements of the CIP Reliability Standards. As discussed above, structural elements of this framework include mitigation steps, a remediation plan, a timeline for eliminating use of the technical feasibility exception unless appropriate justification otherwise is provided, regular review of whether it continues to be necessary to invoke the exception, internal approval by the senior manager, wide-area approval through the ERO's audit process, and cooperation with the ERO to provide the Commission with high-level, wide-area analysis regarding the effects the technical feasibility exception on the reliability of the Bulk-Power System. We direct the ERO to develop appropriate modifications, as discussed above.

G. Use of National Institute of Standards and Technology (NIST) Standards in Developing Future Revisions to the CIP Reliability Standards

1. NOPR Proposal

223. In the CIP NOPR, the Commission stated that it expects NERC

[72] General reliance on the audit process does not preclude the Commission, the ERO or a Regional Entity from exercising its authority to review a claimed exception, whether resulting from a complaint, an incident or on its own initiative outside of the audit process.

[73] CIP NOPR at P 80.

[74] Responsible entities must cooperate with the ERO and the Regional Entities in providing information deemed necessary for the ERO to fulfill its reporting obligation to the Commission.

to monitor the development and implementation of the NIST standards to determine if they contain provisions that will better protect the Bulk-Power System.[75] The CIP NOPR also stated that it expects the ERO to consult with federal entities that are subject to both the CIP Reliability Standards and NIST standards on the effectiveness of the latter. While the Commission declined to propose that NERC incorporate specific provisions of NIST into the CIP Reliability Standards, it indicated that it may revisit the issue in the future.

2. Comments

224. Congressional Representatives filed comments expressing their support for the Commission's efforts to require NERC to develop modifications to the CIP Reliability Standards. However, they believe that Bulk-Power System reliability will be better protected by cyber security standards that incorporate the security measures set forth in NIST Special Publication (SP) 800–53 as applied to industrial control systems. Congressional Representatives state that NIST research prepared a technical report comparing the proposed CIP Reliability Standards with SP 800–53. This technical report found that an organization conforming to the baseline set of security controls in SP 800–53 will also comply with the management, operational and technical security requirements of the CIP Reliability Standards, though the converse may not be true. The technical report concluded that the CIP Reliability Standards are both ''inadequate for protecting critical national infrastructure,'' and ''inadequate for all electric energy systems when the impact of regional and national power outages is considered.'' [76]

225. Further, Congressional Representatives point out that federal government-owned elements of the Bulk-Power System must comply with both CIP Reliability Standards and NIST SP 800–53, while privately owned elements must comply only with the former. They express concern that ''inconsistent regulatory structures create weak links and potential vulnerabilities in the entire system.'' [77] Congressional Representatives, therefore, urge the Commission to modify the CIP Reliability Standards to incorporate aspects of SP 800–53 and the related NIST standards.

226. NIST itself compliments the Commission for proposing a derivative of the CIP Reliability Standards that is an improvement over the original NERC CIP Reliability Standards. However, according to NIST, the CIP NOPR proposal still falls short of meeting the federal mandatory minimum security measures set forth in NIST Special Publication (SP) 800–53 as applied to industrial control systems. In NIST's view, the CIP Reliability Standards, if modified pursuant to the proposals in the CIP NOPR, will leave information systems that support private sector bulk electric power systems less protected than comparable federal information systems. NIST suggests that the Commission consider strengthening the minimum controls currently required by the CIP Reliability Standards.

227. NIST recommends that the Commission adopt the CIP Reliability Standards with the enhancements proposed by the Commission as an interim measure. Additionally, NIST advocates that the Commission prescribe plans for a two to three year transition to cyber security Reliability Standards that are identical to, consistent with, or based on SP 800–53 and related NIST standards and guidelines. NIST argues that this approach would strengthen the CIP Reliability Standards.

228. Although Entergy states that it generally disagrees with the Commission's approach of dictating specific revisions that the ERO must adopt, if the Commission determines that the CIP Reliability Standards require further development, Entergy argues that the Commission should modify its approach to the NIST Framework and require the ERO to consider it as a resource in developing revisions to the CIP Reliability Standards. Entergy argues that the industry needs immediate, clear direction and there already exists guidance that the Commission can rely on to provide such direction. Entergy notes that the NIST ''Security Risk Management Framework'' has been developed over many years by the U.S. Department of Commerce. The NIST Framework is devoid of conflicts of interest and has been broadly vetted, both domestically and internationally.

229. SDG&E states that, while it welcomes the use of industry standards in NERC CIP compliance, it cautions that NIST standards provide many controls that are considered best practices. It also explains that NIST was developed for government and some NIST standards that work well for government may be cost-prohibitive in the private sector.

230. Bonneville understands the Commission's directive that NERC consider NIST standards in the further development of the CIP Reliability Standards to apply to CIP–003–1. Bonneville suggests that existing guidelines, such as the NIST Special Publications, should be incorporated to the extent practicable. Bonneville argues that creating another set of directives describing how the standards are to be met without incorporating, or at least considering, existing guidelines could create considerable confusion and conflict.

231. Applied Control Solutions urges the immediate adoption of the NIST ''Security Risk Management'' framework in place of the CIP Reliability Standards. It explains that the NIST framework provides a hierarchical three-tiered set of countermeasure and controls requirement-sets for application as appropriate and related guidance documents. According to Applied Control Solutions, the NIST framework has been broadly vetted, is not onerous, provides guidance on how to address older in-service cyber assets, and allows flexibility for organizations to tune their cyber security programs for their specific operating scenarios. It also contends that NIST addresses the major concerns raised by the Commission regarding the CIP Reliability Standards, for example, by providing additional granularity and requiring compensating measures where technical feasibility becomes an issue. Applied Control Solutions also comments that the ISA–99 standards process has expertise, and NERC should be directed to work with ISA in revising the CIP Reliability Standards.

3. Commission Determination

232. As proposed in the CIP NOPR, the Commission will not at this time direct NERC to incorporate specific provisions of the NIST standards into the CIP Reliability Standards. While commenters provide compelling information that suggests that the NIST standards may provide superior measures for cyber security protection, the Commission is concerned that the immediate adoption of the NIST standards would result in unacceptable delays in having any mandatory and enforceable Reliability Standards that relate to cyber security.

233. The Commission continues to believe—and is further persuaded by the comments—that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we

[75] CIP NOPR at P 88.

[76] Congressional Representatives comments at 9, citing Marshall D. Abrams, ''Addressing Industrial Control Systems in NIST Special Publication 800–53,'' MITRE Technical Report (March 2007).

[77] *Id.* at 9.

direct 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 report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERC's Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need for new CIP Reliability Standards, or as part of an assessment of NERC's performance of its responsibilities as the ERO.[78]

H. Discussion of Each CIP Reliability Standard

1. CIP–002–1—Critical Cyber Asset Identification

234. Reliability Standard CIP–002–1 deals with the identification of critical cyber assets. The NERC Glossary defines ''cyber assets'' as ''programmable electronic devices and communication networks including hardware, software, and data.'' It defines ''critical cyber assets'' as ''cyber assets essential to the reliable operation of critical assets.'' NERC defines ''critical assets'' as ''facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.'' [79] The accurate identification of critical assets and critical cyber assets pursuant to CIP–002–1 is the cornerstone of the CIP Reliability Standards because it acts as a filter, determining whether a responsible entity must comply with the remaining CIP requirements in CIP–003–1 through CIP–009–1.

235. As the first step in identifying critical cyber assets, CIP–002–1 requires each responsible entity to develop a risk-based assessment methodology to use in identifying its critical assets. Requirement R1 specifies certain types of assets that an assessment must consider for critical asset status and also allows the consideration of additional assets that the responsible entity deems appropriate. Requirement R2 requires the responsible entity to develop a list of critical assets based on an annual application of the risk-based assessment methodology. Requirement R3 provides that the responsible entity must use the list of critical assets to develop a list of associated critical cyber assets that are essential to the operation of the critical assets. CIP–002–1 requires an annual re-evaluation and approval by senior management of the lists of critical assets and critical cyber assets.

236. Pursuant to section 215 of the FPA, the Commission approves Standard CIP–002–1 as mandatory and enforceable. In addition, pursuant to section 215(d)(5) of the FPA, the Commission directs the ERO to develop modifications to Standard CIP–002–1. The required modifications are discussed below in the following topics regarding CIP–002–1: (1) Need for ERO guidance regarding the risk-based assessment methodology; (2) scope of critical assets and critical cyber assets; (3) internal, management, approval of the risk-based assessment; (4) external review of critical assets identification; and (5) interdependency analysis.

a. Guidance on Risk-Based Assessment Methodology

237. Requirement R1 of CIP–002–1 requires each responsible entity to develop a risk-based assessment methodology to identify critical assets. A responsible entity must maintain documentation describing its methodology that includes procedures and evaluation criteria. Requirement R1 identifies specific assets that the methodology must ''consider,'' including control centers, facilities critical to system restoration and automatic load shedding, and substations and generation resources that support reliable operation of the Bulk-Power System—as well as any other assets that support reliable operations and the responsible entity deems appropriate to include in its assessment.

i. NOPR Proposal

238. In the CIP NOPR, the Commission expressed concern that responsible entities have enough guidance to devise an assessment methodology that is adequate to identify the types of assets necessary to protect Bulk-Power System reliability.[80] The Commission stated that responsible entities would benefit from NERC providing some common understanding regarding the scope, purpose and basic direction of the assessment methodology. As an example, the Commission indicated that a proper methodology should examine (1) the consequences of the loss of the asset to the Bulk-Power System and (2) the consequences to the Bulk-Power System if an adversary gains control of the asset for intentional misuse. Accordingly, the Commission proposed to direct the ERO to develop modifications to provide additional guidance as to the features and functionality of an adequate risk-based assessment methodology.

239. The CIP NOPR also noted that smaller entities may have difficulty in determining whether a particular asset is ''critical'' since the impact of the asset may be dependent on their connection with a transmission owner or operator. Thus, the Commission proposed that the ERO and Regional Entities provide reasonable technical support to relatively smaller registered entities to assist them in determining whether their assets are critical to the Bulk-Power System.

ii. Comments

(a) Need for Additional Guidance

240. Many commenters, including NERC, agree with the Commission that there is a need for further guidance regarding the risk-based assessment methodology. Other commenters do not oppose the development of general guidance on what would constitute an acceptable risk-based assessment methodology, provided that this guidance does not rule out other approaches. Commenters also identify specific concerns that they believe would benefit from further guidance.

241. While first reiterating that the CIP Reliability Standards contain the appropriate specificity as performance based standards, NERC agrees that it could provide further guidance in the form of a ''supplemental guideline'' on performing risk-based assessments to be used to determine critical assets. NERC states that its Critical Infrastructure Protection Committee's Risk Assessment Working Group has begun development of such a guideline. NERC asserts that this guideline, when completed, will address the Commission's fundamental concern by providing guidance to responsible entities on how to perform the required risk-based assessments.

242. Numerous commenters agree that additional guidance is needed regarding a risk-based assessment methodology.[81] For example, Energy Producers and California Cogeneration comment that, without such guidance, responsible entities will not know whether they are

[78] *See* Order No. 672 at P 186–91.

[79] ''The term 'Reliable Operation' means operating the elements of the Bulk-Power System within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cyber security incident, or unanticipated failure of system elements.'' 16 U.S.C. 824o(a)(4).

[80] *See* CIP NOPR at P 100–05.

[81] *E.g.,* California Cogeneration California Commission, Congressional Representatives, Duke, Energy Producers, FirstEnergy, ISA99 Team, KCPL, MidAmerican, National Grid, ReliabilityFirst, Reliant, SDG&E and U.S. Power.

complying with the Requirement until they are audited. Arizona Public Service is also concerned that CIP–002–1 lacks sufficient detail and needs to provide further guidance so that responsible entities are not placed in the position of not knowing whether their risk-based methodologies will adequately identify all critical assets in a way that fully satisfies NERC's requirements. Arkansas Electric comments that without needed guidance, a responsible entity could invest large amounts of effort into the assessment, only to be found non-compliant later. Reliant comments that ERO guidance would benefit users of the Bulk-Power System, such as generators, that may not have sufficient information to properly determine whether their assets are critical.

243. While EEI opposes any modification to Requirement R1 of CIP–002–1 to provide additional specificity regarding the assessment methodology, it agrees that responsible entities would benefit from ''some basic guidance'' provided that it is non-prescriptive.[82] EEI supports guidance regarding the common understanding of the scope, purpose and basic direction of the methodology. EEI also urges that the process for developing this guidance should be open and transparent. Similarly, APPA/LPPC comment that they do not object to the proposal that NERC provide some basic guidance on the content of the methodology, provided that it allows needed flexibility to take account of the individual circumstances of a responsible entity.

244. A number of commenters identify specific topics that would benefit from further guidance. For example, NRC comments that the risk-based assessment should identify transmission lines, substations and generators that are relied on to operate or shut down nuclear generating stations as critical assets. U.S. Power maintains that additional guidance is needed as to when generating facilities and their related systems will be deemed ''critical'' to the Bulk Electric System. U.S. Power explains that, given the built-in reserve margin for generation in New England, absent a known local reliability need, any generator in New England could logically assume that none of its individual generating assets would be regarded ''critical.'' U.S. Power states that without additional guidance as to what the Commission and NERC intend, however, there is no way of knowing if this is an appropriate assumption. Further, it seeks additional guidance regarding blackstart units, noting that a generating unit that has blackstart capability but is not part of a system restoration plan may not be deemed critical to Bulk-Power System reliability.

245. Luminant comments that significant regional differences, such as geography, climate, demographics, electric system structure and demands, affect the identification of critical cyber assets and how the particular asset would be protected.

246. Several commenters agree with the Commission's statement that a risk-based assessment methodology should examine the consequences of the loss of the asset to the Bulk-Power System as well as the consequences if an adversary gains control of the asset. For example, Applied Control Solutions states that a proper risk-based assessment methodology should examine the consequences of the loss or improper operation of the assets to the Bulk-Power System. It also comments that the methodology should define ''risk'' as a formula (i.e., risk=frequency multiplied by consequence). Because there is insufficient data available to determine frequency, it should be assumed that an event will occur. Luminant also states that the risk-based assessment methodology should focus on the consequences of an outage, not the likelihood of an outage.

247. ISA99 Team suggests that the guidance to be developed by NERC should be written in a manner that assures that a larger portion of critical infrastructure assets, and associated cyber assets are included within the scope of the standards. In this regard, ISA99 Team states that the results of the current requirements, which are based on an unspecified ''risk-based'' approach, and which place no limits on what constitutes an acceptable risk, may or may not include sufficient assets to provide adequate protection for the bulk power grid. Thus, ISA99 Team argues that a more definitive means of assuring adequate scope needs to be established.

248. A number of entities commented on the Commission's proposal that the ERO and Regional Entities provide reasonable technical support to relatively smaller entities that may have difficulty determining whether a particular asset is critical because, for example, the impact of the facility may be dependent on their connection with a transmission owner or operator. NERC and ReliabilityFirst oppose this proposal, stating that such a ''consulting service'' would place an undue burden on the ERO and Regional Entities.[83] NERC and ReliabilityFirst believe that this creates a serious conflict to impartially assess compliance with the standards and suggest that, if such an external assistance is deemed necessary, it should be the obligation of the responsible entity's reliability coordinator or regional transmission organization. According to NERC, its reliability readiness program is in an ideal position to assess the effectiveness of an entity's risk-based assessment methodology, thus, no additional consulting role by NERC is needed.

249. In contrast, FirstEnergy agrees that NERC should provide guidance to entities without a wide-area view, such as a generation owner or a partial generation owner, on how to approach a risk-based assessment. Likewise, Northern California suggests that NERC establish a process for informal, case-by-case consultations with responsible entities that need assistance in complying with CIP–002–1. In addition, as part of the re-examination of CIP–002–1, Northern California encourages the incorporation of a formalized ''feedback loop'' to assist the industry in developing policies and procedures.

250. Xcel seeks clarification of CIP–002–1, Requirement R1.2.4, which provides that a risk-based assessment methodology consider ''systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.'' Xcel asks that either the Commission clarify or direct NERC to clarify the meaning of the phrase ''used for initial system restoration'' and specify whether it refers to facilities on the primary transmission restoration path or on all potential alternative transmission restoration paths.

251. MidAmerican seeks Commission clarification of the appropriateness of an N minus 1 criterion when applying a risk-based assessment methodology to critical assets. It states that NERC's CIP Reliability Standards require all affected entities to withstand the loss of one element without affecting the reliability of the Bulk-Power System. Yet, MidAmerican notes, the Commission's discussion uses the singular term ''asset'' in the first sentence when describing what a proper risk-based assessment methodology should examine. MidAmerican is concerned that this implies that a risk-based assessment methodology should be based on the loss of a single critical asset (transformer, line or generating

[82] *See also* Alliant, Arizona Public Service, ISO/RTO Council, Luminant, Northern California, OGE, Portland General and Southern.

[83] *See also* Entergy and ISO/RTO Council.

unit) one at a time. MidAmerican submits that the term ''asset'' should be revised to make clear that a broad-based cyber attack should essentially be assumed to affect several of an entity's critical facilities simultaneously.

252. Entergy suggests, as an alternative approach to critical asset identification, that the ERO provide a Design-Basis Threat (DBT)—a profile of the type, composition, and capabilities of an adversary—that would assist the industry as a technical baseline against which to establish the proper designs, controls and processes. Entergy claims that a DBT approach would address many of the Commission's concerns regarding the risk-based methodology. For example, a DBT would focus the appropriate emphasis on the potential consequences from an outage of a critical asset. In addition, a DBT would address the Commission's concern that responsible entities will not have enough guidance in developing a risk-based methodology and not know how to identify a ''critical asset.'' Entergy contends that a DBT approach would provide the industry with more certainty in implementing the CIP Reliability Standards.

iii. Commission Determination

253. The Commission believes that the comments affirm that responsible entities need additional guidance on the development of a risk-based assessment methodology to identify critical assets. While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance. The CIP NOPR proposed to direct that NERC modify CIP–002–1 to incorporate the guidance. However, we are persuaded by commenters that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity. Thus, we modify our original proposal and in this Final Order leave to the ERO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two. A responsible entity, however, remains responsible to identify the critical assets on its system.

254. Commenters raise a number of topics that they believe should be addressed in the NERC guidance, such as how to assess whether a generator or a blackstart unit is ''critical'' to Bulk-Power System reliability, the proper quantification of risk and frequency, facilities that are relied on to operate or shut down nuclear generating stations, and the consequences of asset failure and asset misuse by an adversary. We believe these are all appropriate topics to be addressed and direct the ERO to consider these commenter concerns when developing the guidance.

255. The Commission proposed in the CIP NOPR that the ERO and Regional Entities provide reasonable technical support to relatively smaller entities that may have difficulty determining whether a particular asset is critical because, for example, the impact of the facility may be dependent on their connection with a transmission owner or operator. While we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System.

256. Regarding MidAmerican's comments on use of the N minus 1 criterion when applying a risk-based assessment methodology to the identification of critical assets, we agree with MidAmerican that an N minus 1 criterion is not an appropriate risk-based assessment methodology for identifying critical assets. While the N minus 1 criterion may be appropriate in transmission planning, use of an N minus 1 criterion for the risk-based assessment in CIP–002–1 would result in the nonsensical result that no substations or generating plants need to be protected from cyber events. A cyber attack can strike multiple assets simultaneously, and a cyber attack can cause damage to an asset for such a time period that other asset outages may occur before the damaged asset can be returned to service. Thus, the fact that the system was developed to withstand the loss of any single asset should not be the basis for not protecting that asset. Also, we note that the definition of ''critical assets'' is focused on the criticality of the asset, not the likelihood of an outage. Based on this reasoning, in response to U.S. Power, we clarify that a generator should not assume that none of its individual generating assets would be regarded ''critical'' to the Bulk-Power System.[84]

257. With regard to Xcel's request for clarification regarding the meaning of the phrase ''used for initial system restoration,'' in CIP–002–1, Requirement R1.2.4, we direct the ERO to consider this clarification in its Reliability Standards development process.

258. As to Entergy's suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process. Likewise, the ERO should consider Northern California's suggestion that the ERO establish a formal ''feedback loop'' to assist the industry in developing policies and procedures.[85]

b. Scope of Critical Assets and Critical Cyber Assets

i. Data as a Critical Asset

(a) NOPR Proposal

259. In the CIP NOPR, the Commission noted that NERC's definition of ''cyber assets'' includes ''data.'' The Commission stated that ''marketing or other data essential to the proper operation of a critical asset, and possibly the computer systems that produce or process the data, would be considered critical cyber assets'' subject to the CIP Reliability Standards.[86] The Commission proposed to direct the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to include computer systems that produce the data.

(b) Comments

260. NERC agrees with the Commission that critical cyber assets include ''data,'' as specified in the definition. NERC then states that the ''data'' provision only refers to data associated with the reliable operation of the Bulk-Power System, thereby excluding ''marketing and other data'' as

[84] Further, Requirement R.1.2.3 provides that the risk-based assessment must consider ''generation resources that support the reliable operation'' of the Bulk-Power System. This language indicates that certain generation facilities, and presumably some facilities within a region identified as critical, must be considered in an assessment. Beyond this, we leave it to the ERO to provide sufficient guidelines to inform generation owners and operators on how to determine whether it should identify a facility as a critical asset. As discussed later in the Final Rule, the Commission will monitor and evaluate the outcome of this endeavor—the list of critical assets.

[85] Consistent with our approach in Order No. 693, the ERO should address NOPR comments suggesting specific new improvements to the CIP Reliability Standards. The Commission, however, does not direct any outcome other than that the comments receive consideration. *See* Order No. 693 at P 188.

[86] CIP NOPR at P 114.

well as data market systems that support the market function. NERC suggests that the Final Rule remove references to marketing and other data and supports referring, instead to ''reliability data.'' NERC adds that it is not arguing that these systems do not need protection, but merely that they are beyond the scope of the CIP Reliability Standards. NERC states that, only in cases where reliability functions and market functions are implemented within the same system, or are implemented on systems located within the electronic security perimeter, should they be protected by the CIP Reliability Standards, and then only as cyber assets located within the same electronic security perimeter as critical cyber assets.

261. Numerous other commenters contend that the Commission is mistaken to consider ''marketing and other data'' as a critical cyber asset. For example, NRECA comments that marketing data seldom performs a reliability-related function. Northeast Utilities states that only data pertaining to design or operating specifications necessary for the operation of cyber assets should be included in the definition of cyber assets. PG&E states that the Commission's proposal to include ''marketing and other data'' is unnecessary because the CIP Reliability Standards already apply to data that are housed and maintained within critical cyber assets and information about critical cyber assets. PG&E asserts that Requirement R4 of CIP–003–1 specifically protects critical cyber asset information, so no additional modifications are needed.[87]

262. Bonneville requests clarification whether the Commission's reference to marketing data and system data are intended to apply to data and systems related to power transactions to be delivered physically about which data are sent to grid operators (e.g., systems that generate E-tags) or all marketing data and systems even if the transactions are settled financially and never get to physical delivery.

263. MidAmerican agrees with the Commission on the need for additional guidance regarding the definition of ''data'' as critical cyber assets. It recommends deletion of the term ''data'' from the NERC definition of a ''critical cyber asset'' and, instead, its inclusion in the information protection standard. MidAmerican contends that access to data is of secondary importance when compared to access to a physical critical cyber asset and, thus, data should be protected as any other critical asset information would be protected.

264. ISO/RTO Council and Ontario Power argue that, although the computers and other devices that contain data may use a routable protocol or may be dial-up accessible, the data itself does not use a routable protocol, nor is it, in its own right, dial-up accessible. Therefore, they submit that Reliability Standard CIP–002–1 does not require that ''data'' be considered a critical cyber asset. In addition, ISO/RTO Council argues that, since every responsible entity's definitive list of critical cyber assets is developed pursuant to Reliability Standard CIP–002–1, Requirement R3, the ''further qualified'' reference in Requirement R3 applies to the use of the term ''critical cyber asset'' wherever the term is used in the CIP Reliability Standards. ISO/RTO Council believes that including data as a critical cyber asset would go beyond the scope and intent of any of the Reliability Standards.

265. ISO–NE and SPP agree with ISO/RTO Council that data by itself does not meet the definition of a critical cyber asset. ISO–NE states that the Commission is further viewing data as a potential critical asset. ISO–NE agrees with this view in concept, but believes that consideration of reliability data is already intrinsic to the process of evaluating assets to determine their criticality. Such reliability data are ''real-time data'' and are highly transient as they pass through, and are presented by, such supporting critical cyber assets. Given that protection of critical cyber assets is already addressed, the protection of the data component of a cyber asset during its instance of viability as useful reliability data is satisfied. To address a broader focus of data protection would expand the scope of the current CIP Reliability Standards. Such a focus deserves considerable review and discussion. If the Commission continues to have concern regarding data protection from a broader view, ISO–NE recommends this be considered in a future proceeding.

266. SoCalEdison is concerned that applying the CIP Reliability Standards to data that are essential to the proper operation of a critical asset and including computer systems that produce the data might greatly increase the scope of CIP–002–1 and will have a major impact on the industry's ability to meet the standards requirements schedule. SoCalEdison argues that, if the Commission directs these modifications to the standard, they should be handled through the NERC Reliability Standards development process which should consider any impact to the implementation schedule.

267. OGE also is concerned that a definition of ''critical cyber assets'' that could include computer systems that produce or process such sensitive data may encompass network servers and devices. If network servers and devices are considered critical cyber assets, OGE argues that additional controls will be necessary to isolate and protect these network servers and devices. These additional controls will provide only a minor increase in protection to the bulk electric system.

268. Idaho Power supports the protection of data that defines location, network topography, device descriptions, and similar information; however, Idaho Power cannot support the position that data originating or used in an Energy Management System, for instance, should be treated as ''critical'' after the fact. In Idaho Power's view, the actual data, upon transfer to data historian servers, fails to meet any definition of ''critical.''

269. Juniper recommends that other enterprise databases, such as human resources data, be considered part of the critical assets. Juniper states that its concern applies to any data that can enable a hacker to gain access to cyber assets. Juniper comments that any essential data that could allow an attacker to weaken or defeat any cyber or physical security must be considered a critical cyber asset.

(c) Commission Determination

270. As discussed above, commenters that address the subject uniformly oppose the CIP NOPR statement that ''marketing or other data essential to the proper operation of a critical asset, and possibly the computer systems that produce or process the data, would be considered critical cyber assets'' subject to the CIP Reliability Standards. These commenters contend that marketing data typically does not qualify as a critical cyber asset and the Commission's proposal is beyond the current scope of the CIP Reliability Standards. Moreover, several commenters suggest that some data and support systems may fit the definition of *critical asset* and, thus, supporting critical cyber assets must comply with CIP–002–1.

271. The Commission remains concerned that, while not all marketing data or other data may be considered a critical cyber asset essential to the proper operation of a critical asset, there may be times where it is properly classified as such. For example, if a critical asset is configured such that it cannot operate and support the

[87] *See also* Alliant, EEI, ISO–NE, ISO/RTO Council, Luminant, National Grid, Ontario Power, ReliabilityFirst, SDG&E, SPP and WAPA.

reliability and operability of the Bulk-Power System without a real-time stream of data, that data fits the definition of a critical cyber asset, and should be protected. Once a particular piece of data is no longer needed by the critical asset, it is no longer a critical cyber asset. On this point, we agree with commenters that there is a temporal characteristic to data as a critical asset.

272. Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP–002–1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset. In doing so, the ERO should consider Juniper's comments. Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data.

273. The Commission also agrees with ISO–NE that experience in the implementation of the CIP Reliability Standards may indicate a need to further address this topic in a future proceeding.

ii. Control Systems

274. In the CIP NOPR, the Commission expressed concern that sufficient rigor is applied in examining whether control systems are determined to be critical assets.[88] The Commission stated that, while it seems obvious that an evaluation of a control system for critical asset status would consider the potential loss of operability, the Commission also believes that such an evaluation should examine any misuse of the control system and the impact this misuse could have on any electric facilities that the responsible entity controls, and the combined impact of such facilities.

(a) Comments

275. NERC and ReliabilityFirst comment that the Commission appears to have incorrectly concluded that ''control systems'' are critical assets. They explain that, in context, the control center, substations or power plant could be a critical asset. The ''control system,'' however, would be a critical cyber asset.

276. SPP concurs with the Commission's assertion that consideration of misuse of control systems should be part of the risk-based assessment. Compromise and misuse of a cyber asset often pose greater risks to the reliability of the Bulk-Power System than an induced total failure of the cyber asset. SPP comments that both insider and external threats should be considered as part of the risk-based assessment. In contrast, Entergy opposes the Commission's proposal to require an evaluation of the misuse of control systems.

277. Applied Control Solutions comments that there should be a formally accepted method for identifying critical cyber assets, explaining that existing methods are often reliability-based, not cyber-based, resulting in entities reporting too few assets.

278. ISA99 Team objects to the exclusion of communications links from CIP–002–1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable—by testing and experience. In contrast, Energy Producers notes that CIP–002–1 as proposed by NERC provides that a critical cyber asset must have either routable protocols or a dial-up connection. Energy Producers states that this is a useful, objective criterion which will assist in the unambiguous identification of such assets and therefore should be retained.

(b) Commission Determination

279. The Commission accepts the explanation of the ERO and ReliabilityFirst that a control system could be a critical cyber asset, but not a critical asset.[89]

280. The Commission has two concerns regarding the misuse of facilities, and clarifies those concerns here. First, Requirement R1.2.1 requires responsible entities to consider control centers and backup control centers as potential critical assets. In determining whether those control centers should be critical assets, we believe that responsible entities should examine the impact on reliability if the control centers are unavailable, due for example to power or communications failures, or denial of service attacks. Responsible entities should also examine the impact that misuse of those control centers could have on the electric facilities they control and what the combined impact of those electric facilities could be on the reliability of the Bulk-Power System. The Commission recognizes that, when these matters are taken into account, 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.

281. Second, the Commission is concerned about the misuse of a control system that controls more than one asset. The assets could be multiple generating units, multiple transmission breakers, or perhaps even multiple substations. All of the controlled assets could be taken out of service simultaneously due to a failure or misuse of the control system. Individually, perhaps none of the controlled assets would be considered as a critical asset. However, with a simultaneous outage due to the single point of control, the controlled assets might affect the reliability or operability of the Bulk-Power System and, therefore, should be considered as critical assets. In that case, the common control system should be considered a critical cyber asset.

282. Therefore, consistent with the discussion above, the Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets. The clarification of our concern over misuse of control systems addresses Entergy's comment on this issue as well.

283. The Commission concurs with SPP that both insider and external threats should be considered as part of a risk-based assessment.

284. We share Applied Control Solutions' concern that too few assets may be identified as critical cyber assets. However, there is no evidence that will be the case, and there is no formally accepted method for identifying critical cyber assets before us at this time. Therefore, we decline to direct that such a method be incorporated into the CIP Reliability

[88] CIP NOPR at P 115.

[89] As was stated in the CIP Assessment, a ''control system'' is a device or set of devices to manage, command, direct or regulate the behavior of other devices or systems. It is typically a specialized computer system or programmable logic controller that manages, commands, directs or regulates the behavior of other devices or systems in a physical environment, *e.g.*, open or close switches or relays, start or stop motors, or control motor speed. In the case of the Bulk-Power System, control systems consist primarily of sophisticated computer hardware and software designed to process the mass of real-time data associated with the Bulk-Power System and enable its reliable operation by, among other things, monitoring the grid through remote sensors, sounding alarms when grid conditions warrant, and operating equipment in field locations.

Standards at this time. The Commission may revisit this circumstance in a future proceeding.

285. As to the conflicting comments of ISA99 Team and Energy Producers, Requirement R2 of CIP–002–1 provides that a critical cyber asset must either have routable protocols or dial-up access. Energy Producers argues that Requirement R2 should be retained, while ISA99 Team argues that devices that use non-routable protocols should also be considered as possible critical cyber assets. We do not find sufficient justification to remove this provision at this time. However, we direct the ERO to consider the comment from ISA99 Team. We also do not find sufficient justification to order the inclusion of communication links in CIP–002–1 at this time.

iii. Explanation Why an Asset Chosen or Not Chosen as Critical

286. In the CIP NOPR, at P 115, the Commission expressed concern that all critical assets be identified. To further this goal, the Commission interpreted the phrase, ''[t]he risk-based assessment shall consider the following assets * * *'' in Requirement R1.2 to mean that a responsible entity must be able to show why, based on the risk-based methodology, specific assets were chosen or not chosen. The Commission proposed to direct that the ERO modify Requirement R1.2 to make this obligation explicit.

(a) Comments

287. Most commenters addressing the subject oppose the Commission's proposal.[90] For example, MidAmerican comments that a requirement that a responsible entity provide reasons for selecting or not selecting a particular asset as critical is unreasonably burdensome and unnecessary because this should be adequately addressed when more direction is given for the assessment methodology and selection criteria for critical assets. Likewise, EEI and Entergy oppose the Commission's proposal as unnecessary, contending that responsible entities will identify critical assets based on the risk-based assessment methodology required by CIP–002–1, which will be subject to audit. EEI questions what further explanation an entity could provide beyond the assessment methodology. Entergy notes that many entities operate hundreds of substations and thousands of pieces of field equipment, and a requirement to defend the exclusion of specific equipment would be onerous.[91]

(b) Commission Determination

288. To clarify, the Commission did not propose to direct that the ERO develop a requirement for responsible entities to document why each specific asset was identified or not identified as ''critical.'' Rather, the Commission's intent was that a responsible entity must be able to explain such determinations, for example upon inquiry by an auditor, to confirm compliance with the Reliability Standard. Nonetheless, we are persuaded by the commenters that the documentation of a responsible entity's risk-based assessment methodology pursuant to Requirement R1.1 and the results of its annual application of the methodology pursuant to Requirement R2 should suffice to explain a responsible entity's asset determinations. Accordingly, the Commission will not direct the ERO to develop a modification to address this concern. However, if experience shows that responsible entities are failing to consider in their assessments specific types of assets that the Commission, ERO or others believe should be included in an assessment and therefore not in compliance with the Reliability Standard, there may be a need to revisit this matter in the future.

c. Internal Approval of Risk-Based Assessment

i. NOPR Proposal

289. Requirement R4 of CIP–002–1 requires that a senior manager ''or delegate(s)'' must approve annually the list of critical assets and critical cyber assets. In the CIP NOPR, the Commission proposed to direct that the ERO develop a modification to CIP–002–1 to include a requirement that a senior manager annually review and approve the risk-based assessment methodology.[92] The Commission stated that senior management approval of the risk-based assessment methodology helps to implement Blackout Report Recommendation 43, which calls for establishing clear authority and ownership for physical and cyber security.[93]

ii. Comments

290. Alliant, APPA/LPPC, Congressional Representatives, EEI, KCPL and Luminant agree with the Commission that it is important that there is internal oversight of the responsible entity's activities. EEI adds that, although senior manager review of the risk-based assessment methodology is implicit in the current CIP Reliability Standards, such a provision should be made explicit through the Reliability Standards development process to establish the ''clear authority'' recommended by the Blackout Report. Luminant adds that such a provision would provide a degree of certainty for a responsible entity's senior management to approve the risk-based assessment methodology the responsible entity adopts. KCPL also supports NERC's development of an ''explicit'' requirement that senior management review and approve a responsible entity's risk-based assessment methodology.

291. METC–ITC believe that the Commission can further strengthen the CIP Reliability Standards by raising the apparent level of responsibility of CIP compliance to a corporate officer level, replacing ''senior manager'' with ''officer'' in such instances throughout the CIP Reliability Standards. In contrast, Northern Indiana claims that senior management might not be the most knowledgeable about cyber security issues and urges the Commission to continue to allow a responsible entity to delegate this review to knowledgeable personnel.

292. ISO/RTO Council argues that the requirement for internal oversight already is an implicit requirement under the CIP Reliability Standards. In ISO/RTO Council's view, it is abundantly clear that the senior manager is fully accountable for both the thoroughness of the methodology used to establish the critical asset list as well as the completeness of the list itself.

293. Bonneville seeks clarification whether the intent of the Commission's proposal is to make senior managers personally accountable for a responsible entity's violation of the CIP Reliability Standards so that the senior manager is subject to civil penalties. Bonneville comments that, if this is the intended purpose or result, then the extent of such personal liability must be made clear so that affected senior managers can take necessary precautions, such as obtaining additional insurance coverage. NRECA raises similar concerns regarding a senior manager's penalty liability.

[90] *E.g.,* Alliant, EEI, ISO/RTO Council, KCPL, MidAmerican, National Grid, OGE and Tampa Electric.

[91] *See also* ISO/RTO Council, National Grid, PG &E and Tampa Electric.

[92] *See* CIP NOPR at P 106–08 for the Commission's discussion and proposal on this topic.

[93] *See* U.S.-Canada Power System Blackout Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations (April 2004) (Blackout Report). The Blackout Report is available on the Internet at *http://www.ferc.gov/industries/electric/indus-act/blackout.asp.*

iii. Commission Determination

294. The Commission adopts its CIP NOPR proposal and directs the ERO to develop, pursuant to its Reliability Standards development process, a modification to CIP–002–1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology. This determination is consistent with the Blackout Report's recommendation to establish clear authority and ownership for physical and cyber security. Further, regardless of whether the current Requirements implicitly require senior manager review of the assessment methodology, we believe the matter is too important to rely on inference. Accordingly, the Commission directs the ERO to develop a modification to CIP–002–1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology.

295. With regard to Northern Indiana's concerns, we are not directing a revision to the current language of Requirement R4 which provides for ''the senior manager or delegate(s)'s approval'' of the list of critical assets and list of critical cyber assets. As we understand the provision, the senior manager still retains ultimate responsibility for the determinations of his or her delegate(s). Otherwise, senior management could avoid responsibility by 'delegating downward.'

296. With regard to METC–ITC's comment, the ERO should consider in its Reliability Standards development process the suggestion that the CIP Reliability Standards require oversight by a corporate officer (or the equivalent, since some entities do not have corporate officers) rather than by a ''senior manager.''

297. In response to comments by Bonneville and NRECA, the Commission clarifies that we do not intend that an individual employee of a user, owner or operator of the Bulk-Power System will be subject to a penalty pursuant to section 215 of the FPA because a responsible entity violates a CIP Reliability Standard. This matter is addressed in more detail in our discussion of CIP–003–1.

d. External Oversight of Critical Assets Identification To Provide Regional Perspective

i. NOPR Proposal

298. The CIP NOPR emphasized that the responsibility for identifying critical assets should be placed on the individual responsible entity as the asset owner or operator, and not shifted to Regional Entities or another organization.[94] In addition, the Commission expressed its belief that a systematic approach to external oversight of the identification of critical assets would assure a wide-area view and thereby better ensure that responsible entities are identifying appropriate assets as ''critical.'' The Commission explained that, without external oversight using a wide-area view, trends or deviations may not be identified prior to an incident or audit. The CIP NOPR also noted that a wide-area view would help to ensure that assets that have regional importance, such as for reactive power supply, are included as critical assets. Therefore, the Commission proposed that the ERO develop a modification to CIP–002–1 to include a mechanism for the external review and approval of critical asset lists based on a regional perspective by the Regional Entities, possibly among others. The Commission stated that, while proposing that the Regional Entities perform this review function, it did not exclude the possibility of a critical asset review process that allows for the participation of other organizations, such as transmission planners and reliability coordinators.

ii. Comments

(a) Responsible Entity for Identifying Critical Assets

299. Several commenters, including ISO/RTO Council, EEI, FirstEnergy, National Grid and Northeast Utilities, agree with the Commission that responsibility for identifying critical assets should not be placed on the Regional Entities or any organization other than the categories of applicable entities currently identified in CIP–002–1. They believe that this responsibility rightfully rests with the asset owner or operator, and the Regional Entities would be overburdened by such a task.

300. In contrast, AMP Ohio advocates the revision of CIP–002–1 to make Regional Entities responsible for the identification of critical assets because they have an area-wide view of the grid—as opposed to small generation owners, generation operators and load serving entities that have a limited view of the Bulk-Power System. AMP Ohio also argues that making small generation owners, generation operators and load serving entities responsible for asset identification would place a burden on these small entities that they are ill-positioned to bear. AMP Ohio explains that it is not proposing that responsible entities abdicate responsibility but, rather, suggests that the Regional Entity take the first step to identify critical assets. The asset owner or operator, as a responsible entity, must then ensure that the critical cyber assets associated with the critical asset are identified and protected. AMP Ohio suggests that, if responsible entities remain responsible for identifying assets, the CIP Reliability Standard should include a safe harbor provision for good faith compliance, even if subsequent events demonstrate that critical assets may have been overlooked.

301. SPP and ReliabilityFirst suggest a modification to CIP–002–1 that would allow an entity to rely on the assessment of another entity with interest in the matter. For example, a merchant generator may through a legitimate assessment determine that its plant is not critical whereas the balancing authority's assessment indicates that it is. They suggest that in such a situation the merchant generator would accept the risk-based assessment of the balancing authority as a substitute for performing its own assessment with limited data.

(b) Need for External Review and Alternatives

302. While some commenters agree with the Commission that there is a need for external review and approval of a responsible entity's critical asset list, others believe that such a requirement is unnecessary.

303. Arkansas Electric, Juniper, MidAmerican, National Grid, Ontario IESO, and U.S. Power agree with the Commission that a process for regional review of an entity's critical asset list by either the ERO or the Regional Entity would be beneficial. According to Arkansas Electric, this would provide an entity with the opportunity for a review of its critical asset list prior to a full CIP audit. Arkansas Electric is concerned that, without such a review, entities could be subject to sanctions based on a critical asset list later deemed deficient by an auditor. MidAmerican finds that a regional perspective could add consistency to the critical asset determination. U.S. Power maintains that, in organized markets where a generator does not typically possess a ''regional perspective'' to objectively determine the criticality of an individual asset, external review could be helpful in assuring that a regionally consistent approach is followed; and that such determinations are based on the most relevant, available information.

304. FirstEnergy agrees with the Commission that a formal or systematic approach to external oversight of the identification of critical assets would

[94] *See* CIP NOPR at P 111–13.

better ensure that responsible entities are identifying similar assets. FirstEnergy comments that external review is crucial to the comprehensive application of the CIP Reliability Standards and such review should be conducted by an entity with a wide-area view.

305. National Grid comments that it would support the development of an appropriate mechanism for Regional Entities to collection documentation of each responsible entity's assessment methodology and list of critical assets. However, National Grid would not support a requirement for Regional Entity pre-approval of the methodology or list because the Regional Entity lacks the necessary expertise and resources. Similarly, Northern Indiana supports external review, particularly where lists of cyber security assets will not be shared and responsible entities must determine their asset lists based on mutual distrust. However, Northern Indiana opposes requiring approval of a responsible entity's list of critical assets by the entity conducting the external review. It also opposes granting Regional Entities or reliability coordinators the ability to supplement a critical asset list. This concern would be removed, however, if the regional entity approved the risk-based assessment methodology, rather than the list of critical assets.

306. In contrast, NERC and others oppose modifying CIP–002–1 to require external review and approval of critical asset lists.[95] NERC requests that the Commission allow the current oversight framework—which includes audits, readiness reviews and self-certification—to work without imposing new or different requirements from the current CIP Reliability Standards. Similarly, EEI comments that, while it understands the Commission's view that external oversight may have potential value by providing a wide-area view, it believes that NERC's Uniform Compliance Monitoring and Enforcement Program already provides effective tools that may provide such oversight. EEI does not, however, oppose voluntary random spot checking as a means to provide an ''area-wide view'' before the ''auditably compliant'' stage.

307. Alliant objects to external approval of a critical asset list because the ERO auditing regime provides a ''wide-area view'' and external approval would require an appeals process that would delay implementation without accruing reasonable benefits. Duke claims that the ERO's guidance document should result in adequate consistency in the development of critical asset lists and suggests that any external review should be optional. Southern contends that a responsible entity is generally in the best position to determine which assets are critical to the Bulk-Power System and, if needed, industry experience can be shared through existing forums and through the voluntary exchange of information. Puget Sound and others propose that industry forums could be used to promote a wide-area view in developing critical asset lists. Idaho Power insists that regional concerns should be addressed before an entity develops its critical asset list.

308. Many of the commenters that oppose an external review and approval process believe that the Commission's objectives can be accomplished through a Regional Entity audit process.[96] SERC CIPC claims that the regions, if presented with a raw list of asset names, will have no basis on which to state whether the list is sufficient or not. According to SERC CIPC, during the audit process, the audit team will review the risk-based assessment methodology.

(c) Appropriate Organization to Conduct External Review

309. Among the commenters that support the need for external oversight, some prefer that an organization other than a Regional Entity be made responsible for external oversight. For example, ISO/RTO Council believes that the reliability coordinator is in the best position to provide such oversight because it has a wide-area view that is focused on grid operation. ISO/RTO Council believes that Regional Entities need to remain independent to enforce the CIP Reliability Standards and should not be involved in CIP Reliability Standard implementation; and likewise, considers that transmission planners are not sufficiently focused on the operational aspects of the grid where cyber security is most critical. Further, ISO/RTO Council suggests that reliability coordinator oversight be limited to a review of the methodologies used to identify critical assets, since reliability coordinators have no special expertise in identifying critical *cyber* assets.

310. By contrast, Ontario IESO, Reliant, ReliabilityFirst and SPP advocate that reliability coordinators, not Regional Entities, should provide oversight of critical asset identification. Ontario IESO and SPP believe that the reliability coordinators are most suited for this task because they are directly involved in the daily activities of ensuring Bulk-Power System reliability. They comment that the reliability coordinators currently perform a wide-area function that includes studying power system dynamics and interrelationship of assets as well as coordination among neighboring systems. Reliant urges that the Commission require the reliability coordinator to play a major role in the external review of critical asset lists because it possesses a broad array of operating and system data.

311. Ontario IESO comments that, because Regional Entities perform a critical CIP Reliability Standards development and compliance role, Regional Entity approval of an entity's critical asset list creates a conflict of interest in the situation where a Regional Entity is required to investigate and enforce non-compliance of a CIP Reliability Standard. The Regional Entity may have approved the critical asset list and thus may be reluctant to subsequently find a deficiency in the list discovered during the course of a compliance investigation. Ontario IESO also respectfully suggests that Regional Entities lack the technical expertise and intimate knowledge of their members' power system equipment and behaviors to provide the necessary oversight in the determination of critical asset lists.

312. Ontario IESO suggests that, in the event an asset owner and the reliability coordinator disagree as to whether an asset should be listed as critical, the latter should prevail. APPA/LPPC ask that the Commission direct NERC to develop written procedures for a responsible entity to challenge an external, third-party decision to alter a responsible entity's list of critical assets. APPA/LPPC argue that, regardless of the reviewer, an appellate process akin to the process described in Rule 410 of the NERC Rules of Procedure, providing for appeals to the Commission, is needed. EEI and Alliant also believe that an appeal process would be needed if regional oversight occurs.

(d) Confidentiality Concerns

313. Many of the commenters that oppose an external review and approval process are concerned that an external review process will create new issues regarding the protection of sensitive information that inevitably is included

[95] *E.g.,* Alliant, Mr. Brown, Duke, EEI, Entergy, Idaho Power, Luminant, OGE, Ontario Power, Puget Sound, SERC–CIPC and Southern.

[96] *E.g.,* Duke, EEI, Entergy, National Grid, OGE and SERC–CIPC.

in the critical asset lists.[97] These commenters believe that the review of critical asset lists during on-site audits would better protect this highly-sensitive information.

314. EEI and Manitoba Hydro express concern that off-site, third party review of a critical asset list may conflict with an entity's responsibility to protect information such as a critical asset list in CIP–003–1, Requirement R4.1. EEI urges that the Final Rule clarify that this information should only be divulged in on-the-premise audits.

315. CEA is also concerned that the Commission's proposal to include a mechanism for the external review and approval of critical assets lists would involve the submission of sensitive information. CEA and Manitoba Hydro maintain that some Canadian utilities are prohibited from sharing security information with U.S. authorities. In addition, some utilities regard sharing sensitive security information externally or with a foreign entity as a security risk. Currently, sensitive information is kept on site and shared with external audit teams during visits and the information remains on-site following the audit. The Commission's proposed changes would require sensitive material to be shared on a regular basis and stored externally and perhaps in a foreign jurisdiction. Given the impact on Canadian utilities from such changes to the CIP Reliability Standards, CEA requests that the Commission exercise caution with respect to this issue.

316. Xcel asks, in a situation where an entity's risk-based assessment identifies a critical asset owned by another entity, how should this information properly be communicated while maintaining confidentiality? Xcel recommends that the Regional Entities develop confidentiality protocols to address such situations.

317. SDG&E requests clarification that information associated with the CIP Reliability Standards will be treated with confidentiality. Tampa Electric and SoCal Edison also urge that steps be taken to protect confidentiality if information is released to accomplish external reviews. SoCal Edison is concerned with the risks associated with storing critical information in a common place.

318. Bonneville agrees with the Commission's goal of providing a mechanism for the external review and approval of responsible entities' critical asset lists based on a regional perspective; however, it is concerned that the Commission's proposal could result in FOIA concerns for Bonneville and other federal entities. Under FOIA, the release of information to an external party generally waives any privileges against disclosure with respect to subsequent requests to the federal agency for that same information. Bonneville is concerned that submission of critical asset information to the Regional Entity, particularly disclosure of the vulnerability-related rationales for including and documentation of why it chose to exclude particular facilities from inclusion on the critical asset list, may act as such a waiver. In addition, Bonneville notes that external reviewers of critical federal security information may need to obtain federal security clearances before federal entities can allow such review.

iii. Commission Determination

(a) Responsible Entity for Identifying Critical Assets

319. The Commission affirms its CIP NOPR determination that responsibility for identifying critical assets should not be shifted to the Regional Entity or another organization instead of the applicable responsible entities identified in the current CIP Reliability Standards. As we stated in the CIP NOPR,[98] and confirmed by commenters, such a shift would not improve the identification of critical assets, but would likely overburden the Regional Entities. While we are sympathetic to AMP Ohio's concerns regarding small generation owners, generation operators and load serving entities that have a limited view of the Bulk-Power System, we believe that NERC's development of guidance on the risk-based assessment methodology and our direction above to provide assistance to small entities should support the efforts of entities—both small and large—in performing a proper assessment. We do not believe that the lack of a wide-area view is sufficient reason to forego an assessment or taking responsibility.

320. We will not allow a ''safe harbor'' for good faith compliance as requested by AMP Ohio. We do not believe that blanket waivers from an enforcement action are appropriate in this context and have previously denied other requests for safe harbors from enforcement.[99] Rather, we believe that demonstrable good faith compliance is a legitimate mitigating factor in an enforcement action.

321. SPP and ReliabilityFirst suggest modifying CIP–002–1 to allow an entity to rely upon the assessment of another entity with interest in the matter. We believe that this is a worthwhile suggestion for the ERO to pursue and the ERO should consider this proposal in the Reliability Standards development process. We note that, even without such a provision, an entity such as a small generator operator is not foreclosed from consulting with a balancing authority or other appropriate entity with a wide-area view of the transmission system.

(b) Need for External Review and Alternatives

322. The Commission adopts its CIP NOPR proposal to direct that the ERO develop through its Reliability Standards development process a mechanism for external review and approval of critical asset lists. The Commission finds that an external review of critical assets by an appropriate organization is needed to assure that such lists are considered from a wide-area view (i.e., from a regional perspective) and to identify trends in critical asset identification. Further, while we recognize that individual circumstances may likely vary, an external review will provide an appropriate level of consistency.

323. The Commission disagrees with the suggestion of Luminant and others that external review should be voluntary. The identification of critical assets pursuant to CIP–002–1 is crucial to cyber security protection because this determination controls whether a responsible entity must comply with the remaining CIP requirements in CIP–003–1 through CIP–009–1. External review will help ensure that responsible entities have an accurate and complete list of critical assets, which will in turn allow them to be appropriately protected to further the security of the nation's Bulk-Power System. Allowing external review as a voluntary measure is not adequate to ensure that responsible entities are prepared to address cyber vulnerabilities and cyber threats. Based on the same reasoning, we reject the suggestion of Northern Indiana and others that the external review should only address the assessment methodology, and not critical asset lists.

324. The Commission also disagrees with commenters who insist that the external review can be performed pursuant to the ERO's and Regional Entity's current compliance and enforcement programs, and the audit process in particular. While the Commission decided earlier in the Final Rule to rely on the ERO and regional audit processes to examine exceptions

[97] *E.g.,* Duke, EEI, Entergy, Manitoba Hydro, National Grid and SERC–CIPC.

[98] CIP NOPR at P 111.

[99] *See, e.g., North American Electric Reliability Council,* 119 FERC ¶ 61,060 at P 133; *order on reh'g,* 120 FERC ¶ 61,260 at P 41 (2007).

to compliance based on ''technical feasibility,'' the Commission does not believe that the audit process will provide timely feedback to a responsible entity regarding critical asset determinations. Review of critical asset lists through individual audits would span a significant period of time, measured in years, during which time such lists would not undergo review and possibly gaps in security could result. While EEI's suggestion of spot checks prior to the ''auditably compliant'' stage would provide more timely feedback it would, by design, not be comprehensive. The Commission concludes that a structured program for the formal, timely review of critical assets lists is a reasonable means to provide timely, comprehensive guidance to responsible entities on the adequacy of their critical asset lists.

325. The Commission agrees with Ontario IESO that in a dispute between a responsible entity and the external reviewer over whether to identify an additional asset as critical, the external reviewer should prevail. (However, an external reviewer's role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets.) We recognize, however, that there may be a legitimate reason for a responsible entity to dispute such a determination, possibly through an appeal. We leave it to the ERO to determine the need for such an appeal mechanism and, if appropriate, the development of appropriate procedures (or reliance on appeal procedures currently provided in the NERC Rules of Procedure). While the ERO may determine that an appeals process is a necessary aspect of this program, we do not believe that the burden of such appeals outweighs the benefits of the external review of critical asset lists.

(c) Appropriate Organization To Conduct External Review

326. The Commission in the CIP NOPR proposed that the Regional Entities be responsible for the external review of critical asset lists, and also expressed a willingness to consider a review process that allows for the participation of other organizations such as reliability coordinators and transmission planners. As indicated above, a number of commenters question whether the Regional Entities have the expertise or resources to conduct the reviews. Rather, there was considerable support for reliability coordinators conducting the external review because of their technical expertise, their wide-area view and their role of coordinating among neighboring systems.

327. The Commission believes that the Regional Entities must have a role in the external review to assure that there is sufficient accountability in the process. Further, a Regional Entity role is necessary because the Regional Entities and ERO are ultimately responsible for ensuring compliance with Reliability Standards. For example, if the ERO determines that an appeals process is needed, this process cannot rest with an active owner or operator of the Bulk-Power System such as a reliability coordinator. Moreover, the ERO and the Commission have oversight authority of the Regional Entities' programs and procedures pursuant to section 215 of the FPA.

328. Beyond the direction that the Regional Entities maintain a role in the external review process to assure that there is sufficient accountability, we leave to the ERO to determine whether the Regional Entities have, or can timely develop, the resources to conduct the external reviews.[100] Alternatively, the ERO may determine that another entity such as reliability coordinators may be best equipped to conduct the reviews. While commenters have made what the Commission believes to be a strong case that reliability coordinators are the appropriate entity to perform the reviews, the ERO should decide the best approach with its understanding of the capabilities and limitations of the Regional Entities. Regardless of this determination, however, the Commission notes that the Regional Entities have the oversight responsibility.[101]

329. Based on the above discussion, the Commission directs the ERO, using its Reliability Standards development process, to develop a process of external review and approval of critical asset lists based on a regional perspective.

e. Confidentiality Concerns

330. The Commission agrees with commenters that critical asset lists contain sensitive information that needs to be protected from public dissemination. The Commission, however, does not believe that this concern is a persuasive rationale for not having an external review mechanism. Rather, adequate safeguards need to be developed to assure that the information contained in critical asset lists are not released during the external review process. While Requirement R4 of CIP–003–1 obligates a responsible entity to ''implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets,'' the Commission does not view this as inherently conflicting with an external review process that has adequate safeguards to prevent the release of sensitive information.

331. In developing an appropriate external review mechanism, the ERO should include features for the controlled delivery of critical assets to the entity performing the external review. Likewise, the ERO should identify minimum safeguards that the external reviewer must deploy to protect sensitive information from disclosure. We agree with commenters' concern that the external reviewer should not become a ''central repository'' for critical asset lists, and this information should be returned to the responsible entity once the review is complete. The ERO should develop any other safeguards that it believes to be appropriate to protect the disclosure of sensitive information during the external review process.

332. CEA and Manitoba Hydro comment that some Canadian utilities are prohibited from sharing security information with U.S. authorities. They also note that some Canadian utilities regard sharing sensitive security information externally or with a foreign entity as a security risk. In response, the Commission's Final Rule only addresses the obligations of users, owners and operators of the Bulk-Power System in the United States (excluding Hawaii and Alaska). Accordingly, the Commission's directives regarding the development of an external review mechanism applies only to entities subject to the Commission's jurisdiction pursuant to section 215 of the FPA. Whether a similar review process is appropriate or lawful in other jurisdictions is beyond the scope of this Final Rule.

333. Bonneville comments that external review could result in FOIA concerns for Bonneville and other federal entities. It also cautions that external reviewers of critical federal security information may need federal security clearances before being allowed access to classified information. In response to Bonneville, we agree that a governmental entity subject to FOIA requirements should not be required to share sensitive information about

[100] The Commission does not believe that Regional Entity review creates a conflict of interest as claimed by some commenters because the Regional Entity has no pecuniary interest. The mere fact that a Regional Entity performs a development and compliance role is not a sufficient reason to find a conflict of interest.

[101] The Commission notes that general reliance on Regional Entity oversight does not preclude the Commission, the ERO or a Regional Entity from exercising its authority to review critical asset lists, whether resulting from a complaint, an incident or on its own initiative.

critical assets lists that could be deemed a waiver of FOIA protection that is otherwise available. Nonetheless, a governmental entity's identification of critical assets should be subject to appropriate oversight. Thus, we direct the ERO, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities can safeguard sensitive information. The ERO should consult with governmental entities that are subject to the CIP Reliability Standards in developing such appropriate provisions and we, likewise, encourage Bonneville and other governmental entities to participate in the development of such provisions.

334. Further, if a governmental entity has classified material regarding its critical assets, this information may not be disclosed except in accordance with controlling laws and regulations. The ERO's external review process must explicitly recognize this limitation.

f. Interdependency

i. NOPR Proposal

335. In the CIP NOPR, the Commission noted that, while CIP–002–1 pertains to the identification of assets critical to Bulk-Power System reliability, broader interdependency issues with other infrastructures cannot be ignored.[102] The Commission stated its intention to revisit this matter through future proceedings and in cooperation with other agencies to help to inform the electric sector and itself about the need for future CIP Reliability Standards, especially when the interdependent infrastructures affect generating capabilities, such as through fuel transportation.

ii. Comments

336. APPA/LPPC and other commenters support the Commission's proposed determination that the scope of reliability regulation is properly limited to assets critical to the Bulk-Power System, and does not extend to the management of assets that may be important to the operation of other (even if presumably critical) non-electric assets. MidAmerican comments that the expansion of CIP Reliability Standards beyond Bulk-Power System reliability should be approached with caution and only after the compliance effort is complete for the current CIP Reliability Standards. Luminant agrees with the Commission that issues pertaining to system interdependency are complicated and more appropriately addressed in a separate proceeding after the Commission completes its action approving the current NERC CIP Reliability Standards.

337. By contrast, Applied Control Solutions suggests that interdependencies should be included in risk-based assessments, as they can have direct (e.g., electronic connections between electric entities and major customers) and indirect impacts (e.g., loss of major fuel sources) on Bulk-Power System reliability.

338. Likewise, the Congressional Representatives find fault in the CIP Reliability Standards for failing to address interdependencies with other critical infrastructures. The Congressional Representatives state that the Bulk-Power System is an enormous, interconnected network that is both redundant and resilient, making the sole focus on ''reliability'' and ''operability'' of the grid as a whole inappropriate. They explain that every critical infrastructure in the country is dependent on the Bulk-Power System, including chemical plants, banks, refineries and military installations. Thus, according to the Congressional Representatives, ''focusing on assets relative to the functioning of the grid misses the importance of each individual asset to the functions of our society.'' [103] To address the shortcoming, the Congressional Representatives suggest that every electronically connected asset be considered ''critical.''

339. Related, the Congressional Representatives are critical of NERC's definition of critical assets as ''facilities, systems, and equipment that would affect the reliability and operability'' of the Bulk-Power System. The Congressional Representatives explain that this definition fails to understand the importance of individual elements of the Bulk-Power System that are essential to the delivery of power to the nation's critical infrastructure. They state that generation units serving individual communities, individual substations, telecommunication equipment and distribution assets are critical to the safety and security of the U.S., yet are excluded under CIP–002–1.

iii. Commission Determination

340. The Commission is sensitive to the concerns raised by the Congressional Representatives regarding the severe impact that a cyber attack on assets not critical to the Bulk-Power System could still have on the public. The Commission, however, believes that its authority under section 215 of the FPA does not extend to other infrastructure. Section 215 of the FPA authorizes the Commission to approve Reliability Standards that ''provide for the reliable operation of the bulk-power system,'' which the statute defines as the facilities and control systems necessary for operation of an interconnected electric energy transmission network and the electric energy needed to maintain transmission system reliability. In addition, section 215(a)(1) specifically excludes from the definition of Bulk-Power System ''facilities used in the local distribution of electric energy.'' Moreover, given the complexities surrounding this issue and the aggressive timeline that will be necessary merely to meet the more modest task of developing and implementing cyber security standards capable of protecting the reliability of the Bulk-Power System, we will follow the approach that we described in the CIP NOPR of approving CIP Reliability Standards designed to safeguard the reliability of the Bulk-Power System.

341. Although the Commission will not direct modifications to the scope of critical assets to be identified under CIP–002–1, for the reasons discussed above, the Commission agrees with commenters regarding the importance of considering interdependencies with other critical infrastructures. The Commission believes that to meaningfully address interdependencies with other critical infrastructures, it is important to coordinate with the stakeholders of these other infrastructures as well as with other government agencies and organizations. Thus, we affirm our CIP NOPR approach that ''[w]hile broader interdependency issues cannot be ignored, the Commission intends to revisit this matter through future proceedings and with other agencies. This work will help inform the electric sector and this Commission about the need for future Reliability Standards, especially when the interdependent infrastructures affect generating capabilities, such as through fuel transportation.'' [104]

2. CIP–003–1—Security Management Controls

342. Reliability Standard CIP–003–1 seeks to ensure that each responsible entity has minimum security management controls in place to protect the critical cyber assets identified pursuant to CIP–002–1. To achieve this goal, a responsible entity must develop a cyber security policy that represents management's commitment and ability

[102] CIP NOPR at P 118.

[103] Congressional Representatives comments at 7.

[104] CIP NOPR at P 118.

to secure its critical cyber assets. It also must designate a senior manager to direct the cyber security program and to approve any exception to the policy.

343. CIP–003–1, in addition, requires a responsible entity to implement an information protection program to identify, classify, and protect sensitive information concerning critical cyber assets, as well as an access control program to designate who may have access to such information. Finally, a responsible entity must establish a ''change control and configuration management'' program to oversee changes made to the hardware or software of critical cyber assets.

344. The Commission approves Reliability Standard CIP–003–1 as mandatory and enforceable. In addition, we direct the ERO to develop modifications to this Reliability Standard through its standards development process and to take other actions. These actions pertain to (1) the adequacy of policy guidance; (2) discretion to grant exceptions; (3) leadership; (4) access authorization; (5) change control and configuration management; and (6) interconnected networks.

a. Adequacy of Policy Guidance

345. Requirement R1 of Reliability Standard CIP–003–1 directs a responsible entity to ''document and implement a cyber security policy that represents management's commitment and ability to secure its critical cyber assets.'' The only guidance that is given with regard to the nature and scope of the cyber security policy is that it should address ''the Requirements in CIP–002–1 through CIP–009–1, including the provisions for emergency situations.''

i. NOPR Proposal

346. The Commission proposed in the NOPR that the ERO modify CIP–003–1 to provide additional guidance for the topics and processes that the required cyber security policy should address to ensure that a responsible entity reasonably protects its critical cyber assets.[105] We noted that Recommendation 34 of the Blackout Report called for grid-related organizations to have a planned and documented security strategy, governance model, and architecture for energy management automation systems. The CIP NOPR provided examples of possible topics for security policy guidance, such as communication networks related to control systems; the appropriate use of defense in depth strategy; the use of wireless communications for control systems; uninterruptible power supplies; and heating, ventilation, and air-conditioning (HVAC) equipment for critical cyber assets.

ii. Comments

347. NERC and other commenters contend that the Commission should not direct the ERO to modify CIP–003–1 to provide additional guidance for the topics and processes that the required cyber security policy should address.[106] The Commission should instead permit and encourage the development of ''how'' guidelines and work papers. Ontario Power is concerned that the expectation that security policies will address issues that are not currently reflected in the CIP Reliability Standards implies that an entity could be found non-compliant for not following its own policies that are outside of the Reliability Standards. Ontario Power maintains that this would be an unfounded increase in the scope of the CIP Reliability Standards.

348. ISO/RTO Council opposes the Commission proposal and expresses concern that if a responsible entity's security policies go beyond the specific Requirements of the Reliability Standards, it could be penalized for failure to implement the policies fully. ISO/RTO Council also objects to reporting any steps that exceed what the CIP Reliability Standards require to any third party. It argues that it would be wasteful to require development of one set of plans, policies and standards to meet what is explicitly required by the Reliability Standards and another that is applicable to other assets such as market systems. ISO/RTO Council requests that the Commission clarify that monitoring for non-compliance will pertain to the specific Requirement of the Reliability Standards, not requirements expressed in corporate policies relevant to security.

349. In contrast, SoCal Edison believes that it is appropriate to include guidance in CIP–003–1 on important systems that have not yet been addressed such as data and communications networks, but that guidance on topics such as power supplies, heating, and other equipment is too detailed for a corporate level policy. APPA/LPPC agrees that security policies will address issues that are not currently reflected in the CIP Reliability Standards but that are important for control system security. Further, APPA/LPPC state that the nature and scope of a responsible entity's cyber security management policy generally should be left to the entity's discretion.

350. ReliabilityFirst and SPP comment that an entity's overall organizational security policies should address protection of supporting infrastructure and appropriately define a defense in depth posture. However, they are concerned that, by including such infrastructure in the scope of the CIP Reliability Standards, an audit could determine that the devices supporting the network throughout the entity should be considered either critical cyber assets or electronic security perimeter access points and thus become subject to all of the Requirements of the CIP Reliability Standards. Their concern is the possibility of increasing the scope of the electronic security perimeter to include the entity's entire communications network and all assets connected thereto.

351. Other commenters raise concerns whether specific issues should be addressed in this guidance. Idaho Power disagrees with the Commission's proposal to address the protection of support systems (*e.g.*, communication and HVAC) in the CIP Reliability Standards. It states that other Commission-approved Reliability Standards are better suited for addressing these issues. For example, according to Idaho Power, communication concerns should be addressed in COM–001.

352. Tampa Electric notes that cyber assets associated with communications networks and data communication links between distinct electric security perimeters are exempt under the CIP Reliability Standards. It urges that this exemption be maintained and that further consideration of the exemption's merit should be addressed only in the Reliability Standards development process. Likewise, National Grid and MidAmerican oppose expanding the CIP Reliability Standards to cover communications and data networks beyond those directly involved in the security of control systems.

353. APPA/LPPC agree that it is reasonable for responsible entities to be responsible for the communications systems they own and operate. However, they cannot be expected to oversee the operations of commercial communication carriers. APPA/LPPC state the Commission should recognize that it has no authority to compel commercial communication carriers to comply with the CIP Reliability Standards and that responsible entities cannot compel them to comply.

[105] *See* CIP NOPR at P 123–27.

[106] *E.g.,* Alliant Energy, Mr. Brown, First Energy, Idaho Power, ISO/RTO Council and Ontario Power.

354. ReliabilityFirst and SPP are concerned that environmental systems would become subject, at a minimum, to the requirements of CIP–006–1 (Physical Security). Environmental systems are often not fully enclosed within a physical security perimeter as defined by the Reliability Standard and it is impractical in some instances to do so. ReliabilityFirst states that, besides expanding the scope of the Reliability Standards to encompass issues that either have no bearing on Bulk-Power System reliability, or are specifically excluded from the CIP Reliability Standards, the Commission's proposal improperly deals with ''how'' a responsible entity is to address a Requirement.

iii. Commission Determination

355. The Commission believes that responsible entities would benefit from additional guidance regarding the topics and processes to address in the cyber security policy required pursuant to CIP–003–1. While commenters support the need for guidance, many are concerned about providing such guidance through a modification of the Reliability Standard. We are persuaded by these commenters. Accordingly, the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address. However, we will not dictate the form of such guidance. For example, the ERO could develop a guidance document or white paper that would be referenced in the Reliability Standard. On the other hand, if it is determined in the course of the Reliability Standards development process that specific guidance is important enough to be incorporated directly into a Requirement, this option is not foreclosed. The entities remain responsible, however, to comply with the cyber security policy pursuant to CIP–003–1.

356. In response to ISO/RTO Council, Ontario Power and other commenters, the Commission's intent in the CIP NOPR—as well as the Final Rule—is not to expand the scope of the CIP Reliability Standards. Requirement R1 of CIP–003–1 requires a responsible entity to document and implement a cyber security policy ''that represents management's commitment and ability to secure its Critical Cyber Assets.'' The Requirement then states that the policy, ''at a minimum,'' must address the Requirements in CIP–002–1 through CIP–009–1. The Commission believes that there are other topics, besides those addressed in the Requirements of the CIP Reliability Standards, which are relevant to securing critical cyber assets. The Commission identified examples of such topics in the CIP NOPR. Thus, the Commission, in directing the ERO to develop guidance on additional topics relevant to securing critical cyber assets, is not expanding the scope of the CIP Reliability Standards.

357. Nor do we believe, as suggested by Idaho Power, that the proposed topics for guidance are better addressed by revisions to other Reliability Standards. Again, the guidance is in the context of securing critical cyber assets and is best addressed in the CIP Reliability Standards or a supporting guidance document.

358. In response to SoCal Edison, we disagree that guidance on topics such as power supplies, heating, and other equipment is too detailed for a corporate level policy. These topics are potentially relevant to securing critical cyber assets and, therefore, appropriate topics for guidance.

359. ISO/RTO Council, Ontario Power and other commenters raise concerns regarding potential civil penalty liability if a responsible entity addresses the additional guidance topics in its cyber security policy. The Commission does not believe that the inclusion of additional topics in the cyber security policy will increase a responsible entity's penalty liability. We provide our views regarding the enforcement of cyber security policies below in addressing exceptions to such policies. In particular, we state there that our concern is that a good policy exists and that it is implemented through the exercise of sound reasoning. Consistent with the discussion in the following section, we do not believe that an entity's decision to not follow its cyber security policy in a particular situation should trigger a penalty, as long as no Reliability Standard Requirement (other than Requirement R1 in CIP–003–1) is violated as a result. We do require that the reasoning be documented to ensure that the responsible entity is indeed implementing the security policy as required by Requirement R1 of CIP–003–1.

360. We agree with APPA/LPPC that responsible entities cannot be expected to oversee the operations of commercial communications carriers. However, this is an example of precisely why more guidance would be useful. Since responsible entities cannot oversee commercial communications carriers, it is important that they consider what they can do to guard against potential threats from that quarter.

b. Discretion to Grant Exceptions

361. Requirement R3 of CIP–003–1 provides that a responsible entity must document as an exception each instance where it cannot conform to its security policy developed pursuant to Requirement R1. Exceptions need senior manager approval. The documentation must include ''an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.'' An exception to the cyber security policy must be documented within 30 days of senior management approval. An authorized exception must be reviewed and approved annually to ensure that the exception is still required and valid.

i. NOPR Proposal

362. The Commission expressed concern in the CIP NOPR that Requirement R2 allows a responsible entity too much latitude in excusing itself from compliance with its cyber security policy.[107] The Commission, therefore, proposed to direct the ERO to develop modifications to CIP–003–1 that require a responsible entity to submit documentation of cyber security policy exceptions periodically to the relevant Regional Entity to provide added assurance that exceptions are adequately justified.

363. Further, the Commission distinguished between situations where a responsible entity excepts itself from its cyber security policy and where it excepts itself from specific Requirements of the CIP Reliability Standards based on technical feasibility and stated that exceptions from a policy provision do not also excuse compliance with a Requirement. In that regard, the Commission proposed that the ERO develop modifications to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP–003–1 do not except responsible entities from the Requirements of the CIP Reliability Standards.

ii. Comments

364. While NERC and ReliabilityFirst do not comment specifically on Regional Entity review of exceptions to a responsible entity's cyber security policy, their general comment is that the Commission should rely on NERC's existing oversight structure is applicable here.

365. EEI and other commenters oppose requiring responsible entities to submit documentation of exceptions to the cyber security policy to Regional Entities. EEI disagrees with the Commission's assertion that CIP–003–1

[107] *See* CIP NOPR at P 128–33.

gives a responsible entity too much latitude to excuse itself from compliance with its cyber security policy. EEI adds that it is sufficient that exceptions to a cyber security policy must be explained in writing and approved by a designated manager. According to EEI, external accountability for such decisions is a function of the audit process, and the Commission should not suggest that the Regional Entity step outside its role of enforcing the Reliability Standards and engage in enforcing a responsible entity's internal cyber security policy. PG&E submits that the proposal is burdensome.

366. Entergy disagrees that responsible entities should be required to submit documentation of exceptions periodically to their Regional Entity. Entergy believes that a proper security policy will track what the Reliability Standards require. The Commission, the ERO, and Regional Entities should not be concerned with policy exceptions but rather only with whether the Requirements of the CIP Reliability Standards are being met. Entergy also argues that requiring documentation of exceptions could cause internal policies to be written less rigorously to avoid the burden of excessive documentation.

367. CEA and Manitoba Hydro are concerned that periodic submission of documents on cyber security policy exceptions to Regional Entities may allow the release of highly sensitive information. Manitoba Hydro states that such documentation would contain details about existing critical cyber assets and their security weaknesses that would threaten both security and reliability if it were released inadvertently into the wrong hands. SoCal Edison suggests that it is more appropriate for responsible entities to house all justifications for policy exceptions internally and have them reviewed during an audit. Bonneville is concerned that the practice could be deemed a waiver of FOIA protections. Bonneville also is concerned that external reviewers may be required first to obtain required federal security clearances before accessing the information.

368. MidAmerican believes that the reporting of exceptions will indicate a weak spot in a responsible entity's cyber security policy and a secure method of handling these exceptions would need to be established.

369. Several commenters address the Commission's proposal to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP–003–1 do not except responsible entities from the Requirements of the CIP Reliability Standards. EEI opposes the Commission's proposal for the same reasons described above. MidAmerican comments that it has not interpreted Requirements R2.3 and R3 as the ability to avoid compliance.

370. Related, SPP states that a responsible entity cannot exempt itself from a Requirement of a CIP Reliability Standard. Once a policy is in place to comply with these Requirements, the only recourse in cases of technical infeasibility or other valid reason is to document an exception to the security policy. SPP maintains that the Commission's proposal for reporting and approval of technical feasibility exceptions would, if adopted, extend to exceptions to the required security policy if the exception would make the responsible entity incapable of complying fully with a Requirement of the CIP Reliability Standards.

371. Northern Indiana requests clarification of the information that would be required to justify an exception and suggests that it match the level of information required in self-certifications. It suggests that a responsible entity would benefit from consultation when attempting to justify an exception and that monetary penalties should be waived during this time as well as within the timeframe of any remediation plan. Northern Indiana also contends that security policy exceptions which do not affect compliance with the Reliability Standards need not be documented. Some policies may be stricter than the Reliability Standards, and responsible entities should not be required to submit documentation of exceptions that are consistent with the Reliability Standards Requirements.

iii. Commission Determination

372. The Commission continues to believe that it is important that there be ERO and Regional Entity oversight of exceptions from required security policies, however, the Commission agrees with commenters such as EEI and PG&E that this oversight is best accomplished through the existing Regional Entity oversight and audit process.

373. Requirement R1 of CIP–003–1 requires the development and implementation of a security policy. Requirement R3 provides that a responsible entity must document exceptions to its policy with documentation and senior management approval. The Commission is concerned that, if exceptions mount, there would come a point where the exceptions rather than the rule prevail. In such a situation, it is questionable whether the responsible entity is actually implementing a security policy. We therefore believe that the Regional Entities should perform an oversight role in providing accountability of a responsible entity that excepts itself from compliance with the provisions of its cyber security policy. Further, we believe that such oversight would impose a limited additional burden on a responsible entity because Requirement R3 currently requires documentation of exceptions.

374. That being said, the Commission agrees with EEI and others that Regional Entity review of exceptions to a responsible entity's cyber security policy is best accomplished pursuant to the existing Regional Entity audit process where all the relevant facts and circumstances can be considered. Further, review of exceptions to a cyber security policy in the audit process should effectively address commenter concerns regarding disclosure of sensitive information by keeping that data on site.[108]

375. As we discuss elsewhere in the Final Rule, we agree with Bonneville regarding the need to preserve a governmental entity's FOIA protections and address security clearance concerns. The ERO should address these concerns through consultation with relevant governmental entities.

376. Further, the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP–003–1 do not except responsible entities from the Requirements of the CIP Reliability Standards. In response to EEI, we believe that this clarification is needed because, for example, it is important that a responsible entity understand that exceptions that

[108] In the Final Rule, the Commission has directed the ERO to develop somewhat different external review processes in different contexts. As discussed immediately above, the Commission believes that exceptions to a responsible entity's cyber security policy are appropriately addressed in the course of the Regional Entity's audit process. The Commission has also directed that Regional Entities evaluate and approve a responsible entity's reliance on the technical feasibility exception as part of the audit process. In addition, to provide the Regional Entity with an ''upfront'' understanding regarding the extent of industry reliance on the technical feasibility exception, as well as to allow the Regional Entity to adequately prepare for an audit, the Commission also required that a responsible entity submit a ''notice'' to the Regional Entity when the exception is invoked. In contrast, due to the importance of timely verifying that responsible entities have developed accurate cyber asset lists pursuant to CIP–002–1, the Commission has directed the development of an external review separate from the audit process. Thus, the Commission has tailored different review processes to different situations to minimize the burden on industry yet satisfy the goal of assuring adequate oversight.

individually may be acceptable must not lead cumulatively to results that undermine compliance with the Requirements themselves.

377. The Requirement to develop and implement a security policy differs from many other Requirements in that it is a means to the end of implementing those Requirements. Our concern that exceptions be documented and justified is primarily a concern that there be reasoned decision-making, consistency, and subsequent effectiveness in implementing the policy. We thus disagree with Northern Indiana that security policy exceptions which do not affect compliance with the Reliability Standards need not be documented. Further, in response to Entergy, as stated elsewhere in this Final Rule, our concern is that a good policy exists and that it is implemented through the exercise of sound reasoning. We do not believe that an entity's decision to not follow its cyber security policy in a particular situation should trigger a penalty, as long as no Reliability Standard Requirement (other than Requirement R1 in CIP–003–1) is violated as a result. We do require that the reasoning be documented to ensure that the responsible entity is indeed implementing the security policy as required by Requirement R1 of CIP–003–1.

378. In response to Northern Indiana's request for clarification of the information that would be required to justify an exception, we leave it to the ERO to provide guidance on the level of information that it considers appropriate, consistent with our discussion above.

c. Leadership

i. NOPR Proposal

379. Requirement R2 of CIP–003–1 requires that a senior manager be assigned overall responsibility for implementation of the CIP Reliability Standards. In the CIP NOPR, the Commission interpreted this Requirement to require the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards.[109] The Commission noted that Recommendation 43 of the Blackout Report called for clear lines of authority and ownership for security matters, and it proposed to direct that the ERO modify CIP–003–1 to make clear the senior manager's ultimate responsibility.

[109] *See* CIP NOPR at P 134–36.

ii. Comments

380. Bonneville states that the Commission should clarify whether its intent is to make the senior manager personally accountable for violations of the CIP Reliability Standards, i.e., subject to civil penalties for violations, so that necessary action can be taken to protect the manager, such as acquiring additional personal insurance coverage. Similarly, NRECA asks the Commission to confirm that the senior manager responsible for CIP Reliability Standards compliance is not, by virtue of his position, subject to civil penalties pursuant to section 215 of FPA.

iii. Commission Determination

381. The Commission adopts its CIP NOPR interpretation that Requirement R2 of CIP–003–1 requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards. The Commission's intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The Commission agrees with commenters that the senior manager, by virtue of his or her position, is not a user, owner or operator of the Bulk-Power System that is personally subject to civil penalties pursuant to section 215 of FPA.

d. Information Access Authorization

382. Requirement R5 of CIP–003–1 directs the responsible entity to implement a program for managing access to protected critical cyber asset information and requires, among other things, that the list of personnel responsible for authorizing access to protected information be verified at least annually.

i. NOPR Proposal

383. The Commission explained in the CIP NOPR that CIP–007–1, Requirement R5 (access implementation), CIP–004–1, Requirement R4 (access revocation), and CIP–003–1, Requirement R5 (access review and approval) each contain provisions on access to information, and it took the position that these various provisions are not interlinked as clearly as they should be. The Commission noted that Recommendation 44 of the Blackout Report stresses the need to prevent inappropriate disclosure of information. Thus, the CIP NOPR proposed to direct that the ERO modify Reliability Standards CIP–003–1, CIP–004–1, and/or CIP–007–1, to ensure that when access to protected information is revoked, it is done so promptly.

ii. Comments

384. CPUC agrees with the Commission's proposal on clarifying that a revocation of access to protected information should be accomplished promptly, but it maintains that that the term ''promptly'' is too subjective. It would be more appropriate to specify a definite time interval for revoking access. FirstEnergy agrees with the Commission's proposal and states that in all cases of access authorization under the CIP Reliability Standards, responsible entities should revoke an employee's access to critical cyber assets within 24 hours in cases of termination for cause and within seven days for other personnel no longer needing such access. MidAmerican takes a similar position.

385. Northern Indiana states that while a responsible entity may remove an employee's or vendor's access to its critical cyber assets and systems, it cannot eliminate all possible access to information. A responsible entity cannot enter the employee's home to remove or destroy information that the employee, particularly the vendor's employee, may have maintained in his home because in the course of his employment he wanted ready reference to such information. A responsible entity may make a reasonable request that information be returned, but immediate return may not occur.

iii. Commission Determination

386. The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP–003–1, CIP–004–1, and/or CIP–007–1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly. In general, the Commission agrees with commenters and believes that access to protected information should cease as soon as possible but not later than 24 hours from the time of termination for cause.

387. In response to Northern Indiana, while we acknowledge that responsible entities are not authorized to enter private homes, we believe that an appropriate cyber security policy will ensure that such information is present in an employee's home only for legitimate reasons specified in the policy and should require the return of all information upon request.

e. Change Control and Configuration Management

388. Requirement R6 of CIP–003–1 requires a responsible entity to establish a process of ''change control and configuration management'' for adding,

modifying, replacing, or removing critical cyber asset hardware or software.

i. NOPR Proposal

389. The Commission noted in the CIP NOPR that Requirement R6 does not address accidental consequences or malicious actions by individuals where commercial vendors test and certify that the electronic security patches they provide will not adversely affect other electronic systems already in place.[110] The Commission proposed to direct that the ERO develop a modification to Requirement R6 to require that authorized changes made to critical cyber assets only affect the processes they are intended to affect (to address both accidental consequences and malicious actions by individuals performing the changes). Also, the CIP NOPR proposed that the ERO develop a new requirement for responsible entities to take actions to detect unauthorized changes to critical cyber assets, whether originating from inside or outside the responsible entity.

ii. Comments

390. Entergy, ISO/RTO Council, Northern Indiana and PG&E oppose the Commission's proposed modifications to Requirement R6 of CIP–003–1. Entergy argues that the Commission's concern will be addressed by CIP–007–1 when implemented by information security professionals and changes to CIP–003–1 are unnecessary and burdensome. Entergy and BPA also believe that the NIST Security Risk Management Framework offers further comprehensive controls. Northern Indiana points out that assets and systems targeted by the proposal include software as well as hardware.

391. MidAmerican believes that Requirement R6 is sufficient as written and clearly outlines the process of review, testing and approval, and is adequate for monitoring of change control and configuration management. Idaho Power is concerned about the current availability of technology to assist in detecting accidental and malicious modifications. It asks whether the Commission is concerned with unauthorized changes, unintended changes or both. Idaho Power opposes additional changes and states that it can reduce the risk of unauthorized changes significantly, but it cannot eliminate them entirely. Idaho Power believes that there will be adequate protection against unintended changes where there are appropriate test plans, trained and qualified personnel, and a regimented change management process.

392. ISO/RTO Council states that it does not understand what the Commission meant by ''detection and monitoring controls'' and suggests that it consider the phrase ''verification that unintended changes have not been made.'' ISO/RTO Council objects to testing the functionality of changes made to live production systems. It agrees that verification of manually initiated changes is appropriate, and responsible entities should also be required to monitor and determine whether unintended changes have been made to devices in the production environment and to investigate and remediate any unintended changes. According to ISO/RTO Council, it is not always possible to confirm definitively or safely that applying a tested and approved change on a production device has had the intended effect, especially where the modification is rarely triggered or where testing could adversely affect reliability. ISO/RTO Council prefers a requirement to verify that changes have been made on the intended devices, to monitor for unintended or unplanned changes, and to investigate and remediate any exceptions that are discovered.

393. Further, ISO/RTO Council states some changes are intentionally initiated automatically using pre-approved means, such as automated virus signature updates. These changes can be unpredictable and can occur multiple times per day. ISO/RTO Council agrees these changes need to be verified, but states it is impractical and unnecessary to verify each change as it happens and suggests periodic verification that the necessary updates, or their cumulative equivalent, have been effectuated.

394. PG&E argues that technical problems could cause downtime of critical assets if this requirement is imposed. Any requirements for detection and monitoring controls for unintended changes must allow for controls that do not require considerable downtime for the critical cyber assets.

395. Puget Sound argues that the CIP Reliability Standards should expressly recognize that change control and configuration management processes for critical cyber assets cannot ensure 100 percent integrity for those assets when making changes. The CIP Reliability Standards also should recognize that test environments can mimic portions of the production environment but cannot capture all of the actual interactions among critical cyber assets.

396. ReliabilityFirst and SPP state that changes should be properly tested prior to implementation, although it may not always be feasible to test a change in an offline environment. They believe that a strict interpretation of the Commission proposal would be impossible to implement, as it would require a comprehensive regression test, including failure testing, to be performed on the entire environment. Even that might not detect an unintended consequence of the change and could conceivably result in an expectation to report an issue of non-compliance. Regression testing is appropriately reserved for significant changes, such as version upgrades or new applications, but not all changes. They state that appropriate mitigation measures exist for reducing the risk of unintended consequences resulting from changes.

iii. Commission Determination

397. Based upon the comments received the Commission is altering its position on how best to address the apparent deficiencies of Requirement R6 in CIP–003–1. The Commission directs the ERO to develop modifications to Requirement R6 of CIP–003–1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The Commission believes that these considerations are significant aspects of change control and configuration management that deserve express acknowledgement in the Reliability Standard. While we agree with Entergy that the NIST Security Risk Management Framework offers valuable guidance on how to deal with these matters, our concern here is that the potential problems alluded to be explicitly acknowledged. Our proposal does not speak to how these problems should be addressed. We do not believe that the changes will have burdensome consequences, but we also note that addressing any unnecessary burdens can be dealt with in the Reliability Standards development process.

398. We agree with ISO/RTO Council that the phrase ''verification that unintended changes have not been made'' captures the core issue. Our concern is that some form of verification is performed to detect when unauthorized changes have been made and to identify those changes, as well as ensuring that the proper alerts are issued.

399. Many of the comments address practical issues involved in addressing accidental consequences and malicious actions, and we recognize that such issues exist. We, thus, agree with Puget Sound that change control and

[110] *See id.* P 140–44.

configuration management processes for critical cyber assets cannot ensure 100 percent integrity for those assets when making changes. We do not seek absolute assurances but rather are concerned that there be processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. However, we reject Puget Sound's proposal that the Reliability Standard should expressly recognize that absolute assurances are not required. We also believe that our revised directive to the ERO on Requirement R6 addresses Puget Sound's concern about the limitations imposed by a test environment.

400. In response to ReliablityFirst and SPP, we understand that comprehensive regression testing is not necessary for every change regardless of how insignificant. We also agree with ISO/RTO Council that it can be impractical and unnecessary to verify every intentional automatic change as it occurs. We believe that our revised directive to the ERO addresses these concerns.

f. Interconnected Networks

i. NOPR Proposal

401. The Commission proposed in the CIP NOPR to direct the ERO to modify Reliability Standard CIP–003–1 to provide direction on the issues and concerns that a mutual distrust posture must address to protect a control system from the ''outside world.'' [111] The Commission noted that interconnected control system networks are susceptible to infiltration by a cyber intruder and stated that responsible entities should protect themselves from whatever is outside their control systems.

ii. Comments

402. FirstEnergy agrees with the intent of the Commission's proposal that there be more direction on what constitutes a mutual distrust posture, but it argues that the need for uniform processes should be balanced against the need for flexibility in individual cases. FirstEnergy argues that each entity may have a unique architecture that requires a unique protection scheme. In addition, a common security method could cause a vulnerability of its own, in that one successful cyber attack could compromise all security systems if there are similarities across all systems.

403. ISO–NE agrees that the mutual distrust principle is a useful consideration when determining when to protect cyber assets and in designing a secure system architecture, but it disagrees that it should be used as a measurable requirement. ISO–NE thus asks the Commission to omit any direction to the ERO to address the concept of mutual distrust.

404. Northern Indiana comments that the Commission's proposal on mutual distrust is unnecessary because the issue is addressed in Reliability Standards CIP–005–1 and CIP–007–1. It argues that if the Commission's proposal on mutual distrust were applied in unqualified terms, it would have to sever the Midwest ISO's communication link to the Northern Indiana control system. Northern Indiana states that it trusts the Midwest ISO in its role as the reliability coordinator over the Northern Indiana electric system and thus argues that the Commission should exempt reliability coordinators. If the Commission does not exempt reliability coordinators, Northern Indiana respectfully requests that the Commission clarify and refine the definition of the term mutual distrust.

405. Entergy argues that the Commission needs to direct the ERO to define the term mutual distrust in CIP–003–1 to foreclose ambiguities in application and enforcement. Entergy notes that NIST has many documents in its SP800 Series that provide excellent treatment of the issues and variables involved in the concept of mutual distrust and that complement the NIST Security Risk Management Framework. The Commission could direct the ERO to consider this guidance. Entergy argues that the broad wording of the Commission's proposal extends beyond the scope of the Reliability Standards. It also argues that the Commission's proposal would direct the ERO to specify what the end result must be rather than permitting the Reliability Standards process to establish the optimum solution.

406. MidAmerican submits that the terms mutual distrust and outside world require clarification to facilitate compliance. MidAmerican recommends that the Commission ensure that the guidelines to be developed have no impact on either performance or reliability. EMS/SCADA systems are tuned for and certified by their vendor at specific communication rates. The introduction of delays due to additional security layers to communications and data exchange may impact reliability.

iii. Commission Determination

407. The Commission proposed in the CIP NOPR that the ERO provide direction, i.e., 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. The Commission noted that 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.

408. The Commission agrees with FirstEnergy on the importance of flexibility in developing a mutual distrust posture, but does not see a conflict between the need for flexibility and what it is proposing, which is simply more guidance. More guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and effectively. Additional guidance need not be included in a specific Requirement, but could be in the form of examples. We will leave it to the Reliability Standards development process and the ERO to decide whether some or all of the guidance can be contained in separate guidance documents referenced in the Reliability Standard. In response to Entergy, the Commission is not directing that the ERO establish a specific end result. Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by-case basis. We disagree that providing useful guidance affects the scope of the Reliability Standards.

409. We agree with Entergy that NIST provides much guidance, but we disagree that it is necessary to define the term mutual distrust. Our proposal is that there be guidance on certain issues and concerns, and we therefore do not believe that a formal definition advances that goal. In response to MidAmerican, we believe that clarification of the terms mutual distrust and outside world, as well as ensuring that any guidelines developed do not harm performance or reliability, are matters that the ERO should consider in the Reliability Standards development process.

410. We disagree with Northern Indiana that Reliability Standards CIP–005–1 and CIP–007–1 address the matters of concern to us. Northern Indiana does not explain how these Reliability Standards provide guidance of the type we have described. We also

[111] *Id.* at P 147. An architecture with a mutual distrust posture could involve various hardware or software mechanisms or manual procedures to restrict and verify access to the control system from these outside sources. Examples include: firewalls; data checking software(s); or procedures for manually implementing a connection to allow a vendor to perform maintenance work.

disagree that the mutual distrust principle would require responsible entities to sever their communication links with their ISO or RTO or reliability coordinator. The principle could play a role in determining what precautions would need to be taken to protect those communications, but we do not see why it would lead to the specific result that Northern Indiana identifies. Mutual distrust does not imply refusal to communicate; it means the exercise of appropriate skepticism when communicating. The Commission believes additional guidance on what this means specifically in current practice would help responsible entities to avoid these misunderstandings.

411. We disagree with ISO-NE that guidance on mutual distrust is unnecessary because responsible entities either are compliant or they are not, mutual distrust not withstanding. We do not see how responsible entities can fully understand the compliance issues they face without some understanding of how mutual distrust is applied in a modern security environment. Mutual distrust helps explain where an entity's responsibilities begin and end and what assumptions it can make about factors outside its control when it performs its risk-based assessment.

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.

3. CIP–004–1—Personnel and Training

413. Standard CIP–004–1 requires that personnel having authorized cyber access or unescorted physical access to critical cyber assets must have an appropriate level of personnel risk assessment, training and security awareness. Responsible entities must develop and implement a security awareness program that addresses concerns related to cyber security; a cyber security training program for affected personnel that addresses policies, access controls, procedures for the proper use of critical cyber assets, physical and electronic access to critical cyber assets, proper handling of asset information, and recovery methods after a cyber security incident; and a personnel risk assessment program for all personnel having access to critical cyber assets.

414. As discussed further below, the Commission approves Standard CIP–004–1 as mandatory and enforceable. In addition, we direct the ERO to develop modifications to this CIP Reliability Standard. The Commission also requires the ERO to clarify and provide guidance on other matters. The required modifications are discussed below in the following topic areas of concern regarding CIP–004–1: (1) Training; (2) personnel risk assessments; (3) cyber and physical access; and (4) jointly owned facilities.

a. Training

415. The requirements for ongoing awareness reinforcement in sound security practices specified in Requirement R1 and for training specified in Requirement R2 apply to all personnel, contractors, and service vendors who have authorized cyber access or unescorted physical access to critical cyber assets. Requirement R2.1 allows such personnel to have access to critical cyber assets for up to 90 days prior to receiving any cyber security training.

i. NOPR Proposal

416. In the CIP NOPR,[112] the Commission stated that training is integral to the protection of critical cyber assets, and that allowing personnel access to critical cyber assets prior to receiving training increases the vulnerability of and risk to such assets. The Commission proposed to direct the ERO to modify CIP–004–1 to require affected personnel to receive the required training before obtaining access to critical cyber assets (rather than within 90 days of access authorization), but to limit exceptions to circumstances such as emergencies, subject to documentation and mitigation. To facilitate communications in emergency situations, the Commission proposed to direct the ERO to require responsible entities to identify ''core training'' elements to ensure that essential training elements will not go unheeded in an emergency and in other contingency situations where full training prior to access will not best serve the reliability of the Bulk-Power System. We also proposed that the ERO consider what, if any, modifications to CIP–004–1 should be made to assure that security trainers are adequately trained themselves.

417. In addition, the Commission proposed to direct the ERO to modify CIP–004–1 to clarify that the cyber security training programs required by Requirement R2 are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of the critical cyber assets. The CIP NOPR stated that CIP–004–1 should clearly state that cyber security training concerning a critical cyber asset should encompass the electronic environment in which the asset is situated and the attendant vulnerabilities. To clarify that point, we proposed that the ERO consider adding a provision similar to that in Requirement R1.4 of CIP–005–1, which specifically subjects any non-critical cyber asset within a defined electronic security perimeter to the CIP Reliability Standard.

418. Further, the Commission proposed to direct that the ERO increase the guidance in the CIP Reliability Standard as to the scope and quality of training, including examples of areas where the inclusion of guidance can be considered, as follows: control of electronic devices (such as laptop computers); the appropriate audiences for the training; delivery methods; and updates of training materials. The CIP NOPR stated that the awareness and training programs, addressed separately by Requirements R1 and R2, complement each other and work in tandem. The Commission also stated its expectation that the ERO consider relevant aspects of certain NIST Special Publications, as well as other relevant models, to improve CIP–004–1 and prevent a lowest common denominator result.

ii. Comments

419. Entergy recommends that the Commission modify its direction to the ERO regarding access to critical cyber assets for newly-hired personnel to provide access to critical cyber assets for newly-hired personnel if they are accompanied by qualified escorts. Entergy insists that individuals without training should be allowed to be escorted by a trained individual to access a critical cyber asset and, if similar required training has been received by an unescorted individual at another industry facility, that training should be allowed to be credited at the current facility. SDG&E recommends that new employees be allowed escorted access to critical cyber assets, even in non-emergency situations, since training is not always coincident with a hiring date.

420. Entergy disagrees with the proposal to direct the ERO to require responsible entities to identify core training elements. On the other hand, FirstEnergy and SoCal Edison agree with the Commission's proposal that NERC should require the development of core training elements. They state that additional guidance in this area would be helpful preparation for responsible entities to operate in emergency and other contingency

[112] *See Id.* at P 151–61.

situations. FirstEnergy proposes that CIP–004–1 be revised to further specify what situations should be considered emergency and contingency for the purpose of granting access prior to completion of full training. Northern Indiana agrees with the common sense approach in the CIP NOPR on how responsible entities should be allowed to handle emergency conditions, but would retain the 90-day transition period for conducting training. Northern Indiana requests clarification of what is intended by the term ''core training'' and requests additional guidance in the Final Rule with respect to training.

421. Entergy contends that specific discussion of the many forms of training needed is beyond the current scope of the CIP Reliability Standards. Entergy argues that, if specificity is needed, the Commission should refer to materials issued by other federal agencies, including the Defense Information Systems Agency. Mr. Brown argues that the level of detail the Commission is proposing to be added to the training portion of the CIP Reliability Standards would be more appropriately and efficiently developed through some process other than that of Reliability Standards development process.

422. MidAmerican believes that CIP–004–1, Requirement R2 is adequate as proposed and that specific job-related training requirements are more properly managed by the entity performing or contracting the work. MidAmerican submits that the entity performing the work is best suited to determine the scope and delivery method of job-specific training. MidAmerican believes additional clarification of acceptable awareness and training programs is necessary for compliance purposes, should the Commission's call for increased guidance be adopted.

423. In response to the Commission's proposal that training encompass network and interconnectivity aspects, many commenters suggest that training should be tailored to match up with the trainee's duties, experience, or ''need to know.'' FirstEnergy suggests that CIP–004–1 should include a provision that would direct a responsible entity to establish access categories based on security roles because access categories based on job responsibilities would ensure that the level or frequency of exposure to critical cyber assets will be considered. For example, a systems analyst would need access to certain critical cyber assets on a frequent basis and at a level that allows file manipulation, while a system user would need access to the data output of the systems during working hours and not necessarily file manipulation access. Those with access to critical cyber assets should have training specific to the critical cyber asset and those without such access should have general awareness training.

424. Likewise, National Grid argues that, while a general understanding of networking hardware and software and interconnectivity is important, the focus of the training should be geared toward understanding cyber security policies and each trainee's role in response and recovery plans. National Grid believes that not every employee requires IT training and that training should match an employee's required skill set.

425. FirstEnergy agrees that CIP–004–1 should address training regarding access to the cyber assets themselves and the networking hardware and software linking them, but it also asks the Commission to clarify that only those personnel that have access to both the critical cyber assets and the networking hardware and software should have training on both. FirstEnergy argues that it would be overly burdensome and serve no purpose to do otherwise and, conversely, it serves no purpose to train personnel on the networking hardware and software security methods, if those personnel have access only to the critical cyber asset itself. Training personnel on security measures of equipment for which they have no access can create a potential weakness in the security measures for such equipment.

426. ISO–NE argues that requirements for training relating to networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of the critical cyber assets are a business management decision and should be omitted from the Final Rule. ISO–NE argues that the decision to determine the level of skill training necessary for an individual, based on that employee's functional task requirements and coordinated career goals, is a business decision beyond the scope of security training for access controls, monitoring, and incident response.

427. Similarly, Northern Indiana contends that CIP–004–1 should not specify who should be trained, what the training should include, or how frequently training should occur. Northern Indiana argues that the responsible entity must be given flexibility to differentiate between those aspects of networked systems potentially affecting critical control systems and those that should be included in critical cyber asset training. Northern Indiana argues that the focus should be on the applications, policies and procedures that relate to the critical control systems and other critical cyber assets.

428. ISO/RTO Council and ISO–NE argue that training that addresses vulnerabilities is not appropriate for all individuals with access to critical cyber assets and, therefore, they disagree with the statement in the CIP NOPR that ''CIP–004–1 should leave no doubt that cyber security training concerning a critical cyber asset should encompass the electronic environment in which the asset is situated and the attendant vulnerabilities.'' Information about vulnerabilities associated with critical cyber assets and/or their security perimeters is highly sensitive. Such information should be known only to those with direct responsibility to administer the secure operation of the critical cyber assets and their security perimeters.

429. ReliabilityFirst is concerned that the ERO not lose sight of the fact that Requirement R2.2 requires specific training ''appropriate to personnel roles and responsibilities'' as it develops the additional guidance proposed by the Commission. ReliabilityFirst argues that it is inappropriate, for example, to train an operator in the dispatch operations center on firewalls and networking devices. Training for personnel with electronic or unescorted physical access to systems within the electronic security perimeter should be appropriate to the trainee's scope of access. The goal of the training is not to make operational personnel into network specialists, but to train them on the policies and procedures implemented by the responsible entity to protect their critical cyber assets.

430. In response to the Commission's question regarding what, if any, modifications to CIP–004–1 should be made to address the concern that security trainers be adequately trained themselves, SoCal Edison believes that the Commission should require the ERO to have a program to have qualified trainers in order to determine the adequacy of training. To ensure quality and consistency, this implies that all trainers would have to be qualified by the ERO prior to training. Any vendor training tools (*e.g.*, online training courses) would similarly need to be approved by the ERO.

iii. Commission Determination

431. The Commission adopts the CIP NOPR's proposal and directs the ERO to develop a modification to CIP–004–1 that would require affected personnel to receive required training before obtaining access to critical cyber assets (rather than within 90 days of access

authorization), but allowing limited exceptions, such as during emergencies, subject to documentation and mitigation.

432. The Commission notes that commenters did not provide specific reasons why employees should be granted access prior to training, but focused on the nature and scope of our proposed exceptions. Entergy and SDG&E recommend that newly-hired employees be allowed access to critical cyber assets if they are accompanied by qualified escorts. We note that a qualified escort would have to possess enough expertise regarding the critical cyber asset to ensure that the actions of the newly-hired employee or vendor did not harm the integrity of the critical cyber asset or the reliability of the Bulk-Power System. However, if the escort is sufficiently qualified, we believe such escorted access could be permitted before a newly-hired employee is trained.

433. Based on the concerns of commenters, the Commission modifies its CIP NOPR proposal that the ERO identify core training elements to ensure that essential training elements will not go unheeded in emergencies and in other compelling situations. While the Commission continues to believe that the identification of core training elements is useful, this issue would benefit from further vetting within the Reliability Standards development process. Thus, we direct the ERO to consider, in developing modifications to CIP–004–1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard. If the Reliability Standard development process determines not to identify core requirements, the ERO should provide an explanation of this decision. In reply to commenters, we clarify that by using the term core training our concern is for a responsible entity to pre-plan what information and training is necessary for personnel temporarily called in to help in an emergency—not that the actual scope of such training needs to be articulated in the Reliability Standard and applicable to all responsible entities in all circumstances. It is important that responsible entities have plans for introducing the personnel called in to assist in such situations. We expect that core training would be different for different responsible entities.

434. The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP–004–1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets. CIP–004–1 should leave no doubt that cyber security training concerning a critical cyber asset should encompass the electronic environment in which the asset is situated and the attendant vulnerabilities. We note that, according to Requirement R1.4 of CIP–005–1, all cyber assets within an electronic security perimeter are to be protected, not just the critical cyber assets. In reply to commenters, we clarify that our proposal discussion on this topic was not intended to suggest that personnel have training that is not appropriate for an employee's duties, functions, experience, or access level. We agree with commenters that information concerning vulnerabilities should be revealed on a need to know basis and not universally. However, any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions or inactions could, even inadvertently, affect cyber security.

435. Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP–004–1 should be made to assure that security trainers are adequately trained themselves. Commenters provided minimal input on this proposal and, consistent with the CIP NOPR, we believe that whether a modification is appropriate to address this issue is better determined in the first instance through the ERO's Reliability Standards development process. The ERO should consider the comments of SoCal Edison with regard to what role and steps should be taken by the ERO to ensure quality and consistency of trainers.

b. Personnel Risk Assessment

436. Requirement R3 of CIP–004–1 requires each responsible entity to have a documented personnel risk assessment program. It also requires that a personnel risk assessment, including a criminal background check, be conducted within 30 days after a person receives cyber access or unescorted physical access to critical cyber assets. The wording of Requirement R3 would allow access to critical cyber assets while an investigation is still underway, and even before an investigation has started.

i. NOPR Proposal

437. In the CIP NOPR, the Commission stated that allowing applicable personnel, including vendors, to access critical cyber assets prior to the completion of their personnel risk assessment increases the vulnerability of, and risk to, these assets.[113] We also observed that Recommendation 41 of the Blackout Report emphasizes the need for guidance on implementing background checks.[114] At the same time, the Commission indicated that commenters had raised a valid concern regarding the disruptions that would result if current employees and vendors with established involvement were denied access to critical cyber assets for a 30-day period. Accordingly, the Commission proposed to direct the ERO to develop modifications to Requirement R2 to provide that newly-hired personnel and vendors should not have access to critical cyber assets, except in specified circumstances, such as an emergency. To avoid transition disruptions, the Commission proposed that the 30-day window allowing access before completion of the personnel risk assessment remain in effect for current employees and vendors with existing contractual relationships with the responsible entity as of the effective date of the Reliability Standard. The Commission proposed that the ERO include, in developing modifications to CIP–004–1, criteria that address circumstances in which current personnel can continue access to critical cyber assets during the 30-day investigative period during initial compliance with CIP–004–1.

ii. Comments

438. California Commission and MidAmerican support the Commission's proposal to require that a personnel risk assessment be performed before access is granted except in emergency situations for the reasons articulated in the CIP NOPR. California Commission stresses that the personal risk assessment must be conducted before a person obtains access to critical cyber assets, because, if access is granted before a person clears a risk assessment, Requirement R3 is rendered useless. California Commission states that the point is to keep unwanted persons away from critical cyber assets, not to grant them access for a brief period of time and then bar them from access if they do not pass the risk assessment.

439. ReliabilityFirst and SPP do not believe that the CIP Reliability

[113] *See id.* P 162–66.

[114] *See* Blackout Report at 167–68, Recommendation 41 (recommending that NERC provide guidance on background checks to be completed on contractor and sub-contractor employees in advance of allowing access to secure facilities).

Standards should attempt to define an all encompassing set of emergency contingencies for which unescorted access could be granted in the absence of a background check, because there is a risk that a valid emergency exists for which the guidance is unsuited. They suggest that a more appropriate way to handle the emergency access is to allow a short-term exception to the security policy, appropriately justified and approved as any other exception to the policies implementing the provisions of the CIP Reliability Standards.

440. FirstEnergy agrees with the Commission that newly hired employees or vendors with no previous relationship to the responsible entity should not have access to critical equipment while undergoing the personnel risk assessment. The 30-day window may be appropriate for employees and vendors with which the responsible entity has had a working relationship, such as employees transferring to another position or contractors that are returning from a reassignment. In contrast, SoCal Edison maintains that 30 days is not adequate time to update personnel risk assessments during initial implementation on all current personnel that would require an updated personnel risk assessment. It believes that the 30 days would be adequate if such a timeframe begins when personnel risk assessment certification paperwork is provided for each individual.

441. APPA/LPPC note that they do not object to the requirement in CIP–004–1 R3.1 that ''[t]he responsible entity shall ensure that each assessment conducted include, at least, [a] seven-year criminal check'' on employees with access to critical cyber assets. However, they seek clarification that responsible entities have discretion in reviewing the results of criminal background checks to determine, on a case-by-case basis, whether any crime identified in the background check would disqualify an individual from obtaining access to critical cyber assets.

442. SDG&E comments that Requirement R3 may require refinement on various issues regarding the personnel risk assessment requirements, including whether state and local law should be pre-empted to permit industry-wide protocols for periodic background and criminal checks on existing employees. SDG&E asks the Commission to clarify that an entity may comply with Requirement R3 by using its existing pre-employment background check procedures for current employees, at seven year intervals, provided that such procedures encompass the required social security verification and criminal background checks. SDG&E argues that, otherwise, applicable state and local laws could prohibit an entity from conducting such periodic checks.

iii. Commission Determination

443. The Commission adopts with modifications the proposal to direct the ERO to modify Requirement R3 of CIP–004–1 to provide that newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency. We also direct the ERO to identify the parameters of such exceptional circumstances through the Reliability Standards development process. FirstEnergy and California Commission agree with the Commission's proposals.

444. ReliabilityFirst and SPP believe that it would be appropriate to handle emergency access via a short-term exception to the security policy. We note that such access would not be only an exception to the security policy, but an exception to a CIP Reliability Standard Requirement. Therefore, such exceptions would have to comply with the conditions of a technical feasibility exception that we have specified elsewhere in this Final Rule. The Commission believes that a workable solution is for the Reliability Standards development process to identify emergency circumstances that would warrant allowing access to critical cyber assets. However, if a responsible entity experienced a situation outside of those circumstances that it believed warranted access to critical cyber assets, the responsible entity could treat the situation as a technical feasibility exception and follow the conditions set out by the Commission. With this approach, we believe that in most cases it will be unnecessary to go through the administrative burden of a technical feasibility exception.

445. SoCal Edison expresses concern that the 30 days allowed in CIP–004–1 for completion of the personnel risk assessment may not be enough time to process all existing employees with access. We note that there is no reason why such assessments cannot be completed well before responsible entities are to be auditably compliant with this provision. The ERO should consider SoCal Edison's issue in the Reliability Standards development process.

446. APPA/LPPC seek clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees. SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees. The ERO should consider these issues when developing modifications to CIP–004–1 pursuant to the Reliability Standards development process.

c. Cyber and Physical Access

447. Requirement R4 of CIP–004–1 directs the responsible entity to maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to critical cyber assets. The lists do not serve to deny personnel access from critical cyber assets prior to completion of a personnel risk assessment, although Requirement R4.2 requires that both cyber and physical access to critical cyber assets be revoked within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access.

i. NOPR Proposal

448. The Commission stated in the CIP NOPR that timely system updates to access rights are important because access to critical cyber assets by employees, contractors, or vendors represents a gap in security when such access is no longer needed. We proposed to direct the ERO to develop modifications to CIP–004–1 to require immediate revocation of access privileges when an employee, contractor, or vendor no longer performs a function that requires authorized physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement or termination). Further, we proposed to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list.[115]

ii. Comments

449. Numerous commenters responded to the CIP NOPR proposal to require immediate revocation of access to critical cyber assets when an employee, contractor or vendor no longer performs a function that required authorized physical or electronic access to a critical cyber asset for any reason. California Commission agrees with the requirements of CIP–004–1, and states that access controls should be updated upon termination or transfer of

[115] *See* CIP NOPR at P 167–69.

personnel. However, as with its recommendation regarding CIP–003–1, California Commission suggests that CIP–004–1 should provide a specific time limit for revoking access, rather than requiring access to be revoked promptly.

450. MidAmerican supports the proposal, but believes that the timelines provided in Requirement R4.2 are clearly defined and appropriate for the risk associated with removal of access. ReliabilityFirst and SPP agree with the Commission that access should be revoked as quickly as possible upon termination or reassignment, but believe the use of the term ''immediate'' is subjective and could lead to conflicting interpretations. According to ReliabilityFirst, one entity might interpret the requirement as allowing a reasonable amount of time, perhaps an hour, to revoke access once the termination or reassignment has occurred and notifications made, while another entity might interpret it as needing to terminate access prior to the moment of termination or reassignment, perhaps coincident with the employee being notified of his or her termination.

451. SoCal Edison and Entergy believe that it will be difficult to comply with the immediate revocation of access requirement. For example, SoCal Edison states that meeting the proposed change would be dependent upon direct communication from a manager initiating the termination actions, and SoCal Edison believes it is appropriate to allow 24 hours to revoke access privileges. FirstEnergy similarly argues that an organization will not be aware in advance of personnel that are transferred in short order to address an immediate need or personnel that are dismissed or fired on the spot for misconduct. Entergy asserts that the systems and equipment currently in use across the industry simply cannot operate in the type of networked computing environment necessary to revoke all access immediately. For example, a responsible entity may have a magnetic strip physical access control at a substation perimeter, but if the controller is not networked back to a central access control system, meeting the immediacy requirement would not be possible. The industry will need time and adequate grounds to justify modernization of capabilities for rate relief in order to implement such a proposal.

452. First Energy and Idaho Power suggest that the Commission should soften its position on immediate revocation and propose that the Commission require access to critical cyber assets to be revoked as soon as practicable. They suggest allowing either 24 hours or one business day for revocations. Ontario Power notes that some activities can be performed quickly, but others will take time.

453. ReliabilityFirst argues that, from a risk perspective, it is more time-critical to terminate access when an employee is involuntarily terminated or reassigned due to disciplinary action. ReliabilityFirst argues that an employee who voluntarily terminates or changes positions normally does so on good terms with the employer. In addition, both ReliabilityFirst and SPP maintain that, while an entity should be cognizant of planned terminations and reassignments within the company, the entity has no such insight into a vendor or contractor. The entity must rely upon a timely notification from the vendor or contractor, especially when the services are provided remotely as opposed to on-site. In addition, ReliabilityFirst reasons that primary access needs to be terminated as quickly as possible, with secondary access not as time-critical. Primary access would include the physical access, VPN access, and domain account, and terminating that access will effectively quarantine the terminated employee while remaining access is disabled. ReliabilityFirst and SPP recommend that, in lieu of the term ''immediate,'' a reasonable and measurable time frame already exists and has been defined within the CIP Reliability Standard itself.

454. Similarly, ISO–NE argues that personnel transfers can at times require a protracted, transitional process, where there is good business reason for the individual to retain access privileges after the formal transfer date. Most often this would be where continued back-up support is appropriate while the individual's replacement is being identified, or a personal risk assessment is conducted, and/or is trained and becomes familiar with new job responsibilities.

455. ISO–NE and Northern Indiana oppose requiring revocation of access when an employee is facing disciplinary action. ISO–NE argues that not all disciplinary action should arbitrarily warrant revocation of access privileges. Northern Indiana argues that, notwithstanding the disciplinary action, such an employee might still be responsible for performing tasks that require access. Northern Indiana argues that Requirement R4.2 should be left intact and the timeline for revocation should remain 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require access to critical control systems and other critical cyber assets. ISO–NE requests management discretionary power in determining when revocation is warranted.

456. Various commenters raise concerns about the timelines associated with the Commission's proposal to deny unescorted physical access to individuals not identified on the authorization list. For example, Northern Indiana is concerned that absolute compliance with this requirement would be very difficult to achieve and record within the time specified.

457. EEI objects to the immediate revocation of access privileges proposal if the Commission is proposing to require responsible entities to perform immediate updating of their authorization lists. EEI argues that these changes are not needed, because, at the time any individual is terminated for any reason, the manager collects items such as badges, keys, tokens used for electronic entrance and other methods of access, thus denying the individual access to facilities where critical cyber assets are kept. Access control systems are updated using an efficient overnight batch process. EEI asserts that converting to immediate updates for all situations (including low-risk situations such as individuals transferring or retiring) would require significant expense with minimal improvement in security.

458. Duke and others [116] argue that some flexibility in the promptness of access revocation is warranted, but raise many of the same points as EEI. Duke concedes that immediate updates of access authorization control systems can be performed outside of a batch process, but argues that this would involve additional cost and should be reserved for situations involving a tangible threat, such as when an employee is being terminated for cause.

459. PG&E argues that CIP–004–1 already provides sufficient controls and need not be revised. PG&E argues that CIP–004–1 ensures that individuals who are terminated or who no longer require such access lose their access in a timely manner, but argues that there should be no requirement for immediate updating of authorization lists. In this regard, PG&E argues that, although having the means to identify individuals with valid access rights is important, if the individual has been disabled from access to relevant systems and physical areas, a slight delay in updating the list would not significantly compromise security and thus there is no need to require the impractical task of

[116] *See also* PG&E and Tampa Electric.

immediately updating authorization lists.

iii. Commission Determination

460. The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP–004–1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).

461. As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate. As noted in the CIP NOPR, most organizations will know in advance the timing of personnel actions and can arrange ahead of time for access revocation to be concurrent with any disciplinary action, transfer, retirement or termination. Revocation of access is usually a matter of assuring that a particular employee's credentials no longer permit physical or electronic access. We understand that outlying elements may require some brief lag before denial of access is effective, in which case, the circumstances justifying such lag must be documented for audit purposes.

462. FirstEnergy comments that the term ''immediate'' should be clarified and be interpreted as ''as soon as possible'' but not later than 24 hours to take care of on-the-spot dismissals. Others also comment about various circumstances where advance or coincident preparations for revocation to access cannot be made. We continue to believe that most dismissals can be anticipated in advance and believe that revocation should be immediate upon the employee's notification of any personnel action requiring revocation of access. However, the ERO may define what circumstances justify an exception that is other than immediate and determine what is the fastest revocation possible.

463. We acknowledge that not all disciplinary actions warrant revocation of access privileges. In addition, certain personnel transfers can require a protracted transitional process that warrants retention of access privileges after the formal transfer date. There may be operational reasons that justify retention of access privileges after an employee transfers, but the default procedure should be to cancel access privileges at transfer and to document any exceptions to that policy for audit purposes.

464. We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification. Our concern, in calling for this adjustment, is that the current language in the CIP Reliability Standard does not describe the purpose of the required list of personnel with authorized access; rather, it merely states that such a list must be made, reviewed, and updated. Similar to our expectations expressed earlier regarding implementation of required plans and policies, we believe that the expectation that access not be granted to personnel not on the authorized list should be made clear in the Reliability Standard.[117] However, while a responsible entity should not allow access to any personnel not included on the list, the Commission believes commenters misunderstood the CIP NOPR and inappropriately linked the Commission's proposal with respect to the immediate revocation of access with its proposal with respect to denying access to personnel not on the list. We clarify that we are not requiring the list to be updated simultaneously with the revocation of an employee's access.

d. Jointly-Owned Facilities

465. In the CIP NOPR, the Commission addressed concerns raised with regard to the application of and compliance responsibility for the CIP Reliability Standards, especially on access issues, when facilities governed by existing joint use or joint ownership agreements are involved.

i. NOPR Proposal

466. In the CIP NOPR, the Commission stated that joint owners of critical cyber assets are equally as subject to the CIP Reliability Standards as are other responsible entities.[118] We further stated that, if an asset is designated as a critical cyber asset by one joint owner, it must be treated likewise by the other owner(s) and, therefore, each owner would be responsible to develop a list of its authorized personnel and to respect each other joint owner's corresponding list.

467. With regard to joint use arrangements, the Commission stated the principle that the owner of a critical cyber asset is responsible under the CIP Reliability Standards for ensuring that all persons having access to the critical cyber asset meet the requirements of the CIP Reliability Standards, much as the owner is responsible to ensure that vendor personnel have the required levels of security training, awareness and background checks.

468. The Commission proposed to require the ERO to consider further clarifying CIP–004–1 to address the ''joint use'' concerns expressed by APPA/LPPC while developing any modifications to the CIP Reliability Standards.

ii. Comments

469. APPA/LPPC support the Commission's proposal to direct the ERO to address the joint use concerns.

470. Northern Indiana is concerned that the Commission's proposal means that a responsible entity must perform risk assessments of the other owner's personnel so that such personnel may access a facility that the responsible entity has identified as a critical cyber asset. Northern Indiana argues that such a broad application of the CIP Reliability Standards was never intended and requests that the Commission clarify this point. Northern Indiana sees a conflict with respect to sharing information with other entities that jointly own or jointly use transmission facilities if it is required to maintain a mutual distrust posture. Northern Indiana urges the Commission to provide for flexibility when applying the CIP Reliability Standards to such jointly owned facilities.

471. SPP believes that jointly operated assets may require contractual agreements to assign responsibility and liability for compliance with the CIP Reliability Standards, similar to the Commission's concern with respect to out-sourced service providers in the CIP NOPR. It is unclear to SPP whether the Commission's recommendations adequately cover the situation where each party is uniquely responsible for a subset of the requirements of the CIP Reliability Standards. For example, one entity may place critical cyber assets within a facility managed by a second entity. The second entity would be fully responsible for the physical security requirements of CIP–006–1, while the first entity would be fully responsible for the system management requirements of CIP–007–1 only for their own assets. A contractual agreement between the two entities should be in place to codify the second entity's physical security responsibilities and, as with out-sourced services, to absolve the first entity of any responsibility for CIP–006–1

[117] As we stated in our discussion above, we are directing the ERO to revise the CIP Reliability Standards to explicitly add a requirement for responsible entities to implement any plans they are required to develop as part of these Standards.

[118] *See* CIP NOPR at P 170–73.

beyond ensuring that the cyber assets are within the second entity's physical security perimeter. SPP recommends that the Commission direct the ERO to include recognition of such contractual agreements in its auditing and sanctioning processes.

472. NRECA is concerned that the Commission's joint use proposal would cause problems for small entities. NRECA also raises concerns about how disputes regarding joint use facilities will be addressed.

iii. Commission Determination

473. The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entity's obligations regarding vendors with access to critical cyber assets.

474. Regarding Northern Indiana's comments, we do not believe that this Requirement obligates one joint owner of a critical cyber asset to perform risk assessments of another owner's personnel. Each such owner is responsible for performing assessments of its own personnel.

475. The ERO should consider the suggestions raised by Northern Indiana, SPP and NRECA in the Reliability Standards development process.

476. Therefore, we direct the ERO to modify CIP–004–1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commission's determinations above.

4. CIP–005–1—Electronic Security Perimeter(s)

477. NERC's proposed Standard CIP–005–1 requires identification and protection of the electronic security perimeters inside which all critical cyber assets are located, as well as all access points. The electronic security perimeters are to encompass all the critical cyber assets that are identified using the methodology required by Standard CIP–002–1. Multiple electronic security perimeters may be required; for example, one may be needed around a control room while another may be established around a substation. For any electronic security perimeter established, the responsible entity must develop mechanisms to control and monitor electronic access to all electronic access points and, further, it must assess the electronic security perimeter's cyber vulnerability and test every electronic access point at least annually.[119]

478. The Commission approves Standard CIP–005–1 as mandatory and enforceable. In addition, we direct the ERO to develop modifications to this CIP Reliability Standard. The Commission also requires the ERO to clarify and provide guidance on other matters. The required modifications are discussed below in the following topic areas of concern regarding CIP–005–1: (1) Adequacy of electronic security perimeters; (2) protecting access points and controls; (3) monitoring access logs; and (4) vulnerability assessments.

a. Adequacy of Electronic Security Perimeters

479. Requirement R1 of CIP–005–1 requires each responsible entity to identify electronic security perimeters and ensure that every critical cyber asset resides within one.

i. NOPR Proposal

480. In the CIP NOPR, the Commission stated that, while the electronic security perimeter constitutes a first line of defense, the effectiveness of any one defensive measure is often dependent on the quality of active human maintenance, and that there is no one perfect defensive measure that will guarantee the protection of the Bulk-Power System. The Commission proposed to direct the ERO to develop a requirement that a responsible entity implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter.[120]

ii. Comments

481. Many commenters, including Manitoba, NERC, NRECA, Ontario Power and ReliabilityFirst, maintain that CIP–005–1 is adequate as drafted and they oppose the Commission's proposal to require a defense in depth strategy.[121] In contrast, Juniper and ISA99 Team support the Commission's proposal. Although Idaho Power expresses support for the defense in depth concept, it questions the Commission's proposal to require two distinct security measures when developing an electronic security perimeter. MidAmerican supports the proposal to require implementation of a defensive security approach including two or more defensive measures in a defense in depth posture, but submits that the term ''defensive measure'' requires clarification to facilitate compliance.

482. NERC and ReliabilityFirst argue that the defense in depth provisions recommended by the Commission make sense in a control center environment, because additional layers of electronic security and physical security can be readily implemented, and they are prudent due to the centralized function performed at a control center. However, they question the direct impact to the reliability of the Bulk-Power System from implementing multiple defensive actions in a substation or generating plant environment. NRECA believes that the CIP NOPR contemplates imposing excessive defense in depth requirements, particularly in environments where the additional depth will not yield a significant benefit, but will impose costs. NRECA states that a better course would be for the Commission to defer to the ERO's technical expertise as to the application of defense in depth, rather than dictate a specific outcome.

483. NERC, Idaho Power and ReliabilityFirst further explain that the use of multiple electronic security perimeter devices (i.e., firewalls) obtained from different vendors, creating rings of protection using different methods, is an accepted mainstream information technology approach. The expected result is that a failure of one device only appears on one of the two perimeters, thereby allowing the other perimeter to provide the desired protection. For small numbers of zones, which protect relatively large numbers of assets (e.g., a single zone containing all of the corporate servers), this makes implementation and economic sense.

484. However, NERC states that the use of multiple electronic security perimeter devices comes at a cost to performance and reliability. According to NERC, each ''hop'' through a perimeter device introduces a delay in the transmission of the data. In a traditional information technology environment, this may be tolerable, or may be mitigated through the use of higher-speed networks. In a control system environment, NERC states that neither option may be acceptable or available. Additional equipment takes up space in equipment racks, and uses additional power and cooling, which in

[119] CIP–005–1 only pertains to electronic security. Physical security is addressed in CIP–006–1.

[120] *See* CIP NOPR at P 178–81.

[121] *See also* Arkansas Electric, APPA/LPPC, Alliant, Arizona Public Service, California Commission, Duke, Entergy, FPL Group and Northern Indiana.

some cases, may be at a premium, or may introduce equipment reliability problems. Certified equipment from different vendors may not be available for all protocols and toolsets used in the control system environment. Additionally, there would be more equipment which must be functional in order to maintain reliable operations. Any time there is an increase in the number of components that must be running in series, the availability of the entire system decreases. In this case, this results in an overall decrease in the reliability of the system. Last, but not least, is the impact of having more equipment at a substation or generating plant to install, service, maintain, and for which to provide instruction and training.

485. Ontario Power argues, similarly, that while the multiple layers of security required by a defense in depth strategy may be feasible in some situations, it is impractical or impossible in others and should be excluded from the Final Rule.

486. APPA/LPPC and Northern Indiana state that CIP–005–1 provides the needed degree of flexibility to accommodate very diverse physical and electronic situations.

487. Arkansas Electric, Duke and Northern Indiana state that there is a point at which having multiple defense layers would not be cost-effective. Arkansas Electric and Duke maintain that the CIP Reliability Standards as a whole prescribe a sufficient defense-in-depth strategy. In addition to electronic security controls, Arkansas Electric notes that the Reliability Standards also require physical security controls, access-control, authentication, and intrusion detection at the perimeter. The CIP Reliability Standard also requires a general ''hardening'' of the security of the critical cyber assets. Furthermore, policy and procedural controls are required. Adding security controls for the sake of redundancy adds unnecessary cost, complexity and administrative burden to the system. Further, Duke argues that responsible entities must establish sufficient electronic and physical security perimeters, which in some situations could require multiple layers that other situations do not warrant.

488. Manitoba maintains that providing one monitored and alarmed electronic security measure provides a sufficient and balanced security measure when implemented in conjunction with required physical security measures. The proposed additional security measure may require other security installations within the proposed implementation timeframe for CIP Reliability Standards that could delay implementation of the more important requirement to establish an electronic perimeter for all critical cyber assets.

489. SDG&E and Entergy raise concerns with the Commission's comments regarding the placement of security measures in front of systems. SDG&E cautions against giving such ''in front'' measures a high priority over those placed inside the system. SDG&E comments that consideration of both measures is necessary to make informed defense in depth decisions. Alternatively, it agrees with NERC that the Commission should omit the requirements for a defense in depth approach in the Final Rule. Entergy also disagrees with the Commission's proposal to place measures ''in front of'' systems as opposed to ''inside'' systems. It argues that data/control centers and field sites are two very different matters and that two-factor authentication is more challenging in the field, where most equipment being remotely accessed simply cannot be upgraded or retro-fitted to affect this technological approach.

490. APPA/LPPC argue that, if the Commission continues to direct the ERO to require two or more defensive measures, then it should clarify whether or not the second security measure must be on a par with the first security measure. NERC and APPA/LPPC maintain that an inflexible rule calling for redundant electronic security in all cases poses some very practical problems in a variety of settings. APPA/LPPC believe that, given sufficient flexibility by the Commission, these issues can be worked out in the Reliability Standards development process.

491. In FPL Group's view, the NERC approach of allowing responsible entities to develop strategies appropriate for their environment to protect their critical cyber assets is preferable to the CIP NOPR proposal. FPL Group characterizes the CIP NOPR proposal as a ''one size fits all'' approach that could fail to take into account site-specific realities. It is concerned that the CIP NOPR approach mandates form over function and logic by placing too much emphasis on uniformity and ignoring a site's specific environment.

492. In contrast, Juniper and ISA99 Team argue that multiple layers are essential for defense in depth and that the Reliability Standard must provide guidance on devices that may be considered to be a layer of defense. ISA99 Team argues that single peripheral layers of defense are not adequate to protect control networks. More significantly, ISA99 Team argues, the very nature of the CIP Reliability Standards provides defense in depth for many of the control system components. For example, not only are perimeters identified and established, and defended with access controls, but anti-virus and other defensive measures are applied to components within the perimeters. ISA99 Team argues that this defense in depth is consistent with guidance provided in most references and standards today.[122]

493. In addition, ISA99 Team disagrees that legacy control systems can be excused from defense in depth requirements. ISA99 Team argues that it is unacceptable to leave critical control systems components, like distributed control systems controllers, remote terminal units for supervisory control and data acquisition systems, programmable logic controllers and intelligent electronic devices, without additional protection similar to that commonly used for basic personal computers used in business system networks every day. And this protection can be provided by various means, including further segmentation and isolation of those components from the other parts of the control networks. It does mean additional hardware and does require great caution, but it can be done effectively and should be required for our critical power infrastructure.

494. Juniper comments that, unless wireless access can be limited to a physical boundary, any wireless enabled device must be considered as outside the perimeter and must authenticate to gain access and encrypt its communications. Jamming of RF signals even with spread-spectrum is a real concern. An attack does not have to jam all transmission. It can cause disruption by corrupting data. If this can cause loss of data for even a short duration, that might be enough to perpetrate other incursions without raising alarms.

495. Northern Indiana and Xcel ask the Commission to clarify or direct the ERO to clarify the phrase ''single access point at the dial up device'' in CIP–005–1, Requirement R1.2. Xcel asks whether this refers to the initiating device, the device at the point of termination, or both. Northern Indiana would not modify CIP–005–1, but urges that any modifications to Requirement R2 should

[122] *See* ISA99 TEAM at 4, citing NERC Control Systems Security Working Group's, Top 10 Vulnerabilities of Control Systems and Their Associated Mitigations—2006. The inner layer device may disallow certain protocols on port 520, or only allow read commands from certain networks.

allow continued reliance on legacy systems.

iii. Commission Determination

496. The Commission adopts the CIP NOPR's proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter. However, in light of the comments received, the Commission understands that there may be instances in which certain facilities cannot implement defense in depth or where such an approach would harm reliability rather than enhance it. For that reason, the Commission believes that it is appropriate to allow the ERO and the Regional Entities to grant exceptions based on the technical feasibility of implementing defense in depth, consistent with the Commission's determination on technical feasibility above. However, the responsible entity should implement electronic defense in depth measures or justify why it is not doing so pursuant to our discussion of technical feasibility exceptions.

497. As stated in the CIP NOPR, the Commission recognizes that there is a point at which having multiple defense layers would not be cost effective. However, we continue to believe that the effectiveness of any one defense measure is often dependent on the quality of active human maintenance, and there is no one perfect defense measure that will guarantee the protection of the Bulk-Power System. The Commission does not agree with Manitoba that providing one monitored and alarmed electronic security measure provides a sufficient and balanced security measure when implemented in conjunction with required physical security measures. A single electronic device is too easy to bypass and a physical security measure cannot thwart an electronic cyber attack. Therefore, we believe it is in the public interest to require that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter.

498. Many of the commenters' concerns with regard to the impact on performance and reliability will be alleviated by allowing Regional Entities to grant justified exceptions based on technical feasibility. For example, an exception might be granted if an entity can demonstrate that implementing any defense in depth mechanism would create a delay in the transmission of the data that is not tolerable on the system and cannot be mitigated. In addition, the Commission does not think that there will be a problem with respect to a delay in data transmission. If this is a problem for older or distant equipment, the responsible entity can claim a technical feasibility exception. Newer equipment should operate at sufficiently high speeds that multiple hops will not affect data transmission. In fact, some vendor companies claim that their devices will actually increase transmission speeds due to compression and other techniques.[123]

499. Further, an exception might be granted until equipment is available for a given protocol or toolset used in a specific control system environment. However, the fact that additional equipment may take up space or use additional power and cooling alone does not warrant reversing the Commission proposal.

500. The Commission agrees with the ERO that requiring two or more defensive measures may increase the chance of equipment failure. But, the ERO has not provided the Commission with an adequate explanation of why the availability of the entire system would decrease with two or more defensive measures. Defensive measures can often be formatted so that if they fail, they do so in a fail-safe mode that still allows operation. Therefore, system availability would not decrease.

501. In response to SDG&E and Entergy, in stating that the placement of security measures in front of systems provides a layer of protection for those systems, the Commission was not giving priority to ''in front'' measures. In fact, the Commission acknowledged in the CIP NOPR that defense in depth measures are generally integrated within and constitute part of a system or program. In commenting that defense in depth measures may also be effectively placed in front of a system, the Commission intended only to acknowledge that there are multiple ways to implement a defense in depth strategy. The Commission is not mandating any specific mechanism to be the second security measure. We are also not requiring uniformity of security measures, only that each responsible entity have at least two security measures unless it is not technically feasible to do so. The revised CIP Reliability Standard should allow enough flexibility for a responsible entity to take into account each site's specific environment. The Commission believes that this, in conjunction with the allowance of technical feasibility exceptions, alleviates FPL Group's concern that the Commission's proposal is a ''one size fits all'' approach.

502. In response to APPA/LPPC, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant electronic security in all cases. While the Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process. This would include whether or not the second security measure must be ''on par'' with the first. The Commission also directs the ERO to consider, based on the content of the modified CIP–005–1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

503. In response to Manitoba's concern that the proposed additional security measure could delay implementation of the more important requirement of an electronic perimeter for all critical cyber assets, the Commission notes that this Final Rule approves the Reliability Standard as filed by the ERO. The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures. Until that Reliability Standard is developed by the ERO and approved by the Commission, responsible entities in the United States will not be required to implement two or more defensive measures.

504. The ERO should consider in the Reliability Standards development process Northern Indiana's and Xcel's concerns regarding the phrase ''single access point at the dial up device.''

b. Protecting Access Points and Controls

505. Requirement R2 of CIP–005–1 requires a responsible entity to implement organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the electronic security perimeter. Requirement R2.4 requires ''strong procedural and technical controls'' at enabled external access points ''to ensure authenticity of the accessing party, where technically feasible.''

i. NOPR Proposal

506. The Commission indicated that requiring ''strong'' controls does not provide sufficient guidance toward ensuring authenticity of the accessing party, and proposed to direct the ERO to modify Requirement R2.4 of CIP–

[123] *See, e.g., http://aegistech.us/?page_id=73; http://www.teltone.com/products/security/features.htm.*

005–1 to provide greater clarity regarding the expectation for adequate compliance by identifying examples of specific verification technologies that would satisfy the Requirement, while also allowing compliance pursuant to other technically equivalent measures or technologies.[124] The Commission acknowledged that strong verification includes technologies such as digital certificates and two-factor authentication. We also noted that Recommendation 32 of the Blackout Report emphasizes the need ''to ensure access is granted only to users who have corresponding job responsibilities.''[125]

507. Consistent with our discussion of technical feasibility, we did not propose to direct the ERO to remove the technical feasibility language from Requirement R2.4 of CIP–005–1. However, we proposed that Regional Entities review the application of ''technical feasibility'' as the basis for allowing a responsible entity an exception to full compliance with a Requirement.

508. The Commission also clarified the specific conditions and accountability measures needed to be granted an exception based on technical feasibility.

ii. Comments

509. SoCal Edison and MidAmerican agree with the Commission that Requirement R2.4 needs to be clarified. ISO–NE raises a concern regarding the phrasing of '' 'strong controls' * * * such as digital certificates and two-factor authentication.'' ISO–NE asks that the Commission ensure that ''use of either digital certificates or two-factor authentication'' constitutes an acceptable example for strong authentication. Entergy generally agrees with the Commission's proposal to direct the ERO to modify this CIP Reliability Standard in accordance with the Blackout Report. In Entergy's view, well-constructed passwords should be satisfactory as long as password management best practices are employed, such as configuring equipment to 'drop calls' after presentation of three successive incorrect passwords.

510. Juniper also argues that several CIP Reliability Standards require the use of encryption. Juniper recommends that specific NIST or Federal Information Processing Standards (FIPS) encryption standards be mentioned as minimum requirements for compliance as weak encryption mechanisms can be easily reverse engineered.

iii. Commission Determination

511. The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies. In response to commenters, in discussing digital certificates and two-factor authentication, the Commission was providing examples of strong authentication, not limiting authentication to those options. The Commission is not prescribing the specific methods as an exclusive solution pursuant to Requirement R2.4. The ERO can propose an alternative solution that it believes is equally effective and efficient. If the ERO believes it would be helpful to responsible entities, additional guidance beyond the examples that are eventually included in Requirement R2 can be given in a separate reference document. Since we are directing the ERO to provide guidance on what constitutes strong authentication, it is not necessary for the Commission to respond to ISO–NE's request that digital certifications or two-factor authentication are acceptable methods of authentication. In identifying examples or categories of specific verification technologies that would satisfy Requirement R2.4, the ERO should take into account the specific comments raised in this proceeding. Similarly, while encryption is one method to accomplish two-factor authentication, and is an effective process for ensuring authenticity of the accessing party, for some facilities, we leave it to the ERO in the Reliability Standards development process to evaluate whether and how to address the use of encryption. In the alternative, the ERO may identify verification technologies or categories of verification technologies in a reference document.

c. Monitoring Access Logs

512. Requirement R3 of CIP–005–1 requires responsible entities to implement electronic or manual processes for monitoring and logging access at access points to the electronic security perimeter at all times. Further, where technically feasible, the security monitoring process must detect and alert for attempts at or actual unauthorized access. Where such alerts are not technically feasible, Requirement R3.2 requires a responsible entity to review access logs at least every 90 calendar days.

i. NOPR Proposal

513. The Commission stated that regular manual review of logs is beneficial because, while automated review systems provide a reasonable daily check and a convenient screening for obvious system breaches, periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings. The Commission stated that frequent reviews of access logs are necessary to detect breaches that automated alerts do not detect and, moreover, where automated alerts are not used, frequent monitoring takes on even greater importance.

514. The Commission recognized that accessibility of an access log may affect the review interval. We stated, for instance, that readily available logs, such as those from within a control room setting, should be reviewed at least weekly. Those logs that are not readily available, such as those located at a remote substation, are less accessible and therefore can be read less frequently. We stressed, however, that any attempt to differentiate the required frequency of review of these logs must be balanced against the criticality of the facilities; it is not acceptable to dismiss a critical facility from timely review simply because it is remote.

515. The Commission proposed to direct the ERO to develop a bifurcated review requirement of access logs at electronic access points in which readily available logs are reviewed more frequently than every 90 days. The Commission stated that such review should be performed at least weekly. As part of developing this bifurcated review requirement, the Commission proposed to direct the ERO to include in the Reliability Standard guidance on how a responsible entity should designate individual assets as ''readily accessible'' or ''not readily accessible,'' consistent with our discussion above.

ii. Comments

516. EEI and Tampa Electric maintain that the proposal to revise the log review requirements in CIP–005–1 is overly prescriptive.

517. Entergy, MidAmerican, Northern Indiana, PG&E, ReliabilityFirst, SPP and Tampa Electric do not agree with the Commission that a weekly review of access logs at electronic access points is necessary. A weekly review would place an undue burden on the industry without a clear direct benefit to improved security given the proposed level of increased frequency. Entergy argues that the Commission should

[124] *See* CIP NOPR at P 182–91.

[125] *See* Blackout Report at 164–65, Recommendation 32.

recognize that the other access controls contemplated by the CIP Reliability Standards, as well as the 90-day review, should be sufficient to initially identify any unanticipated form of malicious activity. More frequent reviews should only be required where additional efforts are justified based on site specific or industry information.

518. Tampa Electric argues that weekly manual reviews of substantial data are too burdensome especially when an entity is capable of performing electronic reviews. Along the same lines, Idaho Power argues that the proposed bifurcated review process may be extremely difficult to perform without technological advances in products. Idaho Power agrees that a review must occur; however, without technology to assist, it argues that implementation will be difficult.

519. ISO–NE comments that automated log monitoring to detect and alert on any unauthorized or suspicious events is sufficient, and that manual review of logs should only be required in situations where automated monitoring and alerting tools are not technically feasible. However, ISO–NE does suggest that review of automated alerts should be frequent. ISO–NE maintains that its perspective is supported by evaluations that it conducted against a subset of cyber assets similar to those that would be used to maintain an electronic security perimeter and those that would be found inside an electronic security perimeter. ISO–NE found that the logs generated by its testing were voluminous and any effort to routinely manually review logs would be futile and burdensome. In ISO–NE's view, other than during a forensic investigation in response to an automated alert, any expectation of useful manual review on a routine basis is not reasonable.

520. ReliabilityFirst and SPP disagree that a regular manual review of logs is always beneficial. For example, a weekly manual review of logs in a control room setting may be impossible. In a control center environment, the electronic security perimeter firewalls may log several million events per day. The outer network perimeter firewalls will typically log an even greater number of events per day. Servers and workstations may record hundreds to thousands of events per day across the system, security, and wide variety of application logs. The only way to monitor and analyze the logs is through the use of automation.

521. While MidAmerican supports frequent review, it maintains that the review intervals should be designed to accomplish the detection and improvement objectives discussed in the CIP NOPR. MidAmerican submits that basing review intervals on accessibility of records will not optimally achieve this objective and would be unduly burdensome for responsible entities and should be reconsidered. MidAmerican would support a frequency of 30 days for electronically generated access logs and a 45-day review frequency for manually generated logs.

522. SPP believes that a periodic review of the log correlation and analysis engine's rules should be conducted to ensure the automated analysis is properly alerting on pertinent events. This may require a manual examination of the raw log files. A weekly review is excessive—a quarterly review may be more appropriate, as would a review upon a significant change to the access controls.

523. By contrast, Juniper argues that logs should be reviewed daily, stating that there are correlation tools that can prioritize events automatically and reduce the effort required to go through all logs manually. Juniper argues that the requirement for reporting within an hour of an incident seems to be at odds with not requiring frequent review of the logs.

524. MidAmerican maintains that the term ''bifurcated review'' is inadequately defined. MidAmerican recommends that the Commission add specific language addressing the use of a combination of automated and manual review of logs to satisfy this requirement. Likewise, the terms applying to whether the logs are ''readily available,'' ''readily accessible'' and ''not readily accessible'' need clarification to facilitate compliance. Northern Indiana also requests that the Commission clarify the scope of the reviews and what is meant by the term ''readily accessible.''

iii. Commission Determination

525. The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP–005–1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily, as requested by Juniper.

526. The Commission agrees with MidAmerican that the review intervals should be designed to accomplish the detection and improvement objectives discussed in the CIP NOPR. Requirement R3 of CIP–005–1 does not currently require a responsible entity to manually review logs if it has alerts. However, the Commission continues to believe that, while automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches, periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings. Further, manual review is beneficial to judge the effectiveness of protection measures, such as firewall settings. If a firewall setting is incorrect or ineffective, an automated review system may not identify a cyber security intrusion. For those entities without automated log review and alerts, it is even more important to perform a manual review because this will be the only review of the logs. The Commission believes allowing 90 days to pass without a log review is unacceptable. In that time, an incident could have occurred undetected or an attacker could have gained access to a critical system and extended that access throughout the enterprise with the targeted entity being unaware that the security of their systems had been compromised. For this reason, the Commission directs the ERO to modify CIP–005–1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90-day increments. The Commission continues to believe that, in general, logs should be reviewed at least weekly, but leaves it to the Reliability Standards development process to determine the appropriate frequency. In addition, the Commission directs the ERO to modify CIP–005–1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs.

527. In response to MidAmerican's concern about the term ''bifurcated review,'' the Commission intent was that certain assets, deemed readily accessible, would be reviewed at least weekly while other assets would continue to be reviewed every 90 days. However, the Commission will not adopt this direction from the CIP NOPR. We leave it to the Reliability Standards development process to decide whether different timeframes are appropriate for logs that are readily accessible and not readily accessible. If different review timeframes are adopted, the ERO should provide guidance as to what constitutes a readily accessible log and a log that is not readily accessible. The ERO may also delineate different timeframes for manual review for other reasons, but must clearly define how to determine in

what timeframe a specific log must be reviewed. However, we reiterate that any attempt to differentiate the required frequency of review of these logs must be balanced against the criticality of the facilities; it is not acceptable to dismiss a critical facility from timely review simply because it is remote.

528. Finally, the Commission also agrees with commenters that a full review of logs could be burdensome. Therefore, the Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs. The Commission recognizes that the manner in which a responsible entity determines what sample to review may not be the same for all locations. Therefore, the revised Reliability Standard does not need to prescribe a single method for producing the log sampling. However, any requirements for creating this sample review could be detailed in its cyber security policy so that it can be audited. The Reliability Standards development process should decide the degree to which the revised CIP–005–1 describes acceptable log sampling. The ERO could also provide additional guidance on creating the sampling of log entries, which could be in a reference document. The final review process, however, must be rigorous enough to enable the responsible entity to detect intrusions by attackers.

d. Vulnerability Assessments

529. Requirement R4 of CIP–005–1 requires a responsible entity to ''perform a cyber vulnerability assessment of the electronic access points to [an] electronic security perimeter at least annually.'' The minimum criteria provided do not specify whether a live vulnerability assessment is required, as opposed to a paper assessment.

i. NOPR Proposal

530. In the CIP NOPR, the Commission stated that annual vulnerability assessments are sufficient when no modifications are made, but that when the electronic security perimeter or another measure in a defense in depth strategy is modified, it is not acceptable to wait a year to test modifications.[126] The Commission proposed to direct the ERO to revise the Reliability Standard to require a vulnerability assessment of the electronic access points as part of, or contemporaneously with, any modifications to the electronic security perimeter or defense in depth strategy.

531. The Commission also proposed to direct the ERO to modify Requirement R4 to require live vulnerability assessments at least once every three years, with annual paper assessments allowable in the intervening years. The Commission stated that, if such live vulnerability assessments are not ''technically feasible,'' then a responsible entity may apply to be excused from full compliance to the Regional Entity, fully documenting the necessary interim actions, milestone schedule, and mitigation plan.

ii. Comments

532. Northern California and PG&E support live, not paper, vulnerability assessments of the electronic security perimeter, subject to exceptions where necessary. PG&E qualifies its support, explaining that technical infeasibility is not the only valid reason for not performing a live vulnerability assessment.

533. NERC, ReliabilityFirst, Northern Indiana, SDG&E and Ontario Power address their concerns about live testing issues generally, across Requirements that span several of the CIP Reliability Standards. They argue that the Commission should omit the requirements to include ''live vulnerability testing'' requirements in the Final Rule.[127] NERC and ReliabilityFirst argue that implementing such a requirement would be ill-advised because of the potential for disruption of operations resulting from an improperly run test, or the activation of an unknown or unforeseen vulnerability. NERC and ReliabilityFirst agree that performing such tests in a test environment is extremely useful and desirable, but performing such tests *in situ* in almost all cases would directly lead to significantly degraded reliability at that critical asset. FirstEnergy agrees that the risks of certain forms of live assessments are greater than their benefits. Similarly, NRECA maintains that the Bulk-Power System was not designed to facilitate live testing and is concerned that live testing, where inappropriate, could negatively impact reliability and service to consumers.[128]

534. NERC and ReliabilityFirst believe that ''active'' vulnerability assessments of test systems are beneficial to understanding potential attacks. However, NERC finds it problematic to require test environments for all possible instances of electronic security perimeters and critical cyber assets. While most modern control centers contain such environments, they are rare for substation and generating plant environments, and the required resources could not be justified simply to perform active vulnerability tests once every three years.

535. NERC and ReliabilityFirst argue that, while test systems are required for testing of patches and software updates, these are not required to exactly match or mirror the operational system. For example, if a substation consists of many intelligent electronic devices, but only a few different models of intelligent electronic devices, then the test environment for patches and updates need only have one of each model in order to test updates. Depending on the vendor implementation, a single intelligent electronic device representative of all of the intelligent electronic devices may be sufficient for this purpose. This environment is suitable to test for software vulnerabilities, even though it is not a ''full'' or ''complete'' replication of the real environment, because it represents the essential equipment to perform the test. NERC states that it could support performing active tests in such an environment, provided the responsible entity could document and demonstrate that the test environment and the tests performed do, in fact, map to all the implemented components of the live environment.

536. NERC therefore requests that the Commission decline to include its proposed requirements for live vulnerability testing in the Final Rule. Rather, NERC proposes replacing live vulnerability testing with ''active vulnerability assessments of test systems.'' [129] NERC believes that the active nature of the NERC proposed language addresses the concerns of the Commission, while ensuring reliable operations of the Bulk-Power System. These modifications also must be effectuated through the Commission-approved Reliability Standards development process.

[126] *See* CIP NOPR at P 198–202.

[127] Live vulnerability testing is discussed in several of the CIP Reliability Standards. Where commenters generally discuss live vulnerability testing, those comments are discussed in this section. Comments about specific Reliability Standards are discussed in the section concerning that Reliability Standard.

[128] One example cited by NRECA is software ''patches'' in other industries that failed to work as intended and instead disrupted service.

[129] Alliant, Arizona Public Service and ReliabilityFirst support these wording changes.

537. Northern Indiana argues that the current Reliability Standard allows the flexibility of performing live or paper vulnerability assessments as appropriate.

538. Juniper argues that, in addition to the paper assessment, creation of a ''sandbox'' environment that is fairly representative of the physical plant must be mandatory. Semi-annual penetration test of such a sandbox is essential.

539. MidAmerican believes that conducting a vulnerability assessment of the electronic access points as part of, or contemporaneously with, any modifications to the electronic security perimeter or defense in depth strategy on a three-year cycle would be an extremely burdensome task. It suggests the following: (1) A baseline audit; (2) an assessment during the change control process of the vulnerability implications; and (3) a periodic review based upon the assessment.

540. Several commenters state that the Commission's proposal to require a vulnerability assessment when any ''modification'' of the electronic security perimeter or defense in depth strategy is made is too broad.[130] Commenters generally state that the Commission's use of the modifier ''any'' suggests that the Commission believes that all modifications of the electronic security perimeter, no matter how nominal, must result in a live vulnerability assessment of the entire perimeter. Northern California maintains that, as a result, the contemporaneous testing requirement could be a perverse disincentive that prevents upgrades to increase security when an entity's existing electronic security perimeter is ''good enough.'' An entity with ''good enough'' security may delay upgrades to security in order to minimize testing. Several commenters offer specific examples of modifications which they believe would not warrant a vulnerability assessment. Northern California believes that an appropriate Reliability Standard should require live vulnerability testing within 90 to 180 days of an electronic security perimeter modification.

iii. Commission Determination

541. The Commission notes that the concerns expressed by some commenters of triggering an unknown vulnerability during a live test is one reason why some form of live or active testing is necessary. A responsible entity cannot protect its system from exploitation of vulnerabilities that it does not know about. However, in light of the comments received, the Commission will not adopt its proposal as set out in the CIP NOPR regarding live vulnerability assessments in Requirement R4 of CIP–005–1. Instead, we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments. Further, as discussed below, we clarify that an interim vulnerability assessment will only need to be performed if a responsible entity makes a significant modification to the electronic security perimeter.

542. The Commission's goal in proposing live vulnerability testing is to provide a level of confidence that the Bulk-Power System has a certain level of resistance to attack. We understand the concerns raised by commenters that live vulnerability testing could, at this time, diminish reliability. While the Commission's goal is to require full live vulnerability testing on the entire Bulk-Power System at some point, we understand that this may not be possible at this time. As suggested by FirstEnergy, industry may need time to gain experience in this area before it can conduct full live vulnerability testing. Therefore, the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems.[131]

543. The Commission agrees with the ERO that test systems do not need to exactly match or mirror the operational system. However, to perform active vulnerability assessments, the responsible entities should be required to create a representative system, i.e., one that replicates the actual system as closely as possible. The active vulnerability assessment should be carried out on this representative system. In doing so, a responsible entity must document the differences between the operational and representative system for the auditors. As part of this documentation, the responsible entity should also document how test results on the representative system might differ from the operational system, and how the responsible entity accounts for such differences in operating the system. Our goal is to ensure that each responsible entity understands the differences between its representative system and the operational system and how those differences might affect its test results. The entities remain responsible, however, to ensure that the testing systems are adequate to model the production systems and to document and account for the differences between the two.

544. Further, the Commission agrees with commenters that requiring each responsible entity to perform a vulnerability assessment of the electronic access points when any modification is made to the electronic security perimeter or defense in depth strategy is too broad. Instead, the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification. To be clear, the Commission is not requiring the Reliability Standard to use the terminology that a ''significant change'' is made to the electronic security perimeter or defense in depth strategy. Rather, we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment. For example, we would anticipate that updating an attack signature file on the electronic access point would not require an active vulnerability assessment, but replacing the devices that comprise the electronic access point would require an active vulnerability assessment.

545. Given our changes to the Commission proposal, and based upon the comments, the Commission does not believe performing an active vulnerability assessment once every three years will pose too great a burden on company personnel. The burden above that is required by the Reliability Standard as proposed by the ERO is justified by the insights that will be gained from the active assessments.

546. At this time, the Commission does not believe it is necessary to require twice a year penetration tests by responsible entities, as requested by Juniper. We believe that the combination of annual testing and active vulnerability assessments is sufficient for the Reliable Operation of the Bulk-Power System.

547. In sum, we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years. The ERO should develop the details of how to determine what constitutes a representative system and what modifications require an active vulnerability assessment in the Reliability Standards development process. The revised Reliability Standard should contain the essential

[130] *See, e.g.*, Northern California, FirstEnergy, FPL Group, PG&E and SPP.

[131] The Commission approaches the live testing issues in CIP–007–1, CIP–008–1 and CIP–009–1 from this same perspective.

requirement that an active assessment must be performed at least once every three years. Based on the amount of guidance contained in the modified Reliability Standard, the ERO should consider at that time whether additional guidance should be provided in a reference document.

5. CIP–006–1—Physical Security of Critical Cyber Assets

548. Reliability Standard CIP–006–1 addresses the physical security of the critical cyber assets identified in Reliability Standard CIP–002–1. In particular, CIP–006–1 requires a responsible entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter also reside within an identified physical security perimeter.[132] The physical security plan must be approved by senior management and must contain processes for identifying, controlling, and monitoring all access points and authorization requests.

549. Reliability Standard CIP–006–1 also addresses operational and procedural controls to manage physical access at all access points to the physical security perimeter at all times by the use of alarm systems and/or human observation or video monitoring. The Reliability Standard also requires that the logging of physical access must occur at all times, and the information logged must be sufficient to uniquely identify individuals crossing the perimeter. Finally, the Reliability Standard requires responsible entities to test and maintain all physical security mechanisms on a three-year cycle.

550. In the CIP NOPR, the Commission proposed to approve Reliability Standard CIP–006–1 as mandatory and enforceable. In addition, we proposed to direct the ERO to develop modifications to this Reliability Standard. Further, the Commission also proposed to require the ERO to consider various other matters of clarification, guidance, and modification. In our discussion below, we address the following topic areas regarding CIP–006–1: (1) Physical security plan; (2) physical access controls and monitoring physical access; and (3) maintenance and testing.[133]

a. Physical Security Plan

551. Requirement R1.1 of CIP–006–1 addresses processes that a responsible entity must include in its physical security plan to ensure that all cyber assets within an electronic security perimeter also reside within an identified physical security perimeter. The CIP Assessment noted that Requirement R1.1 anticipates that there may be instances where a completely enclosed border cannot be established and that, in such instances, the responsible entity shall deploy and document ''alternative measures'' to control physical access to the critical cyber assets. It cautioned, however, that Requirement R1.1 does not provide guidance on how an alternative measure should be identified or determined to be adequate.

552. In the CIP NOPR, the Commission stated that the phrase ''alternative measures'' as referenced in Requirement R1.1 should be interpreted to be an exception to the Requirement, and that our discussion of technical feasibility exceptions should apply to Requirement R1.1. We noted that, under this Requirement, the responsible entity is required to deploy and document alternative measures if a completely enclosed six-wall border cannot be established to control physical access to the critical cyber assets. However, we observed that the Requirements did not provide guidance on how an alternative measure should be identified or determined to be adequate. Therefore, the Commission proposed to direct the ERO to treat the allowance of alternative measures as interim actions developed and implemented as part of a mitigation plan under a technical feasibility exception.

i. Comments

553. NERC, APPA/LPPC, OGE, SoCal Edison and SDG&E disagree with the Commission's proposal to treat the allowance of alternative measures as interim actions developed and implemented as part of a mitigation plan under a technical feasibility exception.

554. MidAmerican generally supports the proposal to treat an alternative measure to a six-walled perimeter as an exception and mitigated under a technical feasibility exception for the reasons articulated in the CIP NOPR. However, MidAmerican recommends that the Commission consider the alternative measures to be implemented when a six-wall border cannot be established, where appropriately equivalent, as the mitigation solution and not an interim action. The merits of the alternative measures can be evaluated at the time of an audit.

555. NERC, APPA/LPPC, Arizona Public Service, and Consumers maintain that, where the equipment cannot be contained within a six-wall border, alternative measures should be permitted on a permanent basis. NERC argues that the Commission's proposal implies that by treating these alternative measures as interim actions with required mitigation plans, the responsible entity could overcome the physical or safety-related obstacles to achieving the completely enclosed physical boundary. NERC believes this is impractical, if not impossible. APPA/LPPC assert that the configuration or layout of a specific cyber asset simply may not lend itself to a complete physical perimeter, and alternative means of protection (including electronic protections) may be entirely adequate, given the level of security risk posed by the asset and the nature of the alternative form of protection. In some cases, NERC states that there is no possibility of mitigation. The responsible entity does not choose not to completely enclose the asset—it is a physical limitation which cannot be overcome. In cases where the physical or safety limitations do not exist, the responsible entity is expected to comply with the Requirements, and not use alternative measures. In cases where the physical limitations cannot be overcome, NERC argues that the responsible entity cannot ignore the Requirement, but must implement an alternative. NERC also argues that this alternative is expected to be a permanent solution, not an interim measure.

556. Arizona Public Service agrees with NERC that the Commission should omit this proposal from the Final Rule and supports remanding this provision to NERC to modify R1.1 to permit the use of alternative measures on a permanent basis under requirements, developed through the NERC Reliability Standards development process, which could include documenting and justifying the need for the alternative measure and describing the alternative measures implemented.

557. Georgia Operators states that the industry will continue to struggle for years to agree on a clear definition of

[132] As defined in the NERC Glossary, an ''Electronic Security Perimeter'' means, ''[t]he logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled * * *'' and a Physical Security Perimeter is ''the physical, completely enclosed (''six-wall'') border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets means are housed and for which access is controlled * * *.''

[133] In the NOPR, the Commission also addressed the issue of physical security breaches, and proposed no modification to CIP–006–1. We stated that our concerns would be resolved with modifications proposed to CIP–008–1, pertaining to the term ''reportable incident.'' We affirm that position here.

what comprises six walls for a physical security perimeter: not every wall need necessarily be bunker-strength concrete, but neither should every wall be paper-thin.

558. While APPA/LPPC maintain that alternative measures should be documented by the Regional Entity, Northern Indiana argues that, if a responsible entity establishes or has established adequate alternative measures, then the responsible entity should not need to document or otherwise justify the alternative measure. Northern Indiana requests that, if the Commission does require NERC to modify Requirement R1 in the Final Rule, it clarify what is meant by alternative measures.

ii. Commission Determination

559. We are persuaded by commenters that there may be instances in which the physical or safety-related obstacles to achieving a completely enclosed physical boundary cannot be overcome. In such instances, we agree with commenters that it would be inappropriate to treat the alternative measures under this CIP Reliability Standard as interim actions under the technical feasibility exception, as the exception was proposed in the CIP NOPR. However, the Commission has revised its determination with respect to the technical feasibility exception to address concerns such as those raised by commenters on Requirement R1.1 of CIP–006–1. The Commission believes that allowing a technical feasibility exception to Requirement R1.1 of CIP–006–1, with the changes discussed in the Technical Feasibility section of this Final Rule, should address commenters' concerns. Specifically, the Commission acknowledges that some circumstances merit reliance on mitigation strategies that are ongoing and effective, so long as they are justified and reviewed periodically. This should alleviate the concern of commenters that the Commission is not allowing exceptions to Requirement R1.1 on a long-term basis.

560. Therefore, the Commission directs the ERO to treat any alternative measures for Requirement R1.1 of CIP–006–1 as a technical feasibility exception to Requirement R1.1, subject to the conditions on technical feasibility exceptions.[134] In evaluating the requests for a technical feasibility exception to Requirement R1.1, we expect the ERO to work with the responsible entities to ensure consideration of any emerging technologies that may allow the responsible entity to satisfy Requirement R1.1.

b. Physical Access Controls and Monitoring Physical Access

561. Requirement R2 of the CIP Reliability Standard requires the use of at least one of four listed physical access control methods, but does not require or suggest that the method(s) employed to control physical access consider the characteristics of the access point at issue and the criticality of the asset being protected. Requirement R3 requires monitoring at each access point to the physical security perimeter, including alarm systems and/or human monitoring. For both Requirement R2 and Requirement R3, a responsible entity can choose whether to implement single or multiple access control methods and monitoring devices.

562. The CIP NOPR suggested that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter. It stated that use of a minimum of two different security procedures would, for example, enable continuous security protection when one of the security protection measures is undergoing maintenance and provides redundant security protection in the event that one of the measures is breached. Therefore, while the Commission recognized that there is a point at which implementing multiple layers of defense becomes an unreasonable burden to responsible entities, the Commission nevertheless proposed to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets.

i. Comments

563. While California Commission finds the Requirements of CIP–006–1 to be sound and succinct, it also finds the proposal in the CIP NOPR to require two or more security procedures to be sound policy. It adds that defense in depth strategy should be used in such situations, because multiple security procedures make it harder for a potential attacker to penetrate the system. FirstEnergy finds the Commission's proposal to require a minimum of two different security procedures is appropriate where technically feasible. However, it notes that a variety of different security procedures could satisfy this requirement. For example, the minimum of two different security procedures could be met by having two doors each with one security device or one door with two security devices.

564. Within a substation, NERC and ReliabilityFirst argue that there is no practical way to implement a second physical perimeter without jeopardizing the reliability of the substation itself. If the ''outer'' perimeter is outside the building, NERC and ReliabilityFirst see space problems with adding the mandated physical security perimeter (e.g., monitoring, logging, access control, personnel management, and training) on the border fence, noting that, in most substations, physical space around the control building is at a premium, and implementing an additional perimeter is problematic.

565. NERC and ReliabilityFirst raise similar concerns with requiring two physical security controls as they do with respect to electronic security controls in CIP–005–1. They further argue that, if the control building structure is still expected to be the inner perimeter, then, by necessity, a new perimeter (most likely an additional fence) will need to be built. In space-restricted substations this will likely be impossible. Similarly, if the control building structure is expected to be the outer perimeter, additional construction—whether solid walls or fence-like caging—will need to be constructed inside the control building. In this regard, NERC objects to a requirement to retrofit existing installed equipment to require additional construction or cabinet installation required due to the distributed nature of the equipment. NERC considers it counterintuitive to require that these new constructions be built as ''cabinets within cabinets'' or ''rooms within rooms,'' contending that this kind of construction or implementation is burdensome without real benefit.

566. APPA/LPPC, Idaho Power, Northern Indiana, OGE and Tampa Electric do not believe that it is appropriate to categorically require two different security procedures when establishing a physical security perimeter. APPA/LPPC are concerned that the Commission's proposal to do so could necessitate needless and expensive redundancy. Since Requirements R2 and R3 are already designed to be redundant (controlled access is backed up by monitoring), APPA/LPPC assert the Commission's proposal would appear to require a total of four measures. If the Commission meant that four separate and distinct security measures are necessary to comply with Requirements R2 and R3,

[134] In section II.F.3 of this Final Rule, we explain the circumstances under which technical feasibility exceptions can be claimed and direct the ERO, through the Reliability Standards development process, to revise the Reliability Standards accordingly.

then APPA/LPPC disagree with the proposed change.

567. Entergy argues that the term ''security procedures'' in CIP–006–1 is confusing and that the Commission should direct NERC to define the term. Entergy argues that the terms physical security ''measures'' or ''barriers'' in the context of perimeters would improve clarity, whereas the term ''procedures'' better applies to access control management (R2) and monitoring (R3).

568. Several commenters seek clarification of what the Commission intended in requiring two or more security procedures. For example, SPP interprets the Commission's comment as requiring two independent security procedures at the physical security perimeter access point, as opposed to complementary security controls such as closed-circuit television observation of a secured door. SPP recommends that the Commission clarify that this is its intent, and offers that if a proper defense in depth strategy is used that provides for progressively restricted access or other obstructions to access as one approaches the physical security perimeter, multiple access controls at the physical security perimeter access point are excessive. SPP recommends that a progressive security scheme be acceptable in lieu of implementing multiple access controls at the physical security perimeter access point. SPP further recommends that the Commission clarify its intent as to whether an asset perimeter fence would constitute an acceptable obstruction and achieve the goal of the Commission's proposal. Similarly, MidAmerican requests that the Commission clarify whether the security procedures must be completely independent or may rely on a common component.

569. Arkansas Electric states it is uncertain if the Commission intends the term security procedures to apply to actual methods of implementing physical security (e.g., locks, gates, fences) or to procedural methods (e.g., logging). Arkansas Electric argues that adequate security fencing with a special lock should suffice for a secondary physical security procedure.

570. Idaho Power states that, for example, special locks and key cards would meet the Commission's recommended security procedures; however, they are significantly the same control measure and do nothing to provide defense in depth. While they afford back-up during maintenance, they fall short on defense since one can override the other. If the Commission truly wants to promote defense in depth, Idaho Power states that the chosen options should be required to support one another (e.g., key cards and closed circuit television), and not be just two of the provided four options.

571. Northern Indiana argues that it is unreasonable to put in place two different security measures in remote or field locations. National Grid also argues that two or more different security procedures may not always be needed to accomplish defense in depth.

ii. Commission Determination

572. The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets. However, similar to our determination in CIP–005–1 regarding defense in depth for electronic security perimeters, in light of the comments received, the Commission understands that there may be instances in which certain facilities cannot implement defense in depth or where such an approach would harm reliability rather than enhance it. For that reason, the Commission believes that it is appropriate to allow the ERO and the Regional Entities to grant exceptions based on the technical feasibility of implementing defense in depth, consistent with the Commission's determination on technical feasibility above. However, the responsible entity should implement physical security perimeter defense in depth measures or justify why it is not doing so pursuant to our discussion of technical feasibility exceptions.

573. As stated in the CIP NOPR, the Commission recognizes that there is a point at which implementing multiple layers of defense becomes an unreasonable burden to responsible entities. However, as more fully detailed in our discussion of defense in depth in CIP–005–1, we continue to believe that the effectiveness of any one defense measure is often dependent on the quality of active human maintenance, and there is no one perfect defense measure that will guarantee the protection of the Bulk-Power System.[135] Therefore, we continue to require the use of layered and complementary security procedures that a defense in depth approach embodies.

574. In response to APPA/LPPC's comments, the Commission does not require two or more different monitoring methods under Requirement R3. We did not propose to modify Requirement R3 and are not doing so in this Final Rule. Further, the Commission did not intend to require two or more physical perimeters, as suggested by NERC and ReliabilityFirst. Rather, the Commission intended only to require the ERO to modify R2 to provide for two or more different and complementary physical assess controls at a physical access point of the perimeter. The Commission believes that this should clarify what it meant by the term ''procedures'' and sees no need to direct the ERO to define the term, as requested by Entergy.

575. In response to commenters' questions regarding specific physical access controls, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant physical security. While the Commission continues to believe that a responsible entity must implement two or more distinct and complementary physical access controls at a physical access point of the perimeter, the specific requirements should be developed in the Reliability Standards development process when the ERO develops its modifications in response to this Final Rule.[136] The Commission also directs the ERO to consider, based on the content of the modified CIP–006–1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

576. Northern Indiana raises a concern about security measures in remote or field locations, but did not provide specific information. The Commission believes that, if it is not possible to implement two or more distinct physical security measures in a remote or field location, a Regional Entity could grant justified exceptions based on technical feasibility.

c. Maintenance and Testing

577. Requirement R6 of CIP–006–1 requires responsible entities to implement maintenance and testing programs of physical security systems on a cycle no longer than three years and retain testing and maintenance records for the same timeframe. In addition, Requirement R6 requires retention of outage records of certain physical security systems for a minimum of one year. In the CIP NOPR,

[135] *See* discussion of CIP–005–1, section II.F.4.a, *supra.*

[136] The Commission notes that the requirements in Standard CIP–005–1 are not alone sufficient to address the Commission's goal. CIP–005–1 concerns electronic security perimeters. A single physical security measure is too easy to bypass and an electronic security measure could not thwart a physical attack. Therefore, we believe it is in the public interest to require that a responsible entity must implement two or more distinct physical security measures at a physical access point of the perimeter.

the Commission stated that maintenance and testing of physical security systems should occur more frequently than once every three years. However, the Commission also stated that testing at remote substations should be allowed less frequently. Therefore, the Commission proposed to direct the ERO to modify this Reliability Standard to require that: (1) A readily accessible critical cyber asset be tested every year with a one-year record requirement for the retention of testing, maintenance, and outage records; and (2) a non-readily accessible critical cyber asset be tested in a three-year cycle with a three-year record retention requirement. The Commission stated that this approach provides an appropriate assurance that security measures for geographically dispersed physical assets are functioning properly.

i. Comments

578. FirstEnergy agrees with the Commission that the frequency of the maintenance and testing programs should be a function of the accessibility of critical cyber assets. The Requirement should specify the form of testing and the frequency of such testing that will be considered adequate. For example, testing the functionality of a system that is part of the work environment and used every day may be excessive, while a more extreme form of testing, such as simulated break-ins may be appropriately applied biennially or triennially. In addition, the CIP Reliability Standards should clarify what is considered readily accessible and what is not. Any testing requirements should consider the specific facilities being tested and allow entities to use their discretion until more experience is gained in this area. Finally, changes to the frequency of the maintenance and testing program cycles should be considered in the Reliability Standards development process.

579. National Grid argues that the testing of critical cyber assets (as opposed to testing of physical security measures for such critical cyber assets) is beyond the scope of the physical security requirements in Reliability Standard CIP–006–1. Thus, it requests that the Commission clarify that the CIP NOPR's reference to the testing of critical cyber assets was inadvertent, and that the Commission was merely proposing testing intervals for physical security measures.

580. Northern Indiana requests that the Final Rule clarify what is intended by a ''test.'' A test of a card access system, for example, can be the normal operation with the card and the operation with a non-programmed card to determine whether the lock is working. The protocol for physical security system tests are dictated more by the type of equipment to be tested as well as the equipment's application. Northern Indiana states that, like the Commission, it believes in a strong maintenance and testing program. However, Northern Indiana also believes the focus of the Final Rule should be on whether an unauthorized person accesses the physical security system, and not the administrative nature of testing the system. Clarification of what is intended by, or what makes up, an acceptable test will in effect strengthen the Requirement.

ii. Commission Determination

581. The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP–006–1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years, but clarifies our direction in several respects. Similar to our action with respect to reviewing logs in CIP–005–1, the Commission will not adopt the proposal to require different testing periods for physical security measures on critical cyber assets that are readily accessible or not readily accessible. Instead, we leave it to the Reliability Standards development process to decide whether different timeframes are appropriate for physical security measures on critical cyber assets that are readily accessible and not readily accessible. Similar to our direction in CIP–005–1, if different review timeframes are adopted, the ERO should provide guidance as to what constitutes a readily accessible facility and a facility that is not readily accessible. The ERO may also delineate different timeframes for testing for other reasons, but must clearly define how to determine in what timeframe the physical security measures on a specific critical cyber asset must be reviewed.

582. In response to Northern Indiana, the Commission does not believe it is necessary at this time to specify what would constitute a test, because each test may be different based on the type of physical security measure employed. Northern Indiana may ask the ERO to provide guidance on this matter.

583. In response to National Grid, we clarify that the CIP NOPR's reference to the testing of critical cyber was inadvertent, and that we proposed testing intervals for physical security measures.

6. CIP–007–1—Systems Security Management

584. The Purpose statement in CIP–007–1 states that it requires responsible entities to define methods, processes and procedures for securing those systems determined to be critical cyber assets, as well as the non-critical cyber assets within the electronic security perimeter(s). This Reliability Standard deals primarily with changes made to the operating production systems and verification that such changes will not inadvertently have adverse effects.[137]

585. The Commission approves Reliability Standard CIP–007–1 as mandatory and enforceable. In addition, we direct the ERO to develop modifications to this Reliability Standard. The required modifications are discussed below in the following topic areas of concern regarding CIP–007–1: (1) Acceptance of risk and technical feasibility; (2) test procedures; (3) malicious software prevention; (4) security status monitoring; (5) disposal or redeployment; (6) cyber vulnerability assessment; and (7) documentation review and maintenance.

a. General Issues Regarding Acceptance of Risk and Technical Feasibility in CIP–007–1

586. In the CIP NOPR, the Commission expressed various concerns regarding acceptance of risk and technical feasibility language in CIP–007–1. For example, Requirement R2.3 allows a responsible entity to accept risk rather than take mitigating action where unused ports and services cannot be disabled due to ''technical limitations'' and Requirement R3.2 allows an acceptance of risk in lieu of mitigating risk exposure through a patching program. Requirement R4 requires the responsible entity to use antivirus software and malicious software prevention tools where technically feasible. Requirement R6 of CIP–007–1 requires responsible entities to ensure that all cyber assets within the electronic security perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

587. Requirement R3 of CIP–007–1 requires a responsible entity to establish and document a security patch management program for tracking, evaluating, testing and installing applicable cyber security software patches for all cyber assets within an electronic security perimeter. Among other things, a responsible entity must

[137] *See* CIP NOPR at P 224–25 and CIP Assessment at 31.

document the implementation of security patches. Where a patch is not installed, the responsible entity must document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

588. The Commission proposed to direct the ERO to eliminate the acceptance of risk language from Requirement R3.2.[138] We stated that patch management choices must be weighed in light of the risks involved, with senior management involved in the decision. We noted that this provision is a component of implementing Recommendation 33 of the Blackout Report,[139] which states that using up-to-date patches that deal specifically with security vulnerabilities is of the utmost importance, provided it does not degrade the system and the patch does not create more vulnerability than the problem it is intended to fix.

589. The Commission also proposed to direct the ERO to eliminate the acceptance of risk language from Requirement R2.3. At the same time, the Commission proposed to leave intact the exception for technical limitations in Requirement R2.3. However, the Commission stated that the technical limitations language of Requirement R2.3 raised the same concerns as raised concerning the technical feasibility language. While the Commission acknowledged that an exception for technical limitations might be appropriate, it stated that the language must include the same conditions as discussed in the context of technical feasibility. Accordingly, we proposed that the same conditions and reporting requirements should apply here. Thus, the Commission proposed to direct the ERO to revise Requirement R2 and its subparts to remove the acceptance of risk language and to impose the same conditions and reporting requirements here for ''technical limitations'' as imposed elsewhere in the CIP NOPR regarding ''technical feasibility.''

i. Comments

590. The California Commission agrees with the proposal to remove the phrase ''acceptance of risk'' from the Reliability Standard. The California Commission also finds the existence of the term ''technically feasible'' in this Reliability Standard acceptable with the burden of proof on the individual organization to prove the exception. MidAmerican supports the Commission's proposal to eliminate acceptance of risk from Requirement R2.3 and that exceptions for technical limitation may be appropriate but must be treated as an exception the same as technical feasibility issues. However, MidAmerican cautions that the terms ''technical limitations'' and ''technical feasibility'' need clarification to facilitate compliance.

591. Juniper maintains that it is not technically feasible to turn off ports. It states that, if a device cannot turn off unused ports, it must be protected with a firewall in front of it. Unused open ports are the most common form of attack since devices can fail in unplanned ways when they receive unexpected traffic. Ideally, device providers must be mandated to provide the list of ports they require to be opened, with a description of the protocol expected on each open port.

592. Commenters also raise concerns about the Commission's treatment of security patches. According to APPA/LPPC, the Commission's proposal to eliminate the acceptance of risk language from CIP–007–1, Requirement R3.2 would appear to prevent responsible entities from exercising any discretion to determine not to implement a security patch on the ground that it posed more risk than justified. Limiting the use of acceptance of risk to instances where adoption of a specific compliance measure is determined by the responsible entity to pose more risk than alternative compliance measures, is appropriate, but eliminating all discretion in this area undermines necessary flexibility. In the alternative, APPA/LPPC argue that the Commission should give responsible entities the discretion to determine whether specific security patches create more vulnerability to the Bulk Power System than they solve. In this regard, APPA/LPPC note that the Commission itself stated in the CIP NOPR that the most up-to-date patches should be used, provided this does not ''degrade the system and the patch does not create more vulnerability than the problem it is intended to fix.'' Thus, APPA/LPPC argue that, if the Commission proceeds to delete the acceptance of risk language, it should specifically include the disclaimer on patches referenced above.

593. MidAmerican opposes the Commission's proposal to direct NERC to revise the Reliability Standard to remove acceptance of risk from the provisions for security patch management in Requirement R3. MidAmerican believes that the acceptance of risk should remain in the Reliability Standard if accompanied by a mitigation plan and sunset provisions for the exception. By requiring a mitigation plan to reduce the risk and a time frame to come into compliance the standard provides needed flexibility while maintaining the certainty of a committed end-date.

594. Northern Indiana does not support the Commission's proposal that senior management be involved in each and every case because it is not necessary. The Commission should refine its proposal and provide that senior management should be consulted when mitigation is needed, but not in situations not requiring mitigation. Such situations can be appropriately addressed by senior management's delegate.

595. FPL Group states that, the Commission's statement that patch management must be weighed in light of the risks involved, with senior management involved in the decision, acknowledges that a certain level of risk associated with patch management must be taken into account. However, FPL Group states that this analysis is no different than the acceptance of risk language that the Commission rejects. The Commission is essentially stating that by using technical judgment, a responsible entity's senior management can accept the risk associated with not applying security patches in instances where the patches would degrade performance after performing a risk assessment. Therefore, FPL Group recommends directing the ERO Reliability Standards development process to consider the issue related to acceptance of risk and make appropriate modifications, if any, to the Reliability Standards.

596. Juniper states that an inline intrusion prevention system or intrusion detection system that is able to automatically identify and understand the protocols being used on a control network provides a mitigation for conditions where applying patches against known vulnerabilities is not feasible. Hence, in locations where patches cannot be applied such a network device must be required.

ii. Commission Determination

597. The Commission affirms its proposals with respect to technical feasibility and acceptance of risk. Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirements R2.3 and R3.2. However, as discussed in the CIP NOPR, this leaves intact the exception for technical limitations in Requirement R2.3, so long as the treatment of Requirement R2.3 conforms to our findings regarding the technical feasibility exceptions.

[138] *See id.* P 235–39.

[139] *See* Blackout Report at 164, Recommendation 33.

598. MidAmerican's concerns about clarifying the terms technical limitations and technical feasibility through the Reliability Standards development process are addressed in our findings regarding technical feasibility elsewhere in the Final Rule.

599. In response to Juniper, the Commission does not believe that applying the technical feasibility exception in lieu of acceptance of risk means that a responsible entity would not have to mitigate the risk of not being able to turn off ports. The Commission believes that our discussion of the technical feasibility exception in the Technical Feasibility Exception Remediation and Mitigation section above supplies the obligation to mitigate that Juniper is seeking.

600. With respect to security patch management, the Commission continues to believe that the acceptance of risk language is unacceptable. However, in doing so we do not seek to prevent responsible entities from exercising some level of discretion. The Commission therefore directs the ERO to revise Requirement R3 to remove the acceptance of risk language and to impose the same conditions and reporting requirements as imposed elsewhere in the Final Rule regarding technical feasibility. The Commission believes that this will allow responsible entities the discretion APPA/LPPC seek. Further, this essentially accomplishes the outcome sought by MidAmerican. With respect to the disclaimer requested by APPA/LPPC, the Commission is not convinced to direct such a modification to the Reliability Standard at this time. However, this issue should be examined in the Reliability Standards development process. Given that we are modifying our direction, we do not believe that it is necessary to mandate senior management involvement in these decisions here. While we direct the ERO to modify Requirement R3 of CIP–007–1 to remove the acceptance of risk language, the ERO, through the Reliability Standards development process may choose to allow exceptions to this requirement for technical infeasibility, consistent with the Commission's determination on technical feasibility above. However, the responsible entity should implement the requirements for software patches for all cyber assets within an electronic security perimeter or justify why it is not doing so pursuant to our discussion of technical feasibility exceptions.

b. Test Procedures

601. Requirement R1 of CIP–007–1 requires a responsible entity to ensure that new cyber assets and significant changes to existing cyber assets within the electronic security perimeter do not adversely affect existing cyber security controls. Responsible entities must create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system and its operation. They must document that testing is performed in a manner that reflects the production environment and must document test results.

602. The CIP Assessment suggested that Requirement R1.2 should require the responsible entity to document how each significant difference between the production and testing environments is considered and addressed.[140]

603. In the CIP NOPR, the Commission stated that, if a testing environment does not accurately reflect the production environment, testing of systems may not be adequate to judge impacts on reliability. While, ideally, testing should be conducted on a precise duplicate of the production system, the Commission acknowledged that this is not always possible. When it is not, any differences between the test environment and the production system should be documented. Therefore, the Commission proposed to direct the ERO to modify Requirement R1 and its subparts to require documentation of each significant difference between the testing and the production environments, and how each such difference is mitigated or otherwise addressed.

i. Comments

604. FirstEnergy argues that, while it is reasonable for the Commission to require documentation of significant differences between the testing and production environments, the Commission should clarify that it is not expecting that the differences themselves would be mitigated in the test—other than to simply get the test environment as close as possible to the production environment. The Commission should ensure that the documentation required to document the differences will not be burdensome.

605. MidAmerican supports the proposal to document differences between the testing and production environments, but suggests that these differences not be reported for every test version, but only when the production and test environments are established.

606. Northern Indiana maintains that the existence of any significant difference means the test will not reflect the production environment, which would violate Requirement R1.3. Further, Northern Indiana maintains that differences in testing and production environments may be difficult to eliminate or to mitigate. In a simulated test, differences will exist. Northern Indiana maintains that small differences should not require mitigation.

607. Northern Indiana argues that documenting vulnerability test results or the existence of any mitigation or remediation plans would reveal any vulnerability on its system. Tampa Electric contends that this would produce an unnecessary administrative burden. It explains that there are instances when the production system is too large and complex to practically reproduce in a test environment. In this circumstance, according to Tampa Electric, documenting every detail would expend additional resources without producing useful information.

608. ISO–NE and Northern Indiana ask for clarification of the term ''significant difference'' in the CIP–007–1 proposal. ISO–NE states that the term significant difference is highly subjective and potentially burdensome without actually enhancing an entity's security posture.

ii. Commission Determination

609. The Commission has discussed issues related to testing environments in CIP–005–1.[141] In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP–005–1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a ''representative system''—one that includes the essential equipment and adequately represents the functioning of the production system. We therefore direct the ERO to develop requirements addressing what constitutes a ''representative system'' and to modify CIP–007–1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.

610. Consistent with our action in CIP–005–1, the Commission will not at this time require documentation of each difference between the testing and the production environments and how each such difference is mitigated or otherwise addressed. In using the term mitigation, our goal was to ensure that each responsible entity understands the

[140] CIP Assessment at 32.

[141] Section II.H.4.d, *supra*.

differences between its representative system and the production system and how those differences might affect its test results. The Commission believes that, as a part of this documentation, the responsible entity should also document how any test results might differ from the testing system to the production system and how the responsible entity accounts for such differences in operating the system. Therefore, we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above. Such revision should address what types of differences must be documented. The entities remain responsible, however, to ensure that the testing systems are adequate to model the production systems and to document and account for the differences between the two.

611. With respect to MidAmerican's proposal that the differences between the testing and production environments only be reported when the production and test environments are established, the ERO should consider this matter in the Reliability Standards development process. However, the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production.

612. The Commission understands Northern Indiana's concern that documenting vulnerability test results or any mitigation or remediation plans may reveal system vulnerabilities. The ERO should alleviate this concern by providing for such reports to be reviewed under the confidentiality provisions of its Rules of Procedure.

c. Malicious Software Prevention

613. Requirement R4 of CIP–007–1 requires responsible entities to use antivirus and other malicious software prevention tools where technically feasible, and allowing an acceptance of risk option. The Requirement and its subparts do not provide direction on how to implement this type of protection, where it should be deployed, or what care must be taken to implement and test malicious code protection in order to avoid harm to the production system.

614. The Commission proposed to direct the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere. The Commission discussed the issues of defense in depth, technical feasibility, and risk acceptance elsewhere in the CIP NOPR and applied those conclusions here. The Commission further proposed to direct the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software into a cyber asset within the electronic security perimeter through remote access, electronic media, or other means.[142]

i. Comments

615. Consumers argues that requiring antivirus software on every system in the electronic security perimeter that uses a routable protocol would not be warranted. In Consumers' view, requiring such software on a blanket basis would itself lead to reliability problems. Thus, Consumers argues that only those systems that are vulnerable to this type of threat should require protection under this guideline.

616. In this regard, Consumers argues that many operating systems, like the UNIX operating server systems, switches and bridges, may be critical cyber assets. But they are not directly vulnerable to virus attacks and need not be protected by antivirus applications. In corporate environments, UNIX servers do require antivirus and malware protection, since they use hyper text transfer protocol and e-mail services which can make them infected carriers. However, there are no instances in control system environments requiring any such protection.

617. Consumers concedes that network infrastructure devices that are not directly targeted can be affected as collateral damage. But, it argues, some of the critical cyber assets do not have any mechanism for antivirus installation. Finally, Consumers argues that the Commission should promote the idea of perimeter defense, using firewall based content vulnerability security devices to protect the control systems' electronic security perimeter rather than application of antivirus software to every critical cyber asset.

618. MidAmerican asks the Commission to clarify the intent of the proposal that Requirement R4 be modified to include safeguards against personnel introducing, maliciously or unintentionally, viruses or malicious software to a cyber asset. Northern Indiana believes that systems and protections are in place to prevent unintentional actions affecting a cyber asset. It states that there are no safeguards that protect against all malicious or unintentional acts. Juniper recommends that network-based antivirus and intrusion prevention devices be mentioned as minimum requirement for such safeguards against unintentional introduction of malware by authorized personnel.

ii. Commission Determination

619. The Commission adopts the CIP NOPR proposal with regard to CIP–007–1, Requirement R4. Issues concerning technical feasibility and acceptance of risk are discussed above.

620. The Commission will not adopt Consumers' recommendation that every system in an electronic security perimeter does not need antivirus software. Critical cyber assets must be protected, regardless of the operating system being used. Consumers has not provided convincing evidence that any specific operating system is not directly vulnerable to virus attacks. Virus technology changes every day. Therefore we believe it is in the public interest to protect all cyber assets within an electronic security perimeter, regardless of the operating system being used. Further, as Consumers admits, any network infrastructure devices that are not directly targeted can be affected as collateral damage.

621. While we agree that no safeguard will protect against all malicious or unintentional acts, this does not mean that systems should not be protected against such acts. In response to MidAmerican, the Commission believes that details regarding how to safeguard systems against personnel introducing, maliciously or unintentionally, viruses or malicious software to a cyber asset are best developed in the Reliability Standards development process. The revised Reliability Standard does not need to prescribe a single method for protecting against the introduction of viruses or malicious software to a cyber asset by personnel. However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance with the Reliability Standard. The Reliability Standards development process should decide the degree to which the revised CIP–007–1 describes how an entity should protect against personnel introducing viruses or malicious software to a cyber asset. The ERO could also provide additional guidance in a reference document.

[142] *See* CIP NOPR at P 240–44.

622. Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere. The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above.[143]

d. Security Status Monitoring

623. Requirement R6 of CIP–007–1 requires responsible entities to ensure that all cyber assets within the electronic security perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security. Among other things, a responsible entity must maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Reliability Standard CIP–008–1. Logs must be retained for 90 calendar days, and the responsible entity must review logs of system events related to cyber security and maintain records documenting review of logs.

624. In the CIP NOPR, the Commission stated that logs should be reviewed with the frequency necessary to ensure timely identification of a cyber security incident. We noted that this issue of log review touches on Blackout Report Recommendation 35, which addresses network monitoring, and Recommendation 37 which addresses diagnostic capabilities.[144] The Commission therefore proposed to direct the ERO to revise Requirement R6 to include a requirement that logs be reviewed on a weekly basis for readily accessible critical assets and reviewed within the retention period for assets that are not readily accessible. We stated that this direction should be completed consistent with our discussion above regarding ''readily accessible'' assets.[145] The CIP NOPR stated that accessibility should take into account both physical remoteness and available communications channels. We stated that we would expect control centers to fall within the ''readily accessible'' category.

625. The Commission also proposed to direct the ERO to revise Requirement R6.4 to clarify that while the retention period for all logs specified in Requirement R6 is 90 days, the retention period for logs mentioned in Requirement R6.3 for the support of incident response as required in CIP–008–1 is the retention period required by CIP–008–1, *i.e.*, three years. The Commission maintained that Requirement R6.4 is somewhat unclear and could be read to suggest that the 90 day period also applies to logs kept for purposes of CIP–008–1, and such an interpretation would conflict with the Requirements of that Reliability Standard.

i. Comments

626. Similar to the concerns raised with regard to the log review requirement in CIP–005–1, commenters generally oppose the Commission's proposal to include a requirement that logs be reviewed on a weekly basis for readily accessible critical assets and reviewed within the retention period for assets that are not readily accessible. Northern Indiana, FPL Group, Idaho Power, MidAmerican, Entergy and SPP raise the same concerns as they did with respect to CIP–005–1. MidAmerican and Northern Indiana request clarification of the term ''readily accessible'' to facilitate compliance. Northern Indiana also requests clarification of what is meant by the reference to forensics and how data would be used in forensic investigations.

627. Juniper argues that it is crucial that logs be maintained for at least three years to allow analysis to detect behavioral anomalies and perform forensics in case of a successful attack. It argues that any device that is network enabled in the broadest sense must be considered readily accessible, and its logs ought to be checked at least daily.

ii. Commission Determination

628. Requirement R6 of CIP–007–1 does not address the frequency with which logs should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP–007–1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP–005–1.[146] Also, at this time, the Commission does not believe that it is necessary to require responsible entities to maintain all logs for at least three years, as requested by Juniper.

629. For the reasons discussed in CIP–005–1, in directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the Commission will allow a manual review of a sampling of log entries or sorted or filtered logs. The Commission recognizes that how a responsible entity determines what sample to review may not be the same for all locations. Therefore, the revised Reliability Standard does not need to prescribe a single method for producing the log sampling. However, how a responsible entity performs this sample review should be detailed in its cyber security policy so that it can be audited to determine compliance with the Reliability Standards. The Reliability Standards development process should decide the degree to which the revised CIP–007–1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document. The final review process, however, must be rigorous enough to enable the entity to detect intrusions by attackers.

630. In response to Northern Indiana, the Commission discusses our use of the term forensics in our discussion of CIP–009–1.[147]

e. Disposal or Redeployment

631. Requirement R7 of CIP–007–1 requires the responsible entity to establish formal methods, processes and procedures for disposal or redeployment of cyber assets. In the CIP NOPR, the Commission addressed the concern that solely to ''erase the data,'' as stated several times in Requirement R7, may not be adequate because technology exists that allows retrieval of ''erased'' data from storage devices, and that effective protection requires discarded or redeployed assets to undergo high

[143] *See id.*

[144] *See* Blackout Report at 165–66, Recommendations 35 and 37.

[145] *See* section II.B.4.c (Monitoring Access Logs) in the CIP NOPR.

[146] In our findings on CIP–005–1, we directed the ERO to modify CIP–005–1 through the Reliability Standards development process to require manual review of logs without alerts in shorter than 90 day increments. In addition, the Commission directed the ERO to modify CIP–005–1 to require some manual review of logs even if alerts are employed on the logs.

[147] *See* section II.H.8.b, *infra.*

quality degaussing.[148] We noted that erasure is as much a method as it is a goal, and that the requirement ultimately needs to assure that there is no opportunity for unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it. Degaussing is not the sole means for achieving this goal. The Commission therefore proposed to direct the ERO to modify Requirement R7 to clarify this point.[149]

i. Comments

632. Northern Indiana states that the CIP NOPR is unclear what needs to be clarified in Requirement R7. Northern Indiana believes the only way to allow ''no opportunity'' to access data on storage media is to destroy the media. Northern Indiana states that it takes costly measures to erase data storage tapes and other storage media and follows the requirements of the United States Department of Defense, performing a seven-layer wipe of its storage media. Northern Indiana maintains that, if the clarification sought by the Commission is intended to direct NERC to be more prescriptive about erasure, Northern Indiana states that its cost of compliance will rise because failed disk devices could no longer be returned to manufacturers for replacement without destruction of the drive. Manufacturer warranties will no longer be effective after the storage media is destroyed. Requirement R7 as written is sufficiently broad and can apply to numerous media types. In addition, adherence to Department of Defense requirements should be adequate.

ii. Commission Determination

633. The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it. The Commission notes that there is a difference between redeploying an asset and discarding it. Redeploying an asset within the same responsible entity allows that responsible entity to maintain control over the asset, whereas disposing of an asset places it out of the control of the responsible entity. The Commission believes that, while the seven layer wipe described by Northern Indiana may be sufficient for redeployment because the responsible entity maintains control over the cyber asset, it is not sufficient for disposing of an asset.

634. The Commission disagrees with Northern Indiana that the only way to allow no opportunity to access data on storage media is to destroy the media. As stated in the CIP NOPR, high quality degaussing can adequately protect media from unauthorized access. Northern Indiana has not provided information that convinces the Commission that a cyber asset would have to be destroyed in order to prevent access.

635. Therefore, the Commission directs the ERO to revise Requirement R7 of CIP–007–1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data.

f. Cyber Vulnerability Assessment

636. Requirement R8 of CIP–007–1 requires a responsible entity to perform a cyber vulnerability assessment of all cyber assets within the electronic security perimeter at least annually. Requirement R8.4 requires development of an action plan to remediate or mitigate vulnerabilities identified in the assessment, but it does not provide a timeframe for completion of the action plan.

637. In the CIP NOPR, the Commission stated its belief that vulnerability testing is a valuable tool in determining whether actions that were taken to shore up the security posture of the electronic security perimeter and other areas of responsibility are in fact adequate.[150] We noted that the Blackout Report recognized the importance of vulnerability assessments in Recommendation 38, which called for vulnerability assessment activities to identify weaknesses and mitigating actions.[151] Recognizing that a poorly chosen vulnerability assessment process could result in a false sense of security, the direction provided by this Requirement is important. The Commission noted that monitoring execution status is a good means to keep the action plan on track. Therefore, the Commission proposed to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.

i. Comments

638. MidAmerican supports the proposal to require the ERO to provide additional direction surrounding the vulnerability assessments conducted by the responsible entities, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of an action plan, for the reasons articulated in the CIP NOPR.

639. ISO–NE proposes that the Final Rule omit the Commission's proposal because, given the diversity of hardware and software implementation throughout the industry, providing more meaningful direction on ''features, functionality, and vulnerabilities'' is not feasible. In the view of ISO–NE, no Reliability Standard can evolve fast enough to keep-up with emerging and diverse technologies and newly discovered vulnerabilities. Therefore, ISO–NE requests that the Commission omit this proposal from the Final Rule.

640. FPL Group and NRECA raise the same concerns about cyber vulnerability assessments as they did under CIP–005–1. Further, FPL Group states that, while specific directions may be appropriate with regard to certain Reliability Standards, the intent of this Reliability Standard is to determine whether there are vulnerabilities with regard to a specific system. In FPL Group's view, overly rigid guidance or requirements by the ERO could result in responsible entities failing to properly test for vulnerabilities specific to the entities' environments and systems, thus undermining the intent of the Reliability Standard.

641. SDG&E agrees that a vulnerability assessment should look for and prioritize specific types of vulnerabilities, and provides specific suggestions on such prioritization.[152] SDG&E comments that it should be recommended, but not required, that more than one tool should be used to find vulnerabilities.

642. Northern Indiana states that the responsible entity should maintain the makeup and depth of any vulnerability or penetration tests it undertakes, and control the associated mitigation timeline it establishes to address the results of the tests. Northern Indiana

[148] *See* CIP Assessment at 34–35. To degauss is to demagnetize. Degaussing a magnetic storage medium removes all data stored on it.

[149] *See* CIP NOPR at P 253–56.

[150] *See id.* P 257–60.

[151] *See* Blackout Report at 167, Recommendation 38.

[152] SDG&E identifies: (1) As unacceptable risk, vulnerabilities that can be exploited remotely without a user's cooperation to obtain access to the victim host; (2) as highly critical, vulnerabilities that can be exploited remotely but require the victim to take some action, such as open an attachment, to obtain access; (3) as medium critical, vulnerabilities that unnecessarily increase the attack surface of the victim host such as installed applications and unneeded running services; and (4) as low priority, vulnerabilities that provide potential attackers with reconnaissance information.

raises the same concerns about revealing its vulnerability test results as it did with respect to CIP–005–1

ii. Commission Determination

643. The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.

644. The Commission agrees with ISO–NE that hardware and software is implemented in diverse ways throughout the industry, but does not believe that this renders providing guidance infeasible. We also agree that overly rigid guidance could result in responsible entities failing to properly test for vulnerabilities specific to the entities' environments and systems. The Commission does not believe that the revised Reliability Standard should be inflexible. It should encourage responsible entities to take into account emerging and diverse technologies and newly discovered vulnerabilities as they emerge. The Commission believes that it is appropriate to leave such guidance to the Reliability Standards development process. Further, we leave it to the ERO's discretion whether to put guidance in the revised Reliability Standard or a reference document.

645. The Commission addressed Northern Indiana's concerns about revealing vulnerability test results in our discussion of CIP–005–1. We believe that the ERO's confidentiality provisions should adequately protect against unwanted disclosure of vulnerability test results.

g. Documentation Review and Maintenance

646. Requirement R9 of CIP–007–1 requires the responsible entity to review, update and maintain all documentation needed to support compliance with the Requirements of CIP–007–1 at least annually. Changes resulting from modifications to the systems or controls must be documented within 90 calendar days of the change.

647. The Commission addressed concerns that the 90-day timeframe for updating documentation appears excessively long, especially given the context that this Reliability Standard establishes a significant line of defense for protecting critical cyber assets and that up-to-date documentation is essential in case of an emergency. The Commission proposed to direct the ERO to modify Requirement R9 to state that the changes resulting from modifications to the system or controls shall be documented within a 30-day time period. We stated our belief that the planning and engineering of system and control modifications require sufficient lead time to enable the documentation of such modifications to take place within a 30-calendar-day timeframe.[153]

i. Comments

648. Northern Indiana, Mr. Brown and MidAmerican object to shortening the time allowed for documentation of modifications to the system or controls from 90 to 30 days. Northern Indiana argues that a 90-day period provides flexibility in finalizing such documentation given the nature and type of facilities and their locations, particularly in light of the potential need for internal reviews and approvals by a number of people or groups of people before a documentation change can be effected. MidAmerican agrees that the proposed time line for required documentation may not be sufficient in all instances, particularly for remote locations that are relatively resource constrained.

649. Mr. Brown objects to the proposal to reduce the filing period from 90 to 30 days for documenting changes resulting from modifications to the system or controls. He argues that, in many organizations that will be impossible, or at least extremely costly in staff time. He argues that this will simply lead to unnecessary, trivial instances of technical noncompliance. Thus, Mr. Brown argues that, while 90 days may be too long, a more appropriate, practical and achievable period would be 60 days.

650. ISO–NE and SDG&E ask when the 30-day period begins. They request that the Final Rule direct the ERO to clarify for both CIP–007–1 and CIP–009–1 that changes resulting from modifications to the systems, controls, and procedures shall be documented within 30 days of final implementation of the modifications. Juniper agrees that the 30-day period should begin after the modifications are in place, i.e., accepted, tested, in production and running.

ii. Commission Determination

651. The Commission adopts a modified version of the CIP NOPR proposal. We direct the ERO to revise Requirement R9 to state that the changes resulting from modifications to the system or controls shall be documented quicker than 90 calendar days. The Commission believes that 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process or procedure to secure the system against a known risk. Therefore, the Commission believes that 90 days is too long to allow a responsible entity to have incorrect documentation. Thirty days should be sufficient time to update any necessary documentation.

652. The Commission clarifies that the shorter period should begin upon final implementation of the modifications. The Commission believes that providing that the shorter period begins when the modifications are implemented satisfies Northern Indiana's concern about finalizing documentation and the potential need for internal reviews and approvals. By the time any modification is made, such approvals should already have been granted. Similarly, the Commission believes that MidAmerican's concern about resource constraints relate more to the implementation of a modification, not the documentation of that implementation. Once a modification is developed and implemented, documenting it should not consume significant time or resources.

7. CIP–008–1—Incident Reporting & Response Planning

653. Proposed Reliability Standard CIP–008–1 requires a responsible entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets. Specifically, Requirement R1 of CIP–008–1 requires responsible entities to develop and maintain an incident response plan that addresses responses to a cyber security incident. The plan should characterize and classify pertinent events as reportable cyber security incidents and provide corresponding response actions. The response actions should include: (1) The roles and responsibilities of the incident response teams; (2) procedures for handling incidents; and (3) associated communication plans. In addition, cyber security incidents must be reported to the Electricity Sector Information Sharing and Analysis

[153] *See* CIP NOPR at P 261–63.

Center (ESISAC) either directly or through an intermediary. The incident response plan should be reviewed and tested at least annually. Changes to the incident response plan are to be documented within 90 days. Responsible entities must retain documentation related to reportable cyber security incidents for a period of three years.

654. The Commission approves Reliability Standard CIP–008–1 as mandatory and enforceable. In addition, we direct the ERO to develop modifications to this Reliability Standard. The required modifications are discussed below in the following topic areas of concern regarding CIP–008–1: (1) Definition of a reportable incident; (2) reporting; and (3) full operational exercises and lessons learned.

a. Definition of a Reportable Incident

655. Requirement R1 of CIP–008–1 makes reference to reportable cyber security incidents, but it does not provide a definition of a ''reportable incident.''

656. In the CIP NOPR, the Commission recognized the risk that cyber security incidents may go unreported depending upon a responsible entity's interpretation of a reportable incident.[154] We noted that the Blackout Report also pointed out the need for ''uniform standards for the reporting and sharing of physical and cyber security incident information'' in Recommendation 42.[155] We recognized that the definition of a reportable incident is currently undergoing extensive industry debate, and stated that it could be a catalyst for developing an appropriate level of guidance. We concluded that it is possible to provide guidance regarding what should be included in the term reportable incident and proposed to direct the ERO to: (1) Develop and include in CIP–008–1 language that takes into account a breach that may occur through cyber or physical means;[156] (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced.[157]

i. Comments

657. FirstEnergy, MidAmerican, Northern Indiana, ReliabilityFirst and SPP support the Commission's proposal that the ERO should provide guidance on the definition of reportable incident. Each also provides the Commission with input on how the term should be defined.

658. ReliabilityFirst and SPP recommend that NERC, as the operator of the ESISAC, be directed to publish the reporting criteria and thresholds separately from the CIP Reliability Standards and to provide appropriate reporting mechanisms for that purpose. They maintain that this approach would allow the ERO to maintain maximum flexibility in times of emergency. They state that Reliability Standard CIP–008–1 should then be modified to require entities to report incidents, both physical and cyber, that meet the criteria published by the ESISAC. For audit purposes, both SPP and ReliabilityFirst maintain that NERC should be required to maintain a three-year minimum change history for the published criteria and demonstrate that changes to the criteria were proactively announced and disseminated to all entities in a timely manner. By placing the reporting criteria in the CIP Reliability Standard itself, any changes would have to undergo the defined, lengthy Reliability Standards revision process and could impact the timely collection of information essential to the protection of the North America's critical infrastructure.

659. MidAmerican supports the proposal to further define and clarify the definition and reporting requirements for an incident and including a breach that may occur through cyber or physical means in an incident report, when the breach meets the other requirements outlined for an electronic incident. FirstEnergy states that the Commission should require reportable incident to be defined as an incident report for a security breach that may occur through physical means. According to FirstEnergy, a reportable incident determination should consider the totality of circumstances surrounding a physical breach.[158]

ii. Commission Determination

660. The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. In developing the guidance, the ERO should consider the specific examples provided by commenters, described above. However, we direct the ERO to develop and provide guidance on the term reportable incident. The Commission is not opposed to the suggestion that the ERO create a reference document containing the reporting criteria and thresholds and requiring responsible entities to comply with the reference document in the revised Reliability Standard CIP–008–1, but will allow the ERO to determine the best method to accomplish the goal of better defining reportable incident.

661. Therefore, the Commission directs the ERO to develop a modification to CIP–008–1 to: (1) Include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced.[159]

b. Reporting

662. CIP–008–1, Requirement R1.3, requires each responsible entity to establish a process for reporting cyber security incidents to the ESISAC. The responsible entity must ensure that all reportable cyber security incidents are reported to the ESISAC either directly or through an intermediary. ESISAC procedures require the reporting of a cyber incident within one hour of a suspected malicious incident. However, compliance with ESISAC's Indications, Analysis and Warnings Program Standard Operating Procedure is voluntary.

663. In the CIP NOPR, the Commission addressed concerns regarding the importance of responsible

[154] NERC's FAQ document answers the question of ''what is a reportable incident?'' by referencing definitions in the ESISAC Indications, Analysis, and Warnings Program guidelines document entitled ''Indications, Analysis and Warnings Program Standard Operating Procedure'' and the Department of Energy Form OE 417 Report entitled ''Electric Emergency Incident and Disturbance Report.'' However, since these materials are not incorporated into the proposed CIP Reliability Standards, CIP–008–1 remains ambiguous in this regard. North American Electric Reliability Council, Frequently Asked Questions (FAQs) Cybersecurity Standards CIP–002–1 through CIP–009–1, March 6, 2006, page 27, question 1.

[155] *See* Blackout Report at 168, Recommendation 42.

[156] The Commission emphasized in the CIP NOPR that a cyber security incident that does not result in a material loss of physical assets should not prevent the incident from being reported.

[157] *See* CIP NOPR at P 267–70.

[158] For example, FirstEnergy states that, if it is apparent from an internal assessment of the breach that the intent of the perpetrator was not to gain access to cyber assets, then an incident report should not be required.

[159] *See* CIP NOPR at P 267–70.

entities receiving timely information about other entities' reportable cyber security incidents.[160] Depending on the nature of the incident, timelines of incident reporting may be critical, which raised concern as to whether CIP–008–1 should incorporate ESISAC's one-hour reporting limit or another reporting interval that would provide adequate time for another responsible entity to take meaningful precautions. The Commission concluded that the ESISAC one-hour reporting limit is reasonable and proposed that it be incorporated into CIP–008–1.

664. The Commission proposed to direct the ERO to modify CIP–008–1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report. We left development of the details to the ERO, but stated our view that the reporting timeframe should run from the discovery of the incident by the responsible entity, and not the occurrence of the incident.

i. Comments

665. The Texas PUC states that the Commission's proposal for a one-hour reporting limit is reasonable if there is a uniform reporting form. The Texas PUC states that, if a cyber security attack affects several facilities, the one-hour reporting requirement would provide necessary information to other responsible entities that would allow them to take precautionary measures to protect their systems. Further, a uniform reporting form could be easily submitted to multiple agencies.

666. FirstEnergy maintains that it would be appropriate to include the one-hour time frame for reporting cyber security incidents, but the Reliability Standard should specify that the one-hour time period applies from the time of the discovery of the event, which may include at least a preliminary investigation of the incident by the reporting entity. SDG&E asks for clarification that the one-hour time frame would commence when the responsible entity is made aware of the event, which could be later than actual occurrence.

667. Northern California supports the Commission's recommendation that NERC modify Requirement R1.3 of CIP–008–1 to include a requirement that a cyber security incident be reported after the discovery of the incident. However, both NRECA and ReliabilityFirst state that the appropriate time for response should be addressed through the Reliability Standard development process.

668. In contrast, Entergy, MidAmerican and Northern Indiana object to the one-hour reporting limit. Given the potential penalties involved for non-compliance, Entergy argues that the Commission should require reporting within one hour of discovery of the incident, whether or not the reason or cause is known, unless system restoration takes priority to ensure reliability. If system restoration is a priority, reporting should be performed within four to eight hours depending on the measures required for system restoration. Northern California agrees that the reporting requirement should contain exceptions to ensure entities that are focused on recovery are not punished. According to Northern California, these exceptions should be more than technical feasibility and should allow for the fact that, in a crisis, human beings tend to focus on solving the crisis.

669. Entergy asks the ERO to clarify the relationship between CIP–001–1, which requires the reporting of sabotage events, and CIP–008–1, which requires the reporting of cyber security incidents. Entergy notes that many responsible entities will be required to report an actual or suspected cyber or communication attack that causes major interruptions of electrical systems events to the U.S. Department of Energy on DOE Form OE 417. This report must be submitted within one hour after discovery of an actual attack or six hours after a suspected attack. It is not clear why this report, which may satisfy certain CIP–001–1 requirements, would be submitted under a different timeline than any report required under CIP–008–1. Entergy believes that reporting for cyber security incidents should be coordinated as much as possible. Entergy suggests consideration of consolidating the requirements of CIP–001–1 and CIP–008–1.

670. MidAmerican disagrees with the Commission's contention that a one-hour notification from discovery provides such probative value as to justify the burden involved. On the contrary, MidAmerican submits the more likely result will be to cause far too many false positives from preliminary reports. MidAmerican recommends that the Commission strike a more balanced approach—either extend the window to six to twelve hours from discovery or make it one hour from when it is classified.

671. The California Commission maintains that the term appropriate government authorities should specify the exact authorities in each state. For example, it states that in California, power plants are subject to California Commission jurisdiction. Accordingly, California Commission argues that, for California, the term appropriate government authority should include the California Commission. Similarly, the Texas PUC states that, in Texas, the reports should be sent to NERC, the Texas PUC, the Texas Regional Entity and ERCOT. According to Texas PUC, this would not be unduly burdensome because only minimal changes would be needed to existing cyber security plans.

672. FirstEnergy agrees that there is a need for uniformity for reporting and sharing of physical and cyber security incident information. In this regard, FirstEnergy argues that NERC should adopt the DOE reporting mechanism, DOE Form OE 417, rather than create a new mechanism. On this same topic, Applied Control Solutions comments that NIST, FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, should be used to make this report.

ii. Commission Determination

673. The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP–008–1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report. As stated in the CIP NOPR, the reporting timeframe should run from the discovery of the incident by the responsible entity, and not the occurrence of the incident.[161]

674. Most commenters are concerned with the burden placed on a responsible entity to report an incident when system restoration should take precedence. As stated in the CIP NOPR, while the Commission agrees that, in the aftermath of a cyber attack, restoring the system is the utmost priority, we do not believe that sending this short report would be a time consuming distraction, and we judge that its probative value would justify the minimal time spent in making this report. In this respect, the Commission now clarifies that the responsible entity does not need to initially send a full report of the incident. Rather, to report to appropriate government authorities and industry participants within one hour, it would be sufficient to simply communicate a preliminary report, including the time and nature of the incident and whatever

[160] *See id.* P 271–80.

[161] *Id.* P 280.

useful preliminary information is available at the time. This could be accomplished by a phone call or another method. The responsible entity could then follow up with a full report once the system is restored.

675. With respect to the arguments by California Commission and Texas PUC concerning the term appropriate government authorities, we believe this determination should be made through the Reliability Standards development process.

676. Thus, the Commission directs the ERO to modify CIP–008–1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report. The Reliability Standard development process should consider whether the ESISAC could act as an intermediary to promptly notify government authorities for responsible entities. While we expect the modified Reliability Standard to be consistent with our discussion above, we leave development of the details of how to report incidents while not burdening the recovery process to the Reliability Standards development process.

677. With respect to Entergy's question about the relationship between CIP–001–1 and CIP–008–1, the ERO should consider Entergy's concerns in the Reliability Standards development process. However, the Commission notes that, while CIP–001–1 requires the reporting of sabotage events, CIP–008–1 requires the reporting of all cyber security incidents. Not all cyber security incidents will be caused by sabotage, so not all incidents required to be reported under CIP–008–1 will be required to be reported under CIP–001–1.

c. Full Operational Exercises and Lessons Learned

678. Requirement R1.5 of CIP–008–1 requires the responsible entity to maintain a process to ensure that the cyber security incident response plan is reviewed at least annually. Requirement R1.6 requires a process to ensure that the response plan is tested at least annually, and that such tests can range from a paper drill, a full operational exercise, or the response to an actual incident. CIP–008–1 does not require documentation or reassessment of a plan's adequacy as a result of lessons learned from testing or in response to specific issues.

679. In the CIP NOPR, the Commission addressed questions of whether the annual testing of the incident response plan should require full operational exercises due to the potential for such exercises to uncover unforeseen complications, and whether prospective benefits would balance attendant costs.[162]

680. We recognized that annual testing may be costly and disruptive, but also that periodic operational drills are important because they may reveal weaknesses, vulnerabilities, and opportunity for improvement that a paper drill alone would not identify. The Commission stated its view that a full operational exercise should be performed at least once every three years, and that tabletop exercises are sufficient for the other two years, believing that this arrangement strikes an appropriate balance between the benefits of executing an operational exercise and the associated costs and potential risks of disruptions. Therefore, the Commission proposed to direct the ERO to revise the Reliability Standard to require responsible entities to perform a ''full operational exercise'' at least once every three years, or to fully document its reason for not conducting an exercise in full operational mode pursuant to the parameters used elsewhere for technical feasibility exceptions. Further, the Commission proposed to direct the ERO to provide guidance on the meaning of the term ''full operational exercise.'' [163]

681. The Commission stated that industry will benefit from a requirement to document and implement lessons learned from testing or responses to actual cyber security incidents. While such information may be included in the ''update'' language of Requirement R1.4, we believe that CIP–008–1 would be improved by making a ''lessons learned'' requirement explicit. Therefore, the Commission proposed to direct the ERO to refine CIP–008–1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned. The Commission also proposed to direct the ERO to include language to require revisions to the incident response plan to address these lessons learned.

i. Comments

682. MidAmerican supports the Commission's change to a three-year testing cycle, as long as a full operational exercise doesn't require the asset be taken out of service. MidAmerican argues that the risk to reliability by performing a full operational exercise on a live system seems to outweigh the benefits. MidAmerican states that, while many EMS/SCADA systems are implemented with redundant failover systems that facilitate recovery exercises, this may not be the case for all equipment/systems at control centers, substations and/or plants. MidAmerican argues that taking equipment out of service during these exercises could result in an unexpected impact to reliability. MidAmerican also supports the proposal to refine the Reliability Standard to require complete documentation and a lessons learned section for the reasons articulated in the CIP NOPR.

683. Idaho Power requests that the Commission not include the proposed requirements for full operational exercises in the Final Rule. Idaho Power believes that testing should only be performed on a test platform. The risk to the reliable operation of the Bulk-Power System outweighs the perceived benefit of this type of testing. With adequate test plans, trained and qualified personnel, and a regimented change management process, Idaho Power believes adequate protection is in place without additional modifications to the standard.

684. Entergy also disagrees with the proposed requirement to perform a full operational cyber exercise involving operational systems. This is a formula for unnecessary risk to reliability of the control systems used to operate the grid. There is a wide and permuted range of potential incident types that would need to be simulated in a full exercise, and the response to different incidents can literally mean disconnecting control system elements from the network to which they are attached—while in production operation. This is perhaps the most challenging of all the CIP Reliability Standards to address in practice, and in the absence of a representative identical parallel test suite of equipment upon which to conduct the exercises, the reasonableness of such testing is questionable. Entergy believes that the industry should not be required to perform tests in a real time production command and control system—the potential risks outweigh the potential value.

685. SoCal Edison states that it conducts numerous operational tests and drills and requests clarification that drills conducted under CIP–008–1 can be coordinated with other operational tests currently in place.

ii. Commission Determination

686. The Commission adopts the CIP NOPR proposal to direct the ERO to

[162] *See id.* P 281–87.

[163] The meaning of the term ''full operational exercise'' is addressed below.

modify CIP–008–1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned. The Commission further directs the ERO to include language in CIP–008–1 to require revisions to the incident response plan to address these lessons learned.

687. In light of the comments received, the Commission clarifies that, with respect to full operational testing under CIP–008–1, such testing need not require a responsible entity to remove any systems from service. The Commission understands that use of the term full operational exercise in this context can be confusing. We interpret the priority of the testing required by this provision to be that planned response actions are exercised in reference to a presumed or hypothetical incident contemplated by the cyber security response plan, and not necessarily that the presumed incident is performed on the live system. A responsible entity should assume a certain type of incident had occurred, and then ensure that its employees take what action would be required under the response plan, given the hypothetical incident. A responsible entity must ensure that it is properly identifying potential incidents as physical or cyber and contacting the appropriate government, law enforcement or industry authorities. CIP–008–1 should require a responsible entity to verify the list of entities that must be called pursuant to its cyber security incident response plan and that the contact numbers at those agencies are correct. The ERO should clarify this in the revised Reliability Standard and may use a term different than full operational exercise.[164]

8. CIP–009–1—Recovery Plans for Critical Cyber Assets

688. The purpose of proposed Reliability Standard CIP–009–1 is to ensure that recovery plans for critical cyber assets are in place and following established business continuity and disaster recovery techniques and practices. This Reliability Standard requires the development, updating, and testing of recovery plans, as well as storage and testing of associated backup data and backup media.

689. The Commission approves Reliability Standard CIP–009–1 as mandatory and enforceable. In addition, we direct the ERO to develop modifications to CIP–009–1 through the Reliability Standards development process. Further, the Commission also requires the ERO to consider various other matters of clarification, guidance, and modification. The required modifications are discussed below in the following topic areas of concern regarding CIP–009–1: (1) Recovery plans; (2) forensic data collection; (3) operational exercises; (4) updating recovery plans; (5) backup and storage of restoration data and (6) testing of backup media.

a. Recovery Plans

690. Requirement R1 of CIP–009–1 requires the responsible entity to create and annually review recovery plans for critical cyber assets. Requirement R1.1 requires specification of response to ''events or conditions of varying duration and severity that would activate the recovery plan(s).''

691. In the CIP NOPR, the Commission recognized that the Requirement R1.1 language is very general and does not provide or require a definition of what constitutes a precipitating event or triggering condition necessary for recovery plan implementation. We stated our concern that precipitating events should be readily recognized by responsible entities so that recovery plans are promptly implemented, but declined to propose modifications of the events and conditions language at this time.[165]

692. We also noted that Requirement R1 does not specifically require implementation of a recovery plan because it requires that recovery plans must be created and reviewed but does not explicitly require actual implementation when the events or conditions occur. The Commission proposed to direct the ERO to modify CIP–009–1 to include this requirement. We stated that, in the interim period, the Commission will infer that implementation is embodied in this Requirement when enforcing it, i.e., if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard.

i. Comments

693. MidAmerican supports the proposal to explicitly require the implementation of plans required in this Reliability Standard for the reasons articulated in the CIP NOPR. This issue also has arisen with regard to other Reliability Standards.

ii. Commission Determination

694. For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP–009–1 to include a specific requirement to implement a recovery plan. We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard.

b. Forensic Data Collection

695. Requirement R1 of CIP–009–1, in requiring recovery plans, does not require the collection of forensics data and does not address how such collection activities relate to restoration of service efforts.

696. In the CIP NOPR, the Commission stated that concern for the reliability of the Bulk-Power System requires attention to forensics data collection, and noted that the Blackout Report also emphasized the need to improve forensics and diagnostic capabilities in Recommendation 37.[166] We explained that obtaining forensic data will benefit the long-term reliability of the Bulk-Power System because the lessons learned from one event assist in eliminating or dealing with a repeat or similar event. We noted that forensic data collection procedures could be as minimal as preserving a corrupted drive, making a data mirror of the system before proceeding with recovery, or taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data. The Commission proposed to direct the ERO to modify CIP–009–1 to incorporate use of good forensic data collection practices and procedures into this Reliability Standard.

697. We acknowledged that recovery of critical cyber assets and the Bulk-Power System is of short-term critical importance, and information collection efforts should not impede or restrict system restoration, but emphasized that it is also important to long-term reliability interests that responsible entities make solid forensic efforts in a given situation, such as collecting the data immediately after system restoration or the recovery of critical cyber assets, if that is what can be done. We recognize that collecting forensic

[164] Because the use of the term full operational exercise in CIP–009–1 appears to have different implications for the testing environment, we encourage the development of a different term here in CIP–008–1.

[165] *See* CIP NOPR at P 291–93.

[166] *See* Blackout Report at 166, Recommendation 37.

data may not be technically feasible for all situations due to equipment limitations, such as some legacy systems or older substation installations with little electronic monitoring. Therefore, the Commission suggested that it may be appropriate to allow a technical feasibility exception for forensic data collection where, if invoked, the responsible entity would be required to propose interim actions, milestone schedules, and a mitigation plan, the same as required by other instances of the clause. Also, we proposed to direct the ERO, when incorporating the use of good forensic data collection practices into this Reliability Standard, to make clear that such practices should not impede or restrict system restoration and to consider whether it is necessary to include a technical feasibility provision.[167]

i. Comments

698. NERC, SPP, ReliabilityFirst, Alliant, Arizona Public Service, Entergy, Idaho Power and Manitoba argue that the term forensics in other arenas conveys concepts of scientific rigor and chain of custody to assure that data are not tampered with in a legal proceeding. None of these are conducive to rapidly restoring service, or to maintaining or enhancing reliable operations of an already failed component. Thus, NERC, ReliabilityFirst and Idaho Power argue that this term should be removed from the Final Rule and replaced with the phrase ''data collection for post-event analysis, where technically feasible.'' Alliant agrees with NERC.

699. NERC believes that the Commission's intent would be better served through the development of a guideline concerning how data collection and analysis should be performed to determine causes of failures. NERC, the Commission and the responsible entities could then work together to engage control system vendors and manufacturers to develop and implement changes to their products to more readily allow the collection of high quality cyber event data, that can be used together with operational data to better understand the specific events which caused the outage or failure leading up to the need to invoke the incident response plan. NERC argues that the vendor community is in the best position to develop these toolsets, because, in most cases, both hardware and software modifications would be required to allow the rapid and efficient collection of quality data. Further, NERC argues that technical criteria will need to be developed to allow different manufacturers to generate such event log data in a common format for analysis. Equipment vendors need to be involved in these technical criteria and product development efforts, not the ERO-jurisdictional responsible entities. Idaho Power recommends that the ERO or Regional Entities develop and support work groups to address the latest technologies and methods to alleviate and address the Commission's concerns. Alliant agrees with NERC that these modifications should be effectuated through the Commission-approved Reliability Standards development process.

700. ISO–NE agrees in part with NERC's comments on the proposal to include a reference and requirements regarding the collection of forensic data. Further, forensic analysis is a skill used in the analysis of security incident data, the retention of which for three years is already addressed in CIP–008–1 for incident response. Also, ISO–NE states that CIP–005–1, CIP–006–1 and CIP–007–1 already require the retention of log data to support initial monitoring, analysis, and alerting of identified security incidents.

701. ISO–NE asserts that the broad-brush use of the term forensic data in the Blackout Report included all reliability incident data for post incident analysis. The scope is clear that these Reliability Standards are limited to cyber security incidents, and not all operational incidents impacting reliability. Therefore, ISO–NE believes the Reliability Standards already address this topic adequately, and it is therefore not appropriate to include in CIP–009–1. ISO–NE requests that any direction to the ERO regarding further collection of forensic data, or other operational reliability incident data, be omitted.

702. Entergy argues that forensic procedures can be quite complicated and situation dependent. Entergy argues that, if this CIP Reliability Standard is to be rewritten, it should be limited to the statement that ''use of good forensic data collection practices should be employed.'' Separate guidance could be included in ancillary advisory documents, such as those already available from NIST and various law enforcement authorities.

703. SoCal Edison and Northern Indiana are concerned that forensic data collection practices may hinder efforts to restore Bulk-Power System functionality. SoCal Edison believes that there may be impacts to restoration timeliness as well as additional personnel and hardware required if collection of forensics data are mandated.

704. NRECA believes that restoring service and reliability after an outage or other event must be the primary concern, and the need to preserve evidence should not compromise that objective. In some cases, both objectives can be achieved, and in other cases they cannot. Operating personnel should have the flexibility to make appropriate determinations as long as they can provide a reasonable explanation for their actions, without being exposed to penalties. In any event, it is difficult to reconcile the Commission's statutory authority to approve or remand Reliability Standards with a forensics requirement, which is not itself a Reliability Standard. The ERO, through its Reliability Standards development process, should be allowed to revisit the issue of what priority should be afforded to forensics without having a specific outcome dictated by the Commission.

705. MidAmerican suggests that the Commission substitute a reference to the National Institute of Justice's Forensic Data guideline, in lieu of the reference to ''good forensic data collection.''

ii. Commission Determination

706. The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP–009–1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard. The Commission continues to believe that it is important to long-term reliability interests that responsible entities collect data in certain situations, such as immediately after system restoration or the recovery of critical cyber assets. In response to ISO–NE, the Commission does not believe that the requirement to keep log data contained in other CIP Reliability Standards is sufficient. As we stated in the CIP NOPR, the data collection procedures could include preserving a corrupted drive, making a data mirror of the system before proceeding with recovery, or taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data. None of this is required in the Reliability Standards cited by ISO–NE.

707. The Commission used the term forensic because that is the term used in the Blackout Report. However, the Commission clarifies that it does not intend, as suggested by commenters, that the Reliability Standard impose the extent of scientific rigor or chain of custody required in criminal procedure. Rather, the Commission is concerned with responsible entities preserving the

[167] *See* CIP NOPR at P 294–98.

data necessary to determine the cause of any problem with the system.

708. In response to Entergy, NRECA, SoCal Edison and Northern Indiana, recovery of critical cyber assets and the Bulk-Power System is of immediate critical importance, and information collection efforts should not impede or restrict system restoration, as stated in the CIP NOPR. We agree that preserving evidence should not hinder system restoration.

709. We do not object to the alternate proposal developed by the ERO, including use of the phrase ''data collection for post-event analysis, where technically feasible,'' to describe what should be required under the revised Reliability Standard. The ERO may also consider the methods proposed by Entergy and MidAmerican. We also recognize that collecting forensic data may not be technically feasible for all situations due to equipment limitations, such as older substation installations with little electronic monitoring. Therefore, when revising the Reliability Standard, the ERO may incorporate a technical feasibility exception, subject to the same conditions for exercising the exception as described elsewhere in this Final Rule.

710. Therefore, we direct the ERO to revise CIP–009–1 to require data collection, as provided in the Blackout Report. The modification should focus on responsible entities preserving the data necessary to determine the cause of any problem with the system and may include a technical feasibility exception.

c. Operational Exercises

711. Requirement R2 of CIP–009–1 requires the responsible entity to exercise recovery plans at least annually, and that such exercise can range from a paper drill, to a full operational exercise, or to recovery from an actual incident.

712. In the CIP NOPR, the Commission addressed the question of whether full operational exercises should be required to aid in identifying potential problems and to realize improvements, and concluded that some potential problems that could significantly impair reliability will not be found without them.[168] The Commission stated its belief that table-top exercises alone, on an ongoing basis, will not suffice, given the increasing complexity and interconnection of control systems. We also cautioned that technical feasibility and suitability of risk must be carefully weighed with the possible benefits of conducting the full operational exercises, and therefore opted for a limited approach. We concluded that benefits from operational exercises are sufficient that the industry as a whole should develop suitable operational exercises in the course of evolving good cyber security practices.

713. Accordingly, the Commission proposed to direct the ERO to develop modifications to CIP–009–1 to require a full operational exercise once every three years (unless an actual incident occurs), but to permit reliance on table-top exercises annually in other years. In conjunction, we proposed to direct the ERO to consider the appropriateness of a technical feasibility option, in the limited fashion proposed earlier.[169] As an example, we noted that CIP–009–1 could be modified to allow for partial operational exercises, reduced from full operational exercises, only to the extent a responsible entity explains and documents, for a particular substation or a particular generating plant, technical infeasibility.

714. The Commission noted the lack of clarity of the term full operational exercise and therefore also proposed to direct the ERO to either define in its glossary the term full operational exercise or provide more direction directly in the Reliability Standard as to the parameters of the term for use therein. We acknowledged that many operational exercise practices include table-top components in significant proportions.

i. Comments

715. With the changes included in the CIP NOPR, the California Commission and Texas PUC view this Reliability Standard as acceptable. Consistent with its comments regarding Standard CIP–008–1, MidAmerican supports the Commission's change to a three-year testing cycle, as long as a full operational exercise does not require the asset to be taken out of service.

716. NERC raises similar concerns with the Commission's use of full operational exercises to test recovery plans as it raised with respect to full operational exercises of electronic security perimeters in CIP–005–1.[170] For example, NERC is concerned that the use of the term will require that a substation control environment will need to be completely reconstructed from scratch to ensure that it may be recovered following an incident. In the case of an information technology-only system (such as components of an energy management system), or for high-value centralized systems with limited specialized components (such as a SCADA system with its communications requirements), it may be practical to hold dedicated exercises through the use of dedicated equipment. NERC believes that requiring such full exercises in a substation or generating plant environment wastes resources without providing a significant reliability benefit. Even if such exercises were to be performed, each substation or generating plant implementation is different. Full exercises might imply that each specific substation and generating plant (or even each generating unit at a generating plant) would need to be exercised separately to ensure that the specific nuances of each implementation are exercised.

717. NERC also argues that, when significant damage or failure occurs, responsible entities must take such action as necessary to ensure that their equipment meets the operational and cyber security requirements and expectations. It may not be possible to exactly replicate the damage or failure in a live operations context. NERC maintains that the phrase full operational exercises should be replaced by ''demonstrated restoration of critical cyber assets in a test environment.'' NERC goes on to explain that its comments on representative test environments in CIP–005–1 also apply here.

718. APPA/LPPC support the Commission's proposal. APPA/LPPC also agree with the Commission's determination that NERC should either define full operational exercise in its glossary or provide more direction directly in the Reliability Standard as to the parameters of the term.

719. APPA/LPPC, Arkansas Electric, Idaho Power, FPL Group, SPP and Consumers oppose including a live vulnerability test in a full operational exercise. APPA/LPPC state that, as noted by the Commission, the benefits of operational exercises must be weighed against the technical feasibility and operational risks of such exercises.[171] The commenters state that live vulnerability tests would pose operational risks that would outweigh any benefits such tests would produce. Consumers maintains that, because the activities involved in a live vulnerability/penetration test are intrusive and can result in major vulnerability exploitation beyond control, they can result in unintended damage to the system.

720. FirstEnergy also opposes full operational exercises, on the grounds

[168] *See id.* P 299–304.

[169] *See id.* P 77–86 and section II.F.2–3, *supra* (Technical Feasibility and Acceptance of Risk).

[170] *See* section II.H.4.d.ii, *supra.*

[171] CIP NOPR at P 302.

that they often require entire systems to be shut down, would require a large number of company personnel to be diverted from regular duties, and would provide little value until the industry gains more experience in this area. Until that time, FirstEnergy argues that paper drills and/or table top exercises should be adequate.

721. Northern Indiana requests clarification of what actual incident would excuse a full operational exercise. For instance, an incident (the nature of which may not be known) may occur that compels the responsible entity to stop the full operational exercise, which cannot be rescheduled for several months. The delay in operational testing should reset the clock such that the next paper drill of the tested system is performed one year from completion of the full operational exercise.

722. Idaho Power also argues that, with adequate test plans, trained and qualified personnel, and a regimented change management process, adequate protection is in place without additional changes to the Reliability Standard. ISO–NE asserts that clarification is needed of what constitutes a full operational exercise. ISO–NE thus supports the CIP NOPR's directive to direct the ERO to provide greater clarity as to the meaning of this term. As to whether to provide a definition of full operational exercise in the NERC Glossary, it needs to be understood that what may qualify as such an exercise with regards to readiness of Bulk-Power System operations would be somewhat different from such an exercise with respect to a cyber security incident response plan, or for IT back-up and recovery plans. Therefore, ISO–NE reserves further judgment of requirements for full operational exercises until additional clarity is provided.

723. Arkansas Electric opposes full operational exercises and suggests requiring a ''functional exercise'' be performed at least every three years. Arkansas Electric states that functional exercises are well defined in the emergency management and disaster recovery disciplines. Arkansas Electric notes that the National Incident Management System defines a functional exercise as one that ''simulates the reality of operations in a functional area by presenting complex and realistic problems that require rapid and effective responses by trained personnel in a highly stressful environment.'' Arkansas Electric argues that these exercises are more rigorous than tabletop exercises, yet they do not require the same system disruption as a full scale exercise.

724. Texas PUC maintains that the Commission's proposal to allow some entities to conduct partially operational exercises every three years appropriately recognizes the constraints faced by some entities. However, it states that this exception should not excuse entities from conducting more complex drills.

ii. Commission Determination

725. The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP–009–1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years. Consistent with our goals and discussion of CIP–005–1, the Commission will not at this time require responsible entities to perform full operational exercises. Instead, the Reliability Standard should require the demonstrated recovery of critical cyber assets in a test environment, with the requirements for representative test environments and for addressing differences between the test environment and the production environment, similar to the conditions discussed for live testing in CIP–005–1. Given the range of views presented in comments regarding live testing, as the Reliability Standard development process forms the details of this ''demonstrated recovery'' concept, it should consider offering guidance beyond the actual Requirements of the Reliability Standard in separate reference documents. The Commission believes this alleviates commenters' concerns about the risks associated with such testing.

726. The Commission notes ISO–NE's concerns about providing a definition of full operational exercise in the NERC Glossary are addressed since we are not requiring the use of that term in the Reliability Standards.

d. Updating Recovery Plans

727. Requirement R3 of CIP–009–1 requires the responsible entity to update the recovery plans to reflect any changes or lessons learned from an exercise or the recovery from an actual incident. It requires plan updates to be communicated to the personnel responsible for activating or implementing the recovery plan within 90 days of the change.

728. The Commission stated its concern that individuals responsible for activating and implementing a recovery plan must have the most current information available, and its belief that a 90-day time lag between when a weakness in a recovery plan is discovered and when it is corrected and communicated to such responsible personnel is too long.[172] We noted that failure for the responsible personnel to have current information about a recovery plan could cause unnecessary delay in restoring critical cyber assets to service and thereby jeopardize the reliability of the Bulk-Power System. Therefore, the Commission proposed to direct the ERO to modify Requirement R3 of CIP–009–1 to shorten the timeline for updating recovery plans to 30 days, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. We stated our belief that a 30 day requirement for updating the recovery plans will promote timely incorporation of lessons learned during exercises and actual events, while acknowledging that 90 days is reasonable for the completion of personnel training sessions, due to varied shift schedules and other feasibility issues with regard to facility and organization.

i. Comments

729. MidAmerican supports this proposal for the reasons articulated in the CIP NOPR. Northern Indiana supports retaining the Requirement as is, that is, to allow a 90-day period to both update and communicate recovery plans to responsible personnel.

730. ISO–NE is concerned that there is no clear indication of when the 30 day clock would start and asks that changes resulting from modifications to the systems, controls, and procedure shall be documented within 30 days of final implementation of said modifications, similar to its concerns with respect to CIP–007–1.

ii. Commission Determination

731. The Commission adopts the CIP NOPR proposal to direct the ERO to modify Requirement R3 of CIP–009–1 to shorten the timeline for updating recovery plans. We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective. As we stated with respect to change made pursuant to CIP–007–1, the Commission believes that having correct

[172] *See id.* P 305–08.

documentation is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could attempt to operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process or procedure to secure the system against a known risk. Therefore, the Commission believes that 90 days is too long to allow a responsible entity to have incorrect documentation. Thirty days should be sufficient time to update any necessary documentation. Northern Indiana has not provided us sufficient reason to change the CIP NOPR proposal. Finally, as stated with respect to the documentation requirements in CIP–007–1, the 30 day period should begin upon final implementation of the modifications.

e. Backup and Storage of Restoration Data

732. Requirement R4 of CIP–009–1 requires that a recovery plan include processes and procedures for the backup and storage of information necessary to successfully restore critical cyber assets.

733. We addressed whether the required backups should be tested as part of the system change before they are stored and assumed to be operational.[173] The Commission proposed to direct the ERO to modify CIP–009–1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes.

734. The Commission stated that it understood that preserving multiple generations of restoration backups is common practice, and that competent implementation of the CIP Reliability Standards would tend to include the good and efficient practice of testing recovery backups as they are created. However, the Commission did not find that direction toward these good practices was contained in, implied by, or readily understood from either this or other Requirements among the CIP Reliability Standards, such as Requirement R6 of CIP–003–1. The Commission reiterated its position, stated with regard to the change control processes required by Requirement R6 of CIP–003–1, where no backups of any kind are mentioned, that there is a need for enhanced direction in issues related to proper change control, and that the CIP Reliability Standards should specifically state that a change control process should include procedures for a tested backup. We noted that adding clarification language here to Requirement R4 of CIP–009–1, such as ''these procedures are to include practices to test and verify the operability of the backup before it is stored and relied upon for recovery,'' would eliminate this ambiguity.

i. Comments

735. MidAmerican supports the proposal to modify the Reliability Standard to require the ERO to provide directions on best practices for the back up and restore process for the reasons articulated in the CIP NOPR.

736. FirstEnergy and Northern Indiana disagree with the Commission's proposal to require verification and detection after adding, modifying, replacing or removing critical cyber asset hardware or software, arguing that this requirement is essentially the same as requiring continuous assessment. Northern Indiana argues that verification that backup tapes are operational is merely the assessment that the tapes are functional; verification does not assure the content may be used for restoration purposes. In the Final Rule, the Commission should clarify what is intended by backup and verify in the context of backup and restoration media. MidAmerican requests clarification of what constitutes a significant change that would require verification because it contends that this process could be extremely onerous if required outside of a planned plant shutdown.

737. SPP suggests that testing backups prior to storage is only one mitigation strategy that should be considered along with other available mitigations to assure the ability to recover from a system failure following any event, not just a significant upgrade. SPP suggests that in a properly managed data center environment, a combination of image and incremental backups should be regularly performed, or inter-site disk-to-disk replication should be implemented, regardless of significant system modifications. Periodic recovery testing, coupled with sound system backup/replication management processes, is adequate to assure recovery and restoration of failed cyber assets; special pre-modification backups are not necessary. It is impractical and unnecessary to test every backup media prior to storing it. Other mitigation strategies that may provide equivalent assurance of recovery include reconstitution of the asset from installation media with recovery of data from either backup files or redundant systems, and complete reconstitution of the asset from a redundant system.

738. Moreover, SPP states that some systems cannot be backed up due to their design architecture. In this instance, complete, up-to-date system configuration and recovery/or reconstitution documentation must be maintained. In addition, given the nature of certain deployed cyber assets, it is not possible to perform a restoration test without placing the asset and the facility it serves at risk. All of this must be weighed when developing the business continuity plan.

ii. Commission Determination

739. The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP–009–1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes. Our intent in doing so is to require responsible entities to have a procedure in place that gives them a high confidence level that their backups will actually restore the system as needed. Auditors should be able to determine compliance by reviewing a responsible entity's policies, procedures and records to determine how the testing is done and what recent tests have been performed. In response to commenters' suggestions on how to verify the backup and restoration processes, the ERO should determine appropriate methods to accomplish the Commission's objectives in the Reliability Standards development process.

740. The Commission does not agree with FirstEnergy and Northern Indiana that requiring verification of backup and restoration processes and procedures when a significant change is made to the operational control system requires continuous assessment. The Commission does not believe that every change will necessitate verification of the backup and restoration processes. Rather, it is sufficient to verify a process if a significant change, such as adding new hardware or installing new software to the control system, is made. The Commission does not believe that responsible entities will be making significant changes to their backup and restoration processes continuously. Similar to our determination with respect to Requirement R4 of CIP–005–1, the ERO should determine, through the Reliability Standards development process, what would constitute a

[173] *See id.* P 309–13.

modification that would require verification of the backup and restoration processes.

f. Testing of Backup Media

741. Requirement R5 requires annual testing of information stored on backup media to ensure information essential to recovery is available.

742. The CIP Assessment noted that it is critical that such information be accessible in the event of an actual incident, and that the Reliability Standard does not specify any actions to be taken in the event of a failure in testing, and asked whether such testing should also be conducted on a more frequent basis.

743. In the CIP NOPR, the Commission addressed whether such testing should also be conducted on a more frequent basis and what action should be taken in the event of a failure in testing. We understood that, if these CIP Reliability Standards were implemented in a full and competent manner, then adequate backup verification measures would probably be in place. However, we stated that Reliability Standards demand a higher degree of certainty and should provide the guidance that responsible entities need to have procedures to verify backups are successfully completed every cycle and to have recovery procedures in place for when the backup fails.

744. The Commission proposed to direct the ERO to modify CIP–009–1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, thus guaranteeing that backups are available for future use.[174] We stated that insertion of language such as, ''backup procedures are to include regular verification of successful completion and procedures to address backup failures'' would satisfy this goal. We stated our view that inability to recognize the failure of a backup process poses a great risk, and that the annual restoration testing required here is adequate frequency as long as the backup process is properly managed.

i. Comments

745. ISO–NE agrees with the Commission proposal if the intent is to review the backup process. However, ISO–NE states that testing the actual backup data are not realistic in most instances, because the environment would literally have to be shut down and be restarted with the data in order to test it. ISO–NE asserts that, in an emergency, the restored data are a good starting point for recovery, but for a test process, such activity would not be acceptable due to the impact on reliability and market systems. Therefore, ISO–NE requests that the Commission omit directing the ERO to make any changes to CIP–009–1 Requirements R4 and R5.

746. FirstEnergy states that the requirement to ensure that backups are successful and available for future use should be limited to spot test restorations, such as restoration of a log file, because the ultimate verification of a backup—a complete restoration itself—is not practical.

747. Northern California agrees with the Commission that NERC should expand Requirement R5 of CIP–009–1 to include verification of backups.

ii. Commission Determination

748. The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP–009–1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use. However, the Commission agrees with ISO–NE that it is impractical to require the system to be shut down and be restarted with the data in order to test it. As stated above with respect to verifying backups after a significant change, our intent is to give responsible entities a high confidence level that their backups will actually restore the system as needed. Auditors should be able to look at a responsible entity's policies, procedures and records to determine how the testing is done and what recent tests have been performed. The ERO should determine appropriate methods to accomplish the Commission's objectives in the Reliability Standards development process.

I. Violation Risk Factors

749. Violation Risk Factors delineate the relative risk to the Bulk-Power System associated with the violation of each Requirement and are used by the ERO and the Regional Entities to determine financial penalties for violating a Reliability Standard. The ERO assigns a lower, medium or high Violation Risk Factor for each mandatory Reliability Standard Requirement.[175] The Commission has established guidelines for evaluating the validity of each Violation Risk Factor assignment.[176]

750. In a separate filing, the ERO submitted 162 Violation Risk Factors that correspond to Requirements of the proposed CIP Reliability Standards.[177] While the Commission has addressed the Violation Risk Factors that correspond to the Requirements of the Reliability Standards it has already approved, NERC requested that going forward the Commission approve the Violation Risk Factors when it takes action on the associated Reliability Standards.[178] Accordingly, the Commission addresses the Violation Risk Factors that correspond to the CIP Reliability Standards in this proceeding.

751. In the CIP NOPR, the Commission proposed to approve the 162 proposed Violation Risk Factor assignments that correspond to the Requirements of the CIP Reliability Standards and direct the ERO to revise 43 of them. In addition, the Commission noted that the ERO did not assign Violation Risk Factors to nine Requirements and proposed to direct the ERO to make these Violation Risk Factor assignments and file them for Commission approval.

752. The Commission noted that NERC assigned a ''lower'' designation to almost 85 percent of the Violation Risk Factors corresponding to the Requirements of the CIP Reliability Standards. No Requirements received a ''high'' Violation Risk Factor assignment. The Commission stated that it believed the ERO mischaracterized many of the Requirements as administrative, resulting in a lower Violation Risk Factor assignment, where in fact a medium or high designation was more appropriate.

753. We proposed to direct the ERO to submit a filing containing revised Violation Risk Factors within 60 days of the date of the Final Rule. We also proposed to direct the ERO to include in its filing a complete Violation Risk Factor matrix.

[174] *See id.* P 314–19.

[175] The specific definitions of high, medium and lower are provided in *North American Electric Reliability Corp.,* 119 FERC ¶ 61,145 at P 9 (*Violation Risk Factor Order*), *order on reh'g,* 120 FERC ¶ 61,145 (2007) (*Violation Risk Factor Rehearing*).

[176] The guidelines are: (1) Consistency with the conclusions of the Blackout Report; (2) Consistency within a Reliability Standard; (3) Consistency among Reliability Standards; (4) Consistency with NERC's Definition of the Violation Risk Factor Level; and (5) Treatment of Requirements that Co-mingle More Than One Obligation. The Commission also explained that this list was not necessarily all-inclusive and that it retained the flexibility to consider additional guidelines in the future. A detailed explanation is provided in *Violation Risk Factor Rehearing,* 120 FERC ¶ 61,145 at P 8–13.

[177] *See* NERC's March 23, 2007 filing in Docket No. RR07–10–000, Exh. A.

[178] *See North American Electric Reliability Corporation,* 119 FERC ¶ 61,145 (2007) (May 18 Order) (approving and modifying Violation Risk Factors).

1. General Issues

a. Comments

754. NERC argues that the Commission should not establish a 60-day compliance deadline for NERC to modify the Violation Risk Factors. Instead, it suggests that the Commission should find that Violation Risk Factors may be addressed in the NERC Reliability Standards development process, so long as this produces timely results.[179] Alliant, Arizona Public Service, CEA, Progress and PSEG Companies agree. PSEG Companies point out the numerous procedural hurdles that would make modification of the 43 Violation Risk Factors within a sixty day window extremely difficult. Similarly, while Ontario Power disagrees with the Commission that Violation Risk Factors are not a part of the Reliability Standards, it does not oppose revisiting the Violation Risk Factors through NERC's Reliability Standards development process.

755. While the Commission has elsewhere determined that Violation Risk Factors can be changed outside of the full ERO Reliability Standards development process, NRECA supports and continues to assert that it is preferable for all concerned for such changes to be made within the context of that process. It asserts that institutional bifurcation of the development of the Reliability Standards from the consequences of violation of the Reliability Standards is not a desirable practice and should be minimized. The ERO, through its Reliability Standards development process, should be allowed to revisit the CIP Violation Risk Factors without having a specific outcome dictated by the Commission.

756. Progress maintains that unnecessarily increasing Violation Risk Factors for planning Reliability Standards may have unintended consequences. According to Progress, assigning overly conservative Violation Risk Factors will cause senior managers responsible for CIP Reliability Standard compliance to focus more time and resources on satisfying those Reliability Standards, potentially to the detriment of other Reliability Standards. It maintains that the level of the Violation Risk Factor is intended to communicate the importance of the Reliability Standards and, consequently, the resources that should be devoted to its implementation and the magnitude of the penalty associated with its violation.

[179] NERC cites *North American Electric Reliability Corp.,* 119 FERC ¶ 61,046 (2007) in support of this position.

b. Commission Determination

757. NERC and other commenters ask the Commission to defer to NERC on the determination of Violation Risk Factors and allow NERC to reconsider the designations using the Reliability Standards development process. The Commission has previously determined that Violation Risk Factors are not a part of the Reliability Standards.[180] In developing its Violation Risk Factor filing, NERC has had an opportunity to fully vet the CIP Violation Risk Factors through the Reliability Standards development process. The Commission believes that, for those Violation Risk Factors that do not comport with the Commission's previously-articulated guidelines for analyzing Violation Risk Factor designations, there is little benefit in once again allowing the Reliability Standards development process to reconsider a designation based on the Commission's concerns. Therefore, we will not allow NERC to reconsider the Violation Risk Factor designations in this instance but, rather, direct below that NERC make specific modifications to its designations. NERC must submit a compliance filing with the revised Violation Risk Factors no later than 90 days before the date the relevant Reliability Standard becomes enforceable.

758. That being said, NERC may choose the procedural vehicle to change the Violation Risk Factors consistent with the Commission's directives. NERC may use the Reliability Standards development process, so long as it meets Commission-imposed deadlines.[181] In this instance, the Commission sees no vital reason to direct the ERO to use section 1403 of its Rules of Procedure to revise the Violation Risk Factors below, so long as the revised Violation Risk Factors address the Commission's concerns and are filed no less than 90 days before the effective date of the relevant Reliability Standard.[182] The Commission also notes that NERC should file Violation Severity Levels before the auditably compliant stage.

759. Consistent with the *Violation Risk Factor Order,* the Commission directs NERC to submit a complete Violation Risk Factor matrix encompassing each Commission-approved CIP Reliability Standard.

760. The Commission disagrees with Progress that the Commission's concerns with respect to the CIP Violation Risk Factors will result in overly conservative Violation Risk Factor assignments. We also disagree with the characterization that a Violation Risk Factor delineates the importance of the Reliability Standard. Rather, the Violation Risk Factors delineate the relative risk to the Bulk-Power System associated with the violation of each Requirement. The Commission believes that the analysis below appropriately takes into account the risk of violating each Requirement in the CIP Reliability Standards.

2. Specific Modifications to Violation Risk Factors

761. The Commission proposed to require NERC to assign several Requirements in the CIP Reliability Standards a high Violation Risk Factor. For example, CIP–002–1 Requirement R2, which requires the identification of assets that are critical to the Bulk-Power System, is assigned a lower Violation Risk Factor. While the product of the Requirement is a list of critical assets, the Commission stated that this is clearly not an administrative Requirement. In fact, the failure to properly identify critical assets could place the Bulk-Power System at an unacceptable risk or restoration efforts could be hindered. Further, this Requirement has a controlling effect over all of the CIP Reliability Standards that follow. The Commission stated that, if an asset is critical and is not identified as such, the remaining CIP Reliability Standards will not be applied to that asset. Depending on the asset that is overlooked, and consequently not protected by the Reliability Standards, a higher level of Bulk-Power System failure is possible. Thus, by NERC's definition, this Requirement should have a high Violation Risk Factor assignment. In addition, the recommendations related to physical and cyber security contained in the Blackout Report,[183] while largely addressed by the proposed CIP Reliability Standards, would essentially be thwarted if a responsible entity does not effectively comply with Requirements R2 and R3 of CIP–002–1. Accordingly, we proposed to direct the ERO to modify Requirement R2 to denote a high Violation Risk Factor assignment.

[180] *Violation Risk Factor Rehearing,* 120 FERC ¶ 61,145 at P 11–16 (2007), *citing North American Reliability Corp.,* 118 FERC ¶ 61,030 at P 91, *order on clarification and reh'g,* 119 FERC ¶ 61,046 (2007).

[181] *See North American Electric Reliability Corp.,* 118 FERC ¶ 61,030 at P 91, *order on compliance,* 119 FERC ¶ 61,046 at P 33 (2007).

[182] The Commission notes that this is a change from the CIP NOPR proposal, which proposed to direct the ERO to submit a filing containing these modifications within 60 days of the date of the Final Rule.

[183] Blackout Report at 163–69, Recommendations 32–44.

762. Similarly, CIP–002–1 Requirement R3, which requires the identification of cyber assets that are essential to the operation of critical Bulk-Power System assets, has a medium Violation Risk Factor assignment. By definition, a medium Violation Risk Factor assignment means that the Requirement is unlikely, under emergency, abnormal, or restoration conditions to lead to Bulk-Power System instability, separation, or cascading failures, or to hinder restoration to a normal condition. However, if this Requirement is violated, the Bulk-Power System could in fact be at an unacceptable risk of failure or restoration efforts could be hindered. Further, this Requirement has a controlling effect over all of the CIP Reliability Standards that follow. As with CIP–002–1 Requirement R2, depending on the asset that is overlooked, and consequently not protected by the Reliability Standards, a higher level of Bulk-Power System failure is possible. Also, we stated that proper compliance with CIP–002–1, Requirement R3 is essential to the ability of the proposed CIP Reliability Standards to satisfy the recommendations of the Blackout Report.[184] Accordingly, we proposed to direct the ERO to modify this Requirement to denote a high Violation Risk Factor assignment.

763. The Commission also proposed to direct the ERO to change the Violation Risk Factor assignments for several Reliability Standards from a lower to a medium assignment. The Commission's primary reason for proposing to direct these changes was to promote implementation of the recommendations contained in the Blackout Report; to establish consistency within a Reliability Standard, i.e., among sub- and main Requirements of the same Reliability Standard; and consistency across Reliability Standards.

a. Comments

764. Northern California agrees that many requirements inappropriately have a Violation Risk Factor of lower and that NERC should re-evaluate the Violation Risk Factors of the Requirements identified by the Commission in Appendix B of the CIP NOPR, and urges NERC to adopt the Commission's recommended assessment.

765. While APPA and the LPPC members state that they are committed to complying with all of the CIP Reliability Standards, APPA/LPPC believe that the Commission's proposal to elevate the violation risk factor for CIP–002–1, Requirement R2 from low to high and the violation risk factor for CIP–002–1, Requirement R3 from medium to high should be reexamined. While overlooked assets could result in Bulk-Power System failure, the oversight process now contemplated by Regional Entities over asset designation, and the overwhelming incentive responsible entities have to proceed cautiously, make it difficult to see a substantial potential for assets to be overlooked.

766. EEI states that the proposal to direct the ERO to modify CIP–002–1 to denote a high Violation Risk Factor assignment mandates a particular outcome and does not allow for consideration of any alternative.

b. Commission Determination

767. The Commission adopts the CIP NOPR proposal to direct the ERO to revise 43 Violation Risk Factors. While the Commission hopes that APPA/LPPC are correct that there is not a substantial potential for assets to be overlooked, this is not a reason to not modify the Violation Risk Factors. As we stated in Order No. 672, the fundamental goal of mandatory, enforceable Reliability Standards and related enforcement programs is to promote behavior that supports and improves Bulk-Power System reliability.[185] It is not imposing penalties. However, as APPA/LPPC recognize, overlooked assets could result in Bulk-Power System failure. This comports with the definition of a high Violation Risk Factor as a requirement that, if violated, could directly cause or contribute to Bulk-Power System instability, separation, or a cascading sequence of failures, or could place the Bulk-Power System at an unacceptable risk of instability, separation, or cascading failures. APPA/LPPC have not provided a persuasive reason for the Commission to change its proposal to direct the ERO to modify the Violation Risk Factors.

768. Further, the Commission is not persuaded by the argument that the Violation Risk Factor should not be high because there is an incentive for responsible entities to proceed cautiously. The Violation Risk Factor should consider the risk to the system of non-compliance, regardless of other incentives that users, owners and operators of the Bulk-Power System have to comply.

769. Finally, the regional oversight over asset designation discussed by APPA/LPPC is not in place yet. Therefore, the Commission cannot rule on what it might be.

III. Information Collection Statement

770. The Office of Management and Budget (OMB) Regulations require that OMB approve certain reporting and recordkeeping (collections of information) imposed by an agency.[186] The information collection requirements proposed in the CIP NOPR were identified under the Commission data collection, FERC–725B ''Mandatory Reliability Standards for Critical Infrastructure Protection.'' These proposed information collections will be submitted to OMB for review under section 3507(d) of the Paperwork Reduction Act of 1995.[187] In addition, OMB regulations require OMB to approve certain reporting and recordkeeping requirements imposed by agency rule.[188]

771. The ''public protection'' provisions of the Paperwork Reduction of 1995 require each agency to display a currently valid control number and inform respondents that a response is not required unless the information collection displays a valid OMB control number on each information collection or provides a justification as to why the information collection control number cannot be displayed. In the case of information collections published in regulations, the control number is to be published in the **Federal Register**.

772. *Public Reporting Burden:* The Commission developed its estimate of burden based upon the CIP Reliability Standards as proposed by NERC. The CIP Reliability Standards include only one actual reporting requirement. Specifically, CIP–008–1 requires responsible entities to report cyber security incidents to ESISAC. In addition, the eight CIP Reliability Standards require responsible entities to develop various policies, plans, programs and procedures.[189]

773. The CIP Reliability Standards do not require a responsible entity to report to the Commission, ERO or Regional Entities the various policies, plans, programs and procedures. However, the documentation of the policies, plans, programs and procedures must be available to demonstrate compliance with the CIP Reliability Standards. The Commission has included the cost of developing the required documentation for the required policies, plans, programs and procedures in its burden estimate. The Commission, however,

[184] *Id.*

[185] Order No. 672 at P 455.

[186] 5 CFR 1320.11.

[187] 44 U.S.C. 3507(d).

[188] 5 CFR 1320.11.

[189] *See* CIP NOPR at P 334.

did not include in our burden estimate the cost of substantive compliance with the CIP Reliability Standards, separate from the requirements to develop specific documentation.

774. In formulating our estimate of the reporting burden, the Commission has been guided by several factors.

Number of Entities: As of April 2007, NERC identified 1,266 registered entities in the United States. The Applicability section of each CIP Reliability Standard specifies nine categories of users, owners and operators of the Bulk-Power System (as well as NERC and the Regional Entities) that must comply with the CIP Reliability Standards. The nine categories of users, owners and operators are based on the categories of functions identified in the NERC Functional Model. Based on a review of NERC's registration list, the Commission estimates that approximately 1,000 entities will be required to comply with the CIP Reliability Standards.

Variations in Compliance Burden: The Commission's estimate is based on all 1,000 entities documenting an assessment methodology to identify critical assets and critical cyber assets pursuant to CIP–002–1. As explained above, only those entities that identify critical cyber assets pursuant to CIP–002–1 are responsible to comply with the requirements of CIP–003–1 through CIP–009–1. Accordingly, the cost burden estimate differs for those entities that identify critical cyber assets and those that do not.

Further, the reporting burden would vary with the number of critical cyber assets identified pursuant to CIP–002–1. An entity that identifies numerous critical cyber assets, including assets located at remote locations, will likely require more resources to develop its policies, plans, programs and procedures compared to an entity that identifies one or two critical cyber assets, housed at a single location. Based on this distinction, the Commission has developed separate estimates for large investor-owned utilities and other responsible entities such as municipals, generators and cooperatives.

Customary Practices: Prior to the development of CIP–002–1 through CIP–009–1, NERC approved through its urgent action process a cyber security Reliability Standard known as ''UA–1200,'' which applied to entities ''such as control areas, transmission owners and operators, and generation owners and operators.'' UA–1200 addressed a number of the same reporting burdens as the CIP Reliability Standards at issue in this proceeding. For example, UA–1200 required the creation and maintenance of a cyber security policy, the identification of ''critical cyber assets,'' and the development of a cyber security training program. Thus, entities that voluntarily complied with UA–1200 will continue these practices when the mandatory CIP Reliability Standards are in effect.

Further, many entities, including those that did not comply with UA–1200, typically have followed certain practices specified in the CIP Reliability Standards. The Commission believes that practices such as conducting cyber security training, having procedures for whom to contact in case of a cyber security incident, and developing a plan for how to restore a computerized control system should it fail are usual and customary practices in the electric industry and others. The Commission has taken such customary practices into account when estimating the reporting burden.

Time Period: The proposed CIP Reliability Standards were approved as voluntary reliability standards by the NERC board in May 2006, with a designated effective date of June 1, 2006.[190] The proposed implementation schedule submitted with the CIP Reliability Standards plans for responsible entities to be ''auditably compliant'' with most requirements by mid-2010 or later. Mid-2010 is four years after NERC's voluntary reliability standards went into effect. Therefore, the Commission developed an annual burden estimate by dividing total costs by 4 years.

Data collection	Number of respondents	Number of responses	Hours per response	Total annual hours
FERC–725B:				
Large investor-owned utility	155	1	2,080	322,400
Others, including munis and coops	795	1	1,000	795,000
Entities that have not identified critical cyber assets	50	1	160	8,000
Totals	.....	.....	.....	1,125,400

Information Collection Costs: The Commission estimates the costs to be:

Large investor-owned utility = 322,400 hours@$88 = $28,371,200.

Others, including munis and coops = 795,000 hours@$88 = $69,960,000.

Entities that have not identified critical cyber assets = 8,000 hours@$88 = $704,000.

Because auditably compliant status is not required for many requirements until mid-2010, the Commission has projected the costs over a four-year period. On an annual basis the costs will be ($28,371,200 + $69,960,000 + $704,000)/4 years = $24,758,800 per year.

The hourly rate of $88 is a composite figure of the average cost of legal services ($200 per hour), technical employees ($39.99 per hour) and administrative support ($25 per hour), based on hourly rates from the Bureau of Labor Statistics (BLS). Using the May 2006 OES Industry-Specific Occupational Employment and Wage Estimates, the median hourly rate wage estimate for a computer software engineer is $39.99.[191]

Title: Mandatory Reliability Standards for Critical Infrastructure Protection.

Action: Proposed collection.

OMB Control Number: 1902–0248.

Frequency of responses: On occasion.

Necessity for information: As discussed above, EPAct 2005 adds a new section 215 to the FPA, which 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 the Commission can independently enforce Reliability Standards. Pursuant to section 215 of the FPA, the Commission approves eight CIP Reliability Standards submitted to the Commission for approval by NERC. The CIP Reliability

[190] Although NERC designated an effective date of June 1, 2006, the CIP Reliability Standards are not mandatory and enforceable, *i.e.*, subject to penalties for non-compliance, until they are approved by the Commission.

[191] *See http://www.bls.gov/oes/current/naics2_22.htm.*

Standards require certain users, owners, and operators of the Bulk-Power System to comply with specific requirements to safeguard critical cyber assets. The information collections in the Final Rule are needed to protect the electric industry's Bulk-Power System against malicious cyber attacks that could threaten the reliability of the Bulk-Power System.

1. Comments

775. MidAmerican states that the Commission's information collection assessment warrants revision for significantly underestimating the cost of compliance, even after controlling for variation in the number of critical cyber security assets identified by the responsible entity. MidAmerican alone estimates its total compliance costs as a substantial fraction of the burden amount estimated by the Commission, based upon compliance with the originally proposed CIP Reliability Standards. That cost should be expected to increase by ten percent based upon the more stringent Reliability Standards and rising labor rates. Based on this actual experience to date, MidAmerican submits that the CIP NOPR burden underestimates implementation difficulties by inadequately accounting for both the replacement costs associated with upgrading existing antiquated cyber infrastructure as well as the host of employer recruiting, hiring and training challenges responsible entities will face to demonstrate compliance. The skilled computer software personnel necessary to achieve substantive compliance are in much demand (but short supply), nationally, and accordingly command compensation levels considerably higher than the CIP NOPR assumptions. To remedy these shortcomings, MidAmerican requests that the Commission revisit this issue by sampling the 1,000 or so entities expected to be required to comply with the CIP Reliability Standards and revising the burden estimate accordingly.

2. Commission Determination

776. MidAmerican seems to misunderstand the purpose of the information collection statement. The OMB regulations require agencies to submit a burden estimate for collections of information contained in proposed rules, not for the entire cost of compliance. As stated in the CIP NOPR, the Commission only included the cost of developing the required documentation for the required policies, plans, programs and procedures in its burden estimate, but did not include in our burden estimate the cost of substantive compliance with the CIP Reliability Standards. MidAmerican raises concerns regarding the total cost of compliance with the Reliability Standards, rather than the burden associated with reporting requirements in the Reliability Standards. Therefore, the Commission does not believe it is necessary to revise the burden estimate based on MidAmerican's comments.

IV. Environmental Analysis

777. 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.[192] The Commission has categorically excluded certain actions from these requirements as not having a significant effect on the human environment.[193] The actions proposed here fall within categorical exclusions in the Commission's regulations for rules that are clarifying, corrective, or procedural, for information gathering, analysis, and dissemination, and for sales, exchange, and transportation of electric power that requires no construction of facilities.[194] Therefore, an environmental assessment is unnecessary and has not been prepared in this Final Rule.

V. Regulatory Flexibility Act

778. The Regulatory Flexibility Act of 1980 (RFA) [195] generally requires a description and analysis of any final rule that will have significant economic impact on a substantial number of small entities. The RFA does not mandate any particular outcome in a rulemaking. It only requires consideration of alternatives that are less burdensome to small entities and an agency explanation of why alternatives were rejected.

779. In drafting a rule an agency is required to: (1) Assess the effect that its regulation will have on small entities; (2) analyze effective alternatives that may minimize a regulation's impact and (3) make the analyses available for public comment.[196] In its NOPR, the agency must either include an initial regulatory flexibility analysis (initial RFA) [197] or certify that the proposed rule will not have a ''significant impact on a substantial number of small entities.'' [198]

780. If in preparing the NOPR an agency determines that the proposal could have a significant impact on a substantial number of small entities, the agency shall ensure that small entities will have an opportunity to participate in the rulemaking procedure.[199]

781. In its Final Rule, the agency must also either prepare a Final Regulatory Flexibility Analysis (Final RFA) or make the requisite certification. Based on the comments the agency receives on the NOPR, it can alter its original position as expressed in the NOPR but it is not required to make any substantive changes to the proposed regulation.

A. NOPR Proposal

782. In the CIP NOPR, the Commission analyzed the effect of the proposed rule on small entities.[200] The Commission's analysis found that the DOE's Energy Information Administration (EIA) reports that there were 3,284 electric utility companies in the United States in 2005,[201] and 3,029 of these electric utilities qualify as small entities under the Small Business Administration (SBA) definition. Of these 3,284 electric utility companies, the EIA subdivides them as follows: (1) 883 cooperatives of which 852 are small entity cooperatives; (2) 1,862 municipal utilities, of which 1842 are small entity municipal utilities; (3) 127 political subdivisions, of which 114 are small entity political subdivisions; (4) 159 power marketers, of which 97 individually could be considered small entity power marketers; [202] (5) 219 privately owned utilities, of which 104 could be considered small entity private utilities; (6) 25 state organizations, of which 16 are small entity state organizations; and (7) nine federal organizations of which four are small entity federal organizations.

783. In addition, the Commission's analysis relied on NERC's compliance registry, applying the NERC Statement of Registry Criteria, to identify entities that must comply with the CIP Reliability Standards. For an entity to be included in the compliance registry, the ERO will have made a determination that a specific small entity has a

[192] Order No. 486, Regulations Implementing the National Environmental Policy Act, 52 FR 47897 (Dec. 17, 1987), FERC Stats. & Regs., Regulations Preambles 1986–1990 ¶ 30,783 (1987).

[193] 18 CFR 308.4.

[194] *See* 18 CFR 380.4(a)(2)(ii), 380.4(a)(5), 380.4(a)(27).

[195] 5 U.S.C. 601–612.

[196] 5 U.S.C. 601–604.

[197] 5 U.S.C. 603(a).

[198] 5 U.S.C. 605(b).

[199] 5 U.S.C. 609(a).

[200] CIP NOPR at P 342.

[201] *See* Energy Information Administration Database, Form EIA–861, Dept. of Energy (2005), available at *http://www.eia.doe.gov/cneaf/electricity/page/eia861.html*.

[202] Most of these small entity power marketers and private utilities are affiliated with others and, therefore, do not qualify as small entities under the SBA definition.

material impact on the Bulk-Power System. Consequently, the compliance of such small entities is justifiable as necessary for Bulk-Power System reliability. Based on NERC's compliance registry as of June 2007, the Commission estimated that approximately 1,000 registered entities will be responsible for compliance with the CIP Reliability Standards. Of these, the Commission estimated that the CIP Reliability Standards would apply to approximately 632 small entities, consisting of 12 small investor-owned utilities and 620 small municipal and cooperatives.

784. The Commission's analysis concluded that the CIP Reliability Standards would not have a significant economic impact on a substantial number of small entities. The majority of small entities would not be required to comply with mandatory Reliability Standards based on the application of the NERC Registry Criteria. Moreover, the Commission explained that a small entity that is registered but does not identify critical cyber assets pursuant to CIP–002–1 will not have compliance obligations pursuant to CIP–003–1 through CIP–009–1. While a small entity that identifies only a few critical cyber assets must comply with CIP–003–1 through CIP–009–1, the Commission stated that the economic impact of such compliance would not be significant. Likewise, the housing of a limited number of critical cyber assets in a single location will lessen the economic impact of compliance.

785. The Commission also noted that, while not required or proposed by the CIP NOPR, small entities could choose to collectively select a single consultant to develop model software and programs to comply with the CIP Reliability Standards on their behalf. Such an approach could significantly reduce the costs that would be incurred if each company would address these issues independently.

786. The Commission further explained that, while there would be some portion of small entities that would have to expend significant amounts of resources on labor and technology to comply with the CIP Reliability Standards, the Commission believed that this would be a minority. Further, in such circumstances, the economic impact would be justified as necessary to protect cyber security assets that support Bulk-Power System reliability.

787. The Commission also investigated possible alternatives. These included the Commission's adoption in Order No. 693 of the NERC definition of bulk electric system, which reduces significantly the number of small entities responsible for compliance with mandatory Reliability Standards.[203] The Commission also noted that small entities could join a joint action agency or similar organization, which could accept responsibility for compliance with mandatory Reliability Standards on behalf of its members and also may divide the responsibility for compliance with its members. Based on that analysis, the Commission certified that the proposed rulemaking would not have a significant impact on a substantial number of small entities.

B. Comments

788. NRECA states that, for the most part, the CIP NOPR treats small entities in an appropriate manner. NRECA maintains that the approach of having the CIP and other Reliability Standards apply to small entities only if they have a material impact on the reliability of the Bulk-Power System is appropriate and consistent with the Commission's prior orders, the statute, and the ERO's Statement of Registry Criteria, and NRECA supports it fully, with the exception of the Commission's discussion of jointly-owned facilities, which is discussed with respect to CIP–004–1.[204]

789. APPA/LPPC state that application of the NERC Statement of Compliance Registry Criteria has reduced the total number of public power utilities potentially subject to NERC's Reliability Standards from nearly 2,000 to approximately 326 discrete public power utilities, and APPA/LPPC agree with the Commission that NERC's compliance registry goes a long way toward mitigating the economic impact of the proposed rules on small entities. Nonetheless, APPA/LPPC disagree with the Commission's categorical statement that ''the CIP Reliability Standards will not have a significant economic impact on a substantial number of small entities.''

790. According to APPA/LPPC, approximately 293 of the 326 public power systems included on the NERC compliance registry meet the SBA definition of a small electric utility.[205] Therefore, APPA/LPPC argue that the proposed regulations will have an impact on a substantial number of small entities. They maintain that the question is how significant that impact will in fact be. APPA/LPPC believe that some of these small entities will incur significant economic costs to comply with the CIP Reliability Standards.[206]

791. Despite these reservations, APPA/ LPPC believe that the broad contour of the rule contemplated by the CIP NOPR, subject to the changes they request in comments, satisfies the requirements of the RFA. APPA/LPPC state that they recognize that CIP Reliability Standards are necessary to ensure the reliable operation of the Bulk-Power System. While NERC's proposed standards will place the burden on many small entities to identify critical assets and critical cyber assets, this approach is far superior to a top-down approach to asset classification. Assuming small entities do have critical assets and critical cyber assets, they will have to take on significant burdens and incur significant costs to protect their critical cyber assets. However, APPA/LPPC state that NERC's proposed timeline for the implementation plan appears feasible. Moreover, they state that joint action agencies and other similar organizations may form joint registration organizations that accept compliance responsibilities for their members or provide compliance services to their members.

792. Arkansas Electric fully supports the comments submitted in this docket by NRECA. Arkansas Electric argues that, throughout the CIP NOPR, the Commission proposes significant changes to the Reliability Standards which will increase the amount of effort and expense required to comply. Arkansas Electric is concerned that the costs of these additional resources will be especially high for small entities, when viewed in a relative sense. Arkansas Electric is concerned that, even with the friendly tone that some state regulators have taken toward rate recovery for cyber security-related expenses, these dollars would still come from its members. Arkansas Electric

[203] CIP NOPR at P 347.

[204] We discuss issues concerning jointly-owned facilities in section II.F.3.d above.

[205] The APPA/LPPC estimate is based on a comparison of public power systems listed on the NERC compliance registry as of September 2007 with Energy Information Administration Form 861 data for 2005 MWh sales to ultimate customers and sales for resale. The Commission estimates that ''the CIP Reliability Standards will apply to approximately 632 small entities, consisting of 12 small investor-owned utilities and 620 small municipals and cooperatives.''

[206] For example, APPA/LPPC state that many small distribution utilities with fewer than 50 employees may nonetheless own and operate 20 MVA generators. Many of these generators were constructed prior to the industry's adoption of a modern information technology infrastructure. A rigid implementation of the ''technical feasibility'' exception discussed above may lead to directives to adopt remediation plans that bring these units up to current industry standards. However, the costs required to retrofit such facilities to meet new cyber-security requirements may well force the owners to retire many of these units instead. APPA/LPPC at 30.

respectfully asks the Commission to keep cooperatives and small entities in mind as it proposes changes to the CIP Reliability Standards. The resources available within such organizations to comply with the Reliability Standards are often quite limited.

793. California Cogeneration and Energy Producers argue that the eight cyber security Reliability Standards will impose significant new compliance costs on registered entities to the extent they identify critical cyber assets, under CIP–002–1. They suggest that the Commission should direct the ERO to develop pro forma models of protocols and methodologies to be used by entities to facilitate compliance. California Cogeneration submits that pro forma protocols could help mitigate the costs of compliance with the requirements of Reliability Standards CIP–003–1 through CIP–009–1. California Cogeneration points out that the CIP NOPR suggested that groups of entities could collaborate to reduce compliance costs; California Cogeneration argues that this approach could be expanded to include a formal role for NERC.

794. To maximize the effectiveness and the focus of the Reliability Standards, Energy Producers argues that NERC should revisit the NERC Functional Model to include a qualifying facility (QF) category so that Reliability Standards specific to QFs can be developed to account for their unique operating characteristics. To ensure that the regulations effectively promote reliability while not imposing unreasonable costs, Energy Producers argues that the regulations should provide a rigorous definition of critical cyber assets. Such rigor would be provided, first, by retaining the definitions contained in the current draft of the regulations, and second, by providing greater specificity to the risk-based assessment required in CIP–002–1.

795. Iowa Municipals is concerned about the impact that the CIP Reliability Standards will have on smaller entities. While it is true that smaller entities can provide a cyber gateway to larger entities, and many smaller entities will be excluded through the identification of critical cyber assets, it is equally true that some smaller entities will, nonetheless, be subjected to the CIP Reliability Standards. The CIP NOPR pays insufficient attention to supporting compliance by smaller entities. Iowa Municipals makes some suggestions that will assist the Commission to enable smaller entities to comply with the Reliability Standards.

796. One area in which smaller entities' compliance efforts can be supported is through the self-certification process. Iowa Municipals supports the comments filed by MidAmerican that support a semi-annual certification process. As an enhancement to this process, Iowa Municipals recommends that the Commission require NERC to provide a ''lessons learned'' report to entities within 30 days of the certification deadline. This report has the potential of providing invaluable guidance and assistance to smaller entities.

797. Iowa Municipals also urges the Commission to support smaller entities' compliance efforts by providing either a longer compliance timetable, or providing temporary waivers upon an adequate showing of work to attain compliance. Further, Iowa Municipals suggests that compliance by smaller entities can be promoted by allowing smaller entities to walk in the footsteps of larger entities and reach compliance more quickly by taking advantage of lessons learned by others. Iowa Municipals also argues that following such a better path to compliance by smaller entities should ultimately provide a higher level of system protection.

798. The Southwest TDUs state that the CIP NOPR seems to be of two minds on how the impact of the CIP Reliability Standards might be addressed for smaller entities. On the one hand, the Commission proposes that NERC and the Regional Entities help the small entities by providing technical support to identify critical assets. On the other, the Commission acknowledges that these Reliability Standards could be made applicable down to the smallest entity, which appears to discount the economic impact on these entities required to be analyzed by the RFA because cyber security operations may actually be managed by a control area operator or other larger entity. Southwest TDUs argue that just because a larger entity is performing compliance does not mean the costs of compliance are not being passed on to the small entities. Indeed, there is every likelihood that that will be the case. Southwest TDUs maintain that it does not know how onerous a burden small entities face. The Commission must be ready to adjust the CIP requirements, if experience shows that the burden on small entities proves to be onerous.

C. Commission Determination

799. As of October 2007, there are 1,772 registered entities, of which the Commission estimates that approximately 1,400 will be responsible for compliance with the CIP Reliability Standards. Of these, the Commission estimates that the CIP Reliability Standards would apply to approximately 632 small entities, consisting of 12 small investor-owned utilities and 620 small municipal and cooperatives.

800. Arkansas Electric raises concerns with the cost to small entities of the modifications directed by the Commission. These modifications will be made by the ERO through the Reliability Standards development process. Until NERC files any revised Reliability Standards, the Commission cannot estimate their burden on any user, owner or operator of the Bulk-Power System, including small entities. The Commission therefore does not believe it is appropriate to speculate on the cost of compliance with any modified Reliability Standard at this time.

801. The Commission does not believe it is appropriate to grant California Cogeneration's request that NERC develop pro forma models of protocols and methodologies to be used by entities to facilitate compliance. As discussed in the section regarding guidance, that level of detail could potentially introduce common vulnerabilities resulting from all small entities implementing the Reliability Standards using a nearly identical solution. With respect to California Cogeneration's suggestion that NERC should have a formal role in collaborating to reduce compliance costs, the Commission will not direct that at this time. However, NERC should consider providing information to such groups. Further, the Commission believes that requiring the ERO to develop guidance on how to comply with the Reliability Standards should facilitate compliance by small entities.

802. The Commission also declines to direct the ERO to include a QF category in the Functional Model, as requested by Energy Producers. The Commission believes that this request is outside the scope of this rulemaking, which only concerns the CIP Reliability Standards proposed by NERC.

803. The Commission does not believe it is necessary to allow small entities a longer compliance timetable or to provide temporary waivers upon an adequate showing of work to attain compliance. As we stated in the CIP NOPR, the burden to small entities is not great, but the economic impact is justified as necessary to protect cyber security assets that support Bulk-Power System reliability. Further, the Commission believes that allowing small entities to collectively select a

single consultant to develop model software and programs to comply with the CIP Reliability Standard will allow the small entities to take advantage of any information known by larger entities or their consultants.

804. While Southwest TDUs are correct that the Commission acknowledges that the Reliability Standards could be made applicable down to the smallest entity, the Commission disagrees that this discounts the economic impact on these entities. As we stated in the CIP NOPR, to be included in the compliance registry, the ERO will have made a determination that a specific small entity has a material impact on the Bulk-Power System. A small entity placed on the compliance registry could then appeal the determination to the ERO and the Commission.

805. Further, Southwest TDUs argue that just because a larger entity is performing compliance does not mean the costs of compliance are not being passed on to the small entities. We agree; however, in allowing small entities to pool their resources and select a single consultant to develop model software and programs, each entity need not separately fund model software and programs development. Rather, that cost can be spread over several entities.

806. For the reasons stated in the CIP NOPR and above, the Commission certifies that this rule will not have a significant economic impact on a substantial number of small entities. Accordingly, no regulatory flexibility analysis is required.

VI. Document Availability

807. In addition to publishing the full text of this document in the **Federal Register**, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the Internet through FERC's Home Page (*http://www.ferc.gov*) and in FERC's Public Reference Room during normal business hours (8:30 a.m. to 5 p.m. Eastern time) at 888 First Street, NE., Room 2A, Washington, DC 20426.

808. 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.

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

VII. Effective Date and Congressional Notification

810. This Final Rule is effective April 7, 2008. The Commission has determined, with the concurrence of the Administrator of the Office of Information and Regulatory Affairs of OMB, that this rule is a ''major rule'' as defined in section 351 of the Small Business Regulatory Enforcement Fairness Act of 1996.[207] The Commission will submit the Final Rule to both houses of Congress and to the General Accountability Office.

List of Subjects in 18 CFR Part 40

Administrative practice and procedure, Electric power, Penalties, Reporting and recordkeeping requirements.

By the Commission.

Nathaniel J. Davis, Sr.,

Deputy Secretary.

[FR Doc. E8–1317 Filed 2–6–08; 8:45 am]

BILLING CODE 6717–01–P

[207] *See* 5 U.S.C. 804(2) (2007).