DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

18 CFR Part 39

[Docket No. RM06–22–000]

Mandatory Reliability Standards for Critical Infrastructure Protection

July 20, 2007.

AGENCY: Federal Energy Regulatory Commission, Department of Energy.

ACTION: Notice of proposed rulemaking.

SUMMARY: Pursuant to section 215 of the Federal Power Act (FPA), the Federal Energy Regulatory Commission (Commission), proposes to approve 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 proposes to direct NERC to develop modifications to the CIP Reliability Standards to address specific concerns identified by the Commission. Approval of these standards will help protect the nation's Bulk-Power System against potential disruptions from cyber attacks.

DATES: Comments are due October 5, 2007.

ADDRESSES: You may submit comments, identified by docket number by any of the following methods:

- *Agency Web Site: http://ferc.gov.* Follow the instructions for submitting comments via the eFiling link found in the Comment Procedures section of the preamble.
- *Mail/Hand Delivery:* Commenters unable to file comments electronically must mail or hand deliver an original and 14 copies of their comments to the Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE., Washington, DC 20426.

Please refer to the Comment Procedures section of the preamble for additional information on how to file paper comments.

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.

Paul Silverman (Legal Information), Office of the General Counsel, Federal Energy Regulatory Commission, 888 First Street, NE., Washington, DC 20426, (202) 502–8683.

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

Jan Bargen (Technical Issues), Office of Energy Markets and 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.

1. Pursuant to section 215 of the Federal Power Act (FPA), the Commission proposes to approve 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.[1] In

[1] In the context of the CIP Reliability Standards, cyber assets are programmable electronic devices

addition, pursuant to section 215(d)(5) of the FPA, the Commission proposes to direct NERC to develop modifications to the CIP Reliability Standards to address specific concerns identified by the Commission.

I. Background

A. EPAct 2005 and Mandatory Reliability Standards

2. On August 8, 2005, the Electricity Modernization Act of 2005, which is Title XII, Subtitle A, of the Energy Policy Act of 2005 (EPAct 2005), was enacted into law.[2] EPAct 2005 adds a new section 215 to the FPA, which 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. On February 3, 2006, the Commission issued Order No. 672, implementing section 215 of the FPA.[4] Pursuant to Order No. 672, the Commission certified one organization, NERC, as the ERO.[5] The Reliability Standards developed by the ERO and approved by the Commission will apply to users, owners and operators of the Bulk-Power System, as set forth in each Reliability Standard.

4. Pursuant to section 215(d)(2) of the FPA and § 39.5(c) of the Commission's regulations, the Commission is required to give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard or to a Regional Entity organized on an Interconnection-wide basis with respect to a proposed Reliability Standard or a proposed modification to a Reliability Standard to be applicable within that Interconnection.[6]

5. The ERO must file with the Commission each new or modified Reliability Standard that it proposes to be made effective under section 215 of the FPA. The Commission can then approve or remand the Reliability Standard. The Commission also can, among other actions, direct the ERO to modify an approved Reliability Standard to address a specific matter if it considers this appropriate to carry out section 215 of the FPA.[7] Only Reliability Standards approved by the Commission will become mandatory and enforceable.

6. 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 action related to these Reliability Standards.[8]

B. Development of CIP Reliability Standards

7. In August 2003, NERC approved the Urgent Action 1200 standard, which was the first comprehensive cyber security standard for the electric industry. This voluntary standard applied to control areas (*i.e.*, balancing authorities), transmission owners and operators, and generation owners and operators that perform defined functions. Specifically, it established a self-certification process relating to the security of system control centers of the applicable entities. The Urgent Action 1200 standard 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.

8. On August 28, 2006, NERC submitted to the Commission for approval the following eight proposed 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 an 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 risk-based assessment 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.

9. NERC stated that these Reliability Standards provide a comprehensive set of requirements to protect the Bulk-Power System from malicious cyber attacks.[10] They require Bulk-Power System users, owners, and operators to establish a risk-based vulnerability assessment methodology and use that 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,

---

and communication networks including hardware, software, and data. *See* note 69, *infra*.

[2] Energy Policy Act of 2005, Pub. L. No. 109–58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005), *to be codified* at 16 U.S.C. 824o.

[3] 16 U.S.C. 824o(e)(3).

[4] *Rules Concerning Certification of the Electric Reliability Organization; Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards,* Order No. 672, 71 FR 8662 (Feb. 17, 2006), FERC Stats. & Regs. ¶ 31,204 (2006), *order on reh'g,* Order No. 672–A, 71 FR 19814 (Apr. 18, 2006), 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), *order on compliance,* 118 FERC ¶ 61,030 (2007) (Jan. 2007 Compliance Order), *appeal docket sub nom. Alcoa, Inc.* v. *FERC,* No. 06–1426 (D.C. Cir. Dec. 29, 2006).

[6] 18 CFR 39.5(c)(1), to be codified at 16 U.S.C.824o.

[7] Section 215(d)(5) of the FPA.

[8] *Mandatory Reliability Standards for the Bulk-Power System,* Order No. 693, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007); *reh'g pending.*

[9] The proposed Reliability Standards are not proposed to be codified in the CFR and are not attached to the NOPR. 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/filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection.*

[10] NERC Filing at 24.

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 explained that, because of the expanded scope of facilities and entities covered by the eight CIP Reliability Standards, and the investment in security upgrades required in many cases, NERC has also developed an implementation plan that provides for a three-year phase-in to achieve full compliance with all requirements.[11]

10. Each proposed 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 NOPR, these section titles are capitalized when referencing a designated provision of a Reliability Standard.

C. CIP Assessment

11. On December 11, 2006, the Commission released a ''Staff Preliminary Assessment of the North American Electric Reliability Corporation's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection'' (CIP Assessment). The CIP Assessment identified staff's preliminary observations and concerns regarding the eight proposed CIP Reliability Standards. The CIP Assessment described issues common to a number of the proposed CIP Reliability Standards. It also reviewed and identified issues regarding each individual CIP Reliability Standard but did not make specific recommendations regarding the appropriate action on a particular proposal.

12. Comments on the CIP Assessment were due by February 12, 2007. Entities that filed comments are listed in Appendix A to this NOPR.

II. Discussion

A. General Issues

1. Cyber Security Challenges

13. The CIP Reliability Standards represent the most thorough attempt to date to address cyber security issues that relate to the Bulk-Power System. For many years the control systems for the Bulk-Power System have operated in a stand-alone environment without computer or communication links to an external Information Technology (IT) infrastructure. However, over recent years, such stand-alone enclaves have been increasingly connected to both the corporate environment and the external world.

14. Modern computer and communication network interconnection brings with it the potential for cyber attacks on these systems. These concerns become particularly critical when several entities come under attack simultaneously. The CIP Assessment identified ''defense in depth'' as a widely recognized strategy to address cyber threats. Defense in depth involves the layering of various defense mechanisms in a way that either discourages an adversary from continuing an attack or aids in early detection of cyber threats.

15. A major challenge to preserving system protection is that changes occur rapidly in system architectures, technology, and threats. As a result, cyber security strategies must comprise a layered, interwoven approach to vigilantly protect the Bulk-Power System against evolving cyber security threats.

16. Cyber security involves a careful balance of the technologies available with the existing control equipment and the functions they perform. Cyber security does have purely technical components, which consist of the various available technologies to defend computer systems. The task of balancing technical options comes into play as one selects and combines the various available technologies into a comprehensive architecture to protect the specific computer environment.

17. A key to the successful cyber protection of the Bulk-Power System will be the establishment of CIP Reliability Standards that provide sound, reliable direction on how to choose among alternatives to achieve an adequate level of security, and the flexibility to make those choices. This conclusion is consistent with the lessons learned from the August 2003 blackout occurring in the central and northeastern United States. The identification of the causes of that and other previous major blackouts helped determine where existing Reliability Standards need modification or new Reliability Standards need to be developed to improve Bulk-Power System reliability. The U.S.—Canada Power System Blackout Task Force, in its Blackout Report, developed specific recommendations for the improving the then-current voluntary standards and development of new Reliability Standards.[12]

18. Thirteen of the 46 Blackout Report Recommendations relate to cyber security. They address topics such as the development of cyber security policies and procedures; strict control of physical and electronic access to operationally sensitive equipment; assessment of cyber security risks and vulnerability at regular intervals; capability to detect wireless and remote wireline intrusion and surveillance; guidance on employee background checks; procedures to prevent or mitigate inappropriate disclosure of information; and improvement and maintenance of cyber forensic and diagnostic capabilities.[13] The proposed CIP Reliability Standards address these and related topics.

19. As we noted in Order No. 693, the Blackout Report recommendations address key issues for assuring Bulk-Power System reliability and represent a well-reasoned and sound basis for action.[14] Likewise, in this NOPR, the Commission recognizes the merits of specific Blackout Report recommendations as a basis for proposing certain modifications to the eight CIP Reliability Standards that the Commission proposes to approve.

20. We recognize that the guidance and directives in the cyber security Reliability Standards themselves must also strike a reasonable balance. If the provisions are overly prescriptive they tend to become a ''one size fits all'' solution, which does not suit this environment, where systems vary greatly in architecture, technology, and risk profile. However, if Reliability Standards lack sufficient detail, they will provide little useful direction, thereby making compliance and enforcement difficult, allow flawed implementation of security mechanisms, and result in inadequate protection. The Commission will evaluate the proposed CIP Reliability Standards in the context of the above over-arching considerations.

2. Applicability

21. The Applicability section of each proposed CIP Reliability Standard identifies the following 11 categories of responsible entities that must comply

[11] I*d.* at 24: Exhibit B (Implementation Plan for Cyber Security Standards).

[12] 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*.

[13] *See* Blackout Report at 163–169, Recommendations 32–44.

[14] *See* Order No. 693 at P 234.

with the Reliability Standard: reliability coordinators, balancing authorities, interchange authorities, transmission service providers, transmission owners, transmission operators, generator owners, generator operators, load serving entities, NERC, and Regional Reliability Organizations.

22. The CIP Assessment raised two issues regarding applicability of the CIP Reliability Standards. First, it stated that, although it is likely that NERC and the Regional Entities [15] are not directly subject to mandatory Reliability Standards, their compliance with the CIP Reliability Standards is important to the extent that they have cyber communications with users, owners or operators of the Bulk-Power System.[16] The CIP Assessment suggested that NERC and Regional Entity compliance could be required pursuant to NERC's Rules of Procedure. Some commenters pointed out that NERC out-sources critical application systems that are relied upon by many responsible entities, such as the Interchange Distribution Calculator, and suggest that the out-source provider should be contractually compelled to comply with the CIP Reliability Standards, with NERC ultimately responsible for non-compliance.[17]

23. Second, the CIP Assessment raised concerns about the appropriateness of a size threshold, below which small entities would be exempt from compliance. It explained that, while the assets and operations of a smaller entity may not have a major day-to-day operational impact on the Bulk-Power System, such an entity can provide a cyber gateway to compromise larger users, owners, or operators of the Bulk-Power System. When attacked simultaneously with the facilities of other small entities, the aggregate result could have an adverse impact on the reliability of the Bulk-Power System. Thus, the CIP Assessment suggested that a key to any determination of whether an entity should be subject to the CIP Reliability Standards is whether or not it is a user, owner, or operator of the Bulk-Power System and whether it has a cyber connection to other users, owners or operators of the Bulk-Power System. The CIP Assessment concluded that the CIP Reliability Standards should apply to all users, owners, or operators regardless of size, because a relatively small entity could have critical importance from a cyber security perspective.

24. A number of commenters stated that the focus should be on those entities that own or operate critical assets, rather than being addressed in terms of ''large'' or ''small'' size of entities.[18] These commenters warn that a blanket waiver that uniformly exempts small entities from compliance with certain provisions of the proposed CIP Reliability Standards therefore would not be appropriate. NERC and other commenters maintain that applicability should not be determined based on cyber connections but, rather by identifying those users, owners and operators of the Bulk-Power System that own or operate critical assets and associated critical cyber assets. Another group of commenters urge that the Commission not impose the same compliance obligations on smaller entities as on larger entities when a violation by the smaller entity would not have a critical impact on the Bulk-Power System. They maintain that adverse impacts on the grid from small entities would be an uncommon occurrence and urge a case-by-case approach to granting waivers from compliance with the CIP Reliability Standards.[19]

Commission Proposal

25. 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.[20] Similarly, 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.[21] The Commission believes that this approach is sufficient and, accordingly, does not propose any additional measures or revisions on this issue.

26. The Commission's determinations in Order No. 693 are relevant to deciding the applicability of the CIP Reliability Standards to small entities. In Order No. 693, the Commission approved NERC's compliance registry process as a reasonable means ''to ensure that the proper entities are registered and that each knows which Commission-approved Reliability Standard(s) are applicable to it.'' [22] Further, the Commission approved NERC registry criteria that identify specific categories of users, owners and operators of the Bulk-Power System and criteria for registering entities within each of the categories.[23]

27. The Commission will also rely on the NERC registration process to determine applicability with the CIP Reliability Standards. In other words, an entity would be responsible to comply with the CIP Reliability Standards if the entity is (1) registered by NERC under one or more functional categories and (2) within a functional category for which the entity is registered as identified in the Applicability section of the CIP Reliability Standards. However, even though it is the Commission's present intention to rely on the NERC registration process to identify appropriate entities, we remain concerned about the possibility of entities not identified by the registration process becoming a weakness in the security of the Bulk-Power System. In this regard, we note that, in Order No. 693, the Commission explained that, ''if there is an entity that is not registered and NERC later discovers that the entity should have been subject to the Reliability Standards, NERC has the ability to add the entity, and possibly other entities of a similar class, to the registration list * * *.'' [24] In addition, in Order No. 693, the Commission indicated that it would further examine applicability issues under section 215 of the FPA in a future proceeding, and notes the same intention here.[25]

28. Regarding our concern about small entities becoming a gateway for cyber attacks, some commenters argue that the Commission should not focus on cyber connections to determine applicability of the CIP Reliability Standards. Others state that it would be uncommon for a small entity to cause an adverse impact upon the grid. The Commission's reliance upon the NERC registration process to determine the applicability of the CIP Reliability Standards is in part based upon our expectation that industry will use the ''mutual distrust'' posture discussed below regarding CIP–

[15] In Order No. 693, at P 157, the Commission directed NERC to remove all references to the Regional Reliability Organization and replace them with a reference to the Regional Entity where appropriate. This directive should apply to the CIP Reliability Standards as well.

[16] *See* CIP Assessment at 12–14.

[17] *E.g.,* ISO–NE, ISO/RTO Council, and SPP.

[18] *E.g.,* Allegheny, California PUC, EEI, Georgia System, ISO–NE, MidAmerican, NERC, ReliabilityFirst, Northeast Utilities, NRECA, Ontario IESO, Tampa Electric, and Xcel.

[19] *E.g.,* APPA/LPPC and Santa Clara.

[20] *See* NERC Rules of Procedure, section 100.

[21] *See North American Electric Reliability Corp.*, 119 FERC ¶ 61,060 at P 4–5 (2007) (approving the delegation agreements and directing certain modifications).

[22] Order No. 693 at P 92, *quoting ERO Certification Order*, 116 FERC ¶ 61,062 at P 689.

[23] Order No. 693 at P 93–95. NERC's Statement of Compliance Registry Criteria (Revision 3), approved by the Commission in Order No. 693, is available on NERC's Web site at: *ftp://www.nerc.com/pub/sys/all_updl/ero/Statement_of_Compliance_Registry_Criteria_Rev3.pdf.*

[24] Order No. 693 at P 97.

[25] *Id.* at P 77.

003–1. The term ''mutual distrust'' is used to denote how these ''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.

29. Similarly, the Commission is relying on the NERC registration process to include all critical assets and associated critical cyber assets. For example, if assets are important to the reliability of the Bulk-Power System, such as black start units, we would expect that the NERC registration process would identify the owners or operators of those units as critical, and require them to register, even though the facilities may be ''smaller'' or at low voltages. 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.

30. As discussed later, as an initial compliance step, each entity that is responsible for compliance with the CIP Reliability Standards must identify critical assets through the application of a risk-based assessment as required by CIP–002–1. Whether that entity must comply with the remainder of the requirements in the CIP Reliability Standards would depend on the outcome of that assessment and the subsequent identification of critical cyber assets, also required by CIP–002–1. Thus, CIP–002–1 acts as a filter, determining which entities must comply with the remaining CIP requirements (*i.e.*, CIP–003–1 through CIP–009–1).

31. The Commission agrees with the commenters that access to information essential to the operation of critical cyber assets by out-sourced entities that are not otherwise subject to the CIP Reliability Standards presents a potential vulnerability to the Bulk-Power System. We understand that, on occasion, NERC negotiates contracts with such 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 invites comment on whether and how such out-sourced entities should be contractually obligated to comply with the CIP Reliability Standards while satisfying their other contractual obligations.

3. Compliance Measured by Outcome

a. Performance-Based Standards

32. The CIP Assessment expressed concern that the lack of specificity within the proposed CIP Reliability Standards could result in inadequate implementation efforts and inconsistent results.[26] NERC, along with a number of other commenters, states that the CIP Reliability Standards are not prescriptive, positing that the level of specificity they embody is appropriate. NERC explains that the use of a performance-based structure frames the CIP Reliability Standards in terms of required results or outcomes with criteria for verifying compliance, but without prescribing the methods for achieving the required results. In other words, the specific means to achieve that outcome are left to the discretion of the responsible entity. Such an approach contrasts with a prescribed or design-based standard. NERC concludes that, when taken together, the proposed Reliability Standards constitute a comprehensive set of cyber security activities, stating that it is more important that a pre-defined, desirable outcome is achieved than prescribing the means to that end.

33. The Commission generally agrees that use of performance-based standards is a part of the design of cyber security safeguards for the Bulk-Power System's critical assets. However, as we indicated in Order No. 672, 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.'' [27] Accordingly, where necessary, the Commission proposes to direct NERC to modify the CIP Reliability Standards to address the ''how.'' Moreover, the Commission is concerned that, while NERC explains that the CIP Reliability Standards are performance-based, the CIP Reliability Standards do not provide a mechanism to measure performance or otherwise determine whether a responsible entity has met the goals of a particular requirement set forth in the standards.

34. The Commission believes that monitoring the performance of responsible entities identified in the CIP Reliability Standards involves three strategies. First, it is important that there be both internal and external oversight of the responsible entity's activities. While the proposed Reliability Standards embody internal management oversight strategies, there should also be oversight that embodies a wide-area view. Second, when flexibility is exercised in a way that excepts an entity from a Requirement, such action should be monitored, documented, and periodically revisited to determine consistency and effectiveness of the implementation. Third, reporting certain wide-area information and analysis to the Commission is vital to its role in ensuring that approved CIP Reliability Standards achieve on an ongoing basis an adequate level of cyber security protection to the Bulk-Power System. These three strategies are applied in our discussion below of various provisions of the CIP Reliability Standards.

b. Adequacy of Outcomes

35. The CIP Assessment explained that many of the Requirements in the proposed CIP Reliability Standards consist of broad directives, and that the Measures and Compliance provisions focus largely on proper documentation. The Reliability Standards themselves do not explain the interplay between the Requirements, on one hand, and the Measures and Levels of Non-Compliance, on the other.

36. The CIP Assessment expressed the view that the focus of the Measures and Compliance provisions on documentation could be interpreted to suggest that possession of documentation can demonstrate compliance, regardless of the quality of its contents. It suggested that compliance with the CIP Reliability Standards must be understood in terms of compliance with the Requirements, which, according to NERC, define what an entity must do to be compliant and establishes an enforceable obligation.

Comments

37. NERC and others do not share the CIP Assessment concern regarding the focus on documentation.[28] NERC and ReliabilityFirst acknowledge the extensive use of documentation throughout the CIP Reliability Standards, but note that the majority of this documentation is used to demonstrate that the Requirements have been met. NERC indicates that, while the ''mere possession of documentation'' does not guarantee compliance, appropriate documentation is essential to demonstrate that steps to comply with the Requirements have been taken and will streamline after-the-

[26] CIP Assessment at 3.

[27] Order No. 672 at P 260. The Commission also explained that, for some Reliability Standards, ''leaving out implementation features could [*inter alia*] sacrifice necessary uniformity in implementation * * *''.

[28] *E.g.,* ReliabilityFirst, APPA/LPPC, and SPP.

fact compliance audits. Similarly, EEI believes that the quality of the documentation is an important factor for assessing compliance and should be the subject of an audit. FirstEnergy and Santa Clara state that it would be helpful for NERC to provide guidance on what constitutes reasonable documentation.

38. Others raise concerns regarding the emphasis on documentation. For example, Duke Energy agrees with the CIP Assessment that the CIP Reliability Standards rely heavily on documentation to verify compliance. Duke Energy believes that the accumulation of documentation to facilitate audits may prove to be less than optimum for the CIP Reliability Standards and suggests that efforts to improve the CIP Requirements should gradually focus less on documentation, and more on the actual level of cyber security to be implemented by the responsible entity. ISA Group states that the CIP Reliability Standards do not specify clear Requirements and do not provide sufficient guidance. ISA Group believes that the clarity and detail of the Levels of Non-Compliance in terms of documentation give the impression that the documentation is the focus of the CIP Reliability Standards.

Commission Proposal

39. The Commission agrees with NERC that, while documentation is necessary, the documentation by itself does not satisfy the Requirements of a Reliability Standard. Rather, implementation of the substance of the Requirements is most important in determining compliance. As we explained in Order No. 693, ''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 circumstances of its use, ownership or operation of the Bulk-Power System.'' [29] Moreover, the Commission recognized that:

> The most critical element of a Reliability Standard is the Requirements. As NERC explains, ''the Requirements within a standard define what an entity must do to be compliant * * * [and] binds an entity to certain obligations of performance under section 215 of the FPA.'' If properly drafted, a Reliability Standard may be enforced in the absence of specified Measures or Levels of Non-Compliance.[30]

40. To reiterate, while documentation set forth in the Measures and Levels of Non-Compliance plays an important role in assuring that a responsible entity is able to demonstrate to an auditor or others that it has complied with the substantive Requirement of a Reliability Standard, adequate documentation does not substitute for substantive compliance with the obligations and responsibilities set forth in the Requirement.

41. Related, certain Requirements of the CIP Reliability Standards obligate a responsible entity to develop and maintain a plan, policy or procedure. However, such Requirements do not always explicitly require implementation of the plan, policy or procedure.[31] The Commission interprets such provisions to include an implicit requirement to implement the plan, policy or procedure; and to make a responsible entity subject to a non-compliance action for failing to implement the policy. Such an interpretation is reasonable to prevent the scenario in which the ERO, Regional Entity or the Commission could assess a penalty against a responsible entity for failure to develop a plan, policy or procedure that satisfies the Requirements of the Reliability Standard, but unable to assess a penalty against a responsible entity that has developed an adequate plan but fails to implement it. Further, the Commission proposes that the ERO, in developing modifications to the CIP Reliability Standards, include explicitly in such Requirements that a responsible entity must implement a plan, policy or procedure that it is required to develop.

4. Implementation Plan

42. Unlike the Reliability Standards approved in Order No. 693, which NERC formulated based on existing voluntary standards, the CIP Reliability Standards are new and require applicable entities in many cases to develop new cyber security systems and procedures, which will take time to develop and implement. To address this task, NERC developed an implementation plan that includes a proposed four-stage schedule for implementing the proposed CIP Reliability Standards over a three-year period.[32]

43. 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 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.

44. According to the implementation plan, ''auditably compliant'' must be achieved in 2009 for certain Requirements by certain responsible entities, and in 2010 for the remainder.

CIP Assessment

45. The CIP Assessment suggested that it may be possible to assess a responsible entity's level of compliance prior to the time when it achieves its ''auditably compliant'' status. It noted that, if a responsible entity is in the ''begin work'' phase, it has: (1) Developed and approved a plan to address the Requirements of a Reliability Standard; (2) identified and planned for necessary resources; and (3) begun implementing the Requirements. These are specific steps that an audit can examine. The CIP Assessment observed that the difference between the ''compliant'' and ''auditably compliant'' status for many of the Requirements is the accumulation of 12 months of compliance records. It sought comment on whether it would be beneficial to audit a responsible entity at the ''begin work'' and ''compliant'' stages, even though the responsible entity may not have the full 12 month accumulation of compliance records.

Comments

46. A number of commenters agree that some type of assessment, although not necessarily in the form of an audit, is both possible and potentially beneficial prior to the time an entity achieves ''auditably compliant'' status.[33] NERC agrees that there is a benefit to ensuring that responsible entities are moving timely toward ''auditably compliant'' status. While NERC believes that audits at an interim stage are not possible, it states that it plans to monitor progress through self-certification without assessing penalties. Other commenters oppose interim audits, stating that they could interfere with implementation plans and lead to penalties for non-compliance.[34]

[29] Order No. 693 at P 253.

[30] *Id., quoting* NOPR at P 105 (footnote omitted).

[31] *See, e.g.*, CIP–006–1, Requirement R1 (requiring a responsible entity to ''create and maintain a 'physical security plan' ''); *cf.* CIP–003–1, Requirement R1 (requiring a responsible entity to ''document and implement a cyber security policy'').

[32] NERC August 28, 2006 Filing, Exhibit B ''Implementation Plan for Cyber Security Standards'' (Implementation Plan).

[33] *E.g.,* Santa Clara, SPP, APPA/LPPC, NERC, Allegheny, Georgia Operators, ISO RTO Council, MidAmerican, SoCal Edison, and NRECA.

[34] *E.g.,* ATC, EEI, National Grid, Tampa Electric, and FirstEnergy.

Commission Proposal

47. The Commission proposes to approve NERC's Implementation Plan, including the proposed timelines for achieving compliance. NERC indicates that the proposed timelines were developed with input from all sectors of the electric industry. Further, while some responsible entities have already installed the necessary equipment and software to address cyber security, the Commission recognizes that many responsible entities must purchase and install new equipment and software to achieve compliance. Based on these considerations, the Commission believes that the timetable proposed by NERC sets reasonable deadlines for industry compliance.

48. However, the Commission is concerned whether the industry will be fully prepared for compliance upon reaching the implementation deadline and will take reasonable action to protect the Bulk-Power System during this interim period. The Commission believes that NERC's plans to require self-certification during the interim period are helpful. NERC, however, does not indicate the interval for self-certification. We believe that an annual certification would not allow adequate monitoring of progress and propose to direct that the ERO develop a self-certification process with more frequent certifications, either tied to target dates in the schedule or perhaps quarterly or semi-annual certifications. While we agree with NERC that 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, 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.

49. To further address our concerns about the period prior to when responsible entities achieve full compliance with the CIP Reliability Standards, the Commission also proposes to direct the ERO to add a cyber security assessment to NERC's existing readiness reviews. In this readiness assessment process, the ERO should assist in the identification of best practices and deficiencies of the reviewed entities, both to help them prepare for implementation of the CIP Reliability Standards and to assess the status of their compliance efforts. The readiness reviews will also help the Commission to evaluate the potential effectiveness of the cyber security Reliability Standards before they are implemented by disclosing the progress made by reviewed entities in their CIP Reliability Standards implementation efforts.

5. Issues Presented by Terminology

a. Business Judgment

NERC Proposal

50. 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.

Each of the subsequent CIP Reliability Standards includes a statement that ''Responsible Entities should interpret and apply the Reliability Standard using reasonable business judgment.''

51. NERC's Glossary of Terms Used in Reliability Standards (NERC glossary) does not define the term ''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.[35] 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 suggests that this history is relevant to the use of this rule in the context of the CIP Reliability Standards. The document goes on to say:

> Courts 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. A common formulation indicates the business judgment of an entity—even if incorrect in hindsight—should not be overturned as long as it was made (1) in good faith (not an abuse or indiscretion), (2) without improper favor or bias, (3) using reasonably complete (if imperfect) information as available at the time of the decision, (4) based on a rational belief that the decision is in the entity's business interest. This principle, however, does not protect an entity from simply failing to make a decision.

CIP Assessment

52. The CIP Assessment acknowledged the importance of flexibility and discretion in implementing cyber security strategies. However, it expressed skepticism about the appropriateness of the business judgment rule in this context, given the unusually broad discretion it permits. The CIP Assessment thus expressed concern that such an approach to flexibility and discretion would unduly compromise the effectiveness of the CIP Reliability Standards and the ability to enforce compliance with them.

53. The CIP Assessment sought comment on: (1) Specific examples of the differing roles of entities in relationship to their potential impact on cyber security risks to Bulk-Power System reliability; (2) alternatives to reliance on the reasonable business judgment rule that would allow for recognition of differing roles of entities, vulnerability of assets, and exposure to risk but also permit effective enforcement of the CIP Reliability Standards; and (3) the ramifications of removing the ''reasonable business judgment'' language from the proposed CIP Reliability Standards while an alternative approach is developed using the ERO's Reliability Standards development process.

Comments

54. A number of commenters stress the importance of flexibility and discretion in implementing the CIP Reliability Standards, but agree that it would not be reasonable to give the term ''business judgment'' the meaning it has in the context of corporate fiduciary responsibility.[36] Other commenters state that the use of reasonable business judgment was not meant to allow entities to evade application of the CIP Reliability Standards, but they acknowledge that legal precedent

[35] 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*.

[36] *E.g.*, California PUC, APPA/LPPC, EPSA, and Progress Energy.

suggests that inclusion of the term could increase the potential for disputes.[37] These commenters support the use of alternative terms to acknowledge the need for flexibility and discretion, such as ''reasonableness,'' ''good utility practice,'' or ''good engineering practices.''

55. Other commenters argue that the ''reasonable business judgment'' language is essential to provide balance in the implementation of the CIP Reliability Standards and should not be removed. Some indicate that use of the term was intended to allow consideration of cost or business implications of an action.[38] For instance, NERC states that, if business considerations are left out of account, the CIP Reliability Standards would describe an impossibly high level of technical content, and the cost of implementing such a solution would approach an infinite amount of time, money, and resources. Commenters also state that use of reasonable business judgment allows every entity the flexibility to make the best choice for its unique situation.[39] Finally, some commenters believe that the term reasonable business judgment will ensure that the CIP Reliability Standards are enforceable by permitting development of a record of industry practices over time that provides a body of reasonable, industry cyber security practices.[40]

56. Some commenters argue that use of the term ''reasonable business judgment'' was not intended to trigger the exculpatory ''business judgment rule'' as used in connection with the actions of corporate directors.[41] They contend the term was intended as a ''reasonableness'' standard that was meant to add a defined and objective measure for assessing an entity's actions in implementing the CIP Reliability Standards based on the entity's particular system and assets. EEI argues that while the NERC FAQ accurately describes traditional use of the reasonable business judgment rule in the context of corporate law, it does not articulate how this language is being used in the context of cyber security standards. EEI also states that it is unlikely that the FAQ document would control interpretation of the CIP Reliability Standards.

57. Finally, some commenters acknowledge that the traditional corporate business judgment rule does grant officers and directors broad discretion, but also contains elements that temper this discretion.[42] To receive the benefit of the rule, a business decision must be made on an informed basis, in good faith and in honest belief that the action taken was in the best interests of the company. In addition, the person making the decision must act with the care that an ordinarily prudent person would reasonably be expected to exercise in a like position with similar circumstances. The commenters argue that these requirements permit the term reasonable business judgment to be adapted to the cyber security context.

Commission Proposal

58. For the reasons discussed below, the Commission proposes 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.

59. The Commission agrees with commenters 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 acknowledges that cost can be a valid consideration in implementing the CIP Reliability Standards. However, the Commission believes that the traditional concept of reasonable business judgment is ill suited to the task of implementing an appropriate program of cyber security pursuant to FPA section 215. The concept of reasonable business judgment addresses the issue of whether a decision-making process conforms to certain standards. It 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. As explained below, when transferred to the realm of cyber security or Bulk-Power System reliability generally, recourse to reasonable business judgment is inconsistent with the purpose of FPA section 215.

60. Cyber 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.

61. While some commenters argue that references to reasonable business judgment in the CIP Reliability Standards were not intended to trigger the traditional corporate business judgment rule, the FAQ document can be read to suggest the contrary. In fact, the FAQ document states explicitly that ''reasonable business judgment'' means what the courts have said it means in the corporate context. It states that the phrase has an almost 200 year history in the common law nations and notes 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.'' The FAQ document then goes on to list the elements of reasonable business judgment as the courts generally define it. The FAQ document nowhere states or suggests that the meaning and significance of reasonable business judgment is subject to some modification or qualification in the context of implementing and complying with the CIP Reliability Standards.

62. Moreover, as the FAQ document makes clear, compliance turns on whether a decision was ''based on a rational belief that the decision is in the entity's business interest.'' That test is fundamentally incompatible with Congress' decision to adopt a regime of mandatory Reliability Standards. As we stated above, the vulnerability of one entity can pose risks to the entire grid. We therefore cannot allow each user, owner or operator to determine compliance based on its own parochial business interests. The purpose of section 215 is to protect the national interest in grid reliability.

63. The business judgment rule was adopted in a context that is simply not appropriate for mandatory Reliability Standards. The business judgment rule recognizes that officers and directors

[37] *E.g.*, Duke, Progress Energy, Xcel, and National Grid.

[38] *E.g.*, NERC, Southern, and PG&E.

[39] *E.g.*, NERC, NU, PJM, Santa Clara, and Cleveland Public Power.

[40] *E.g.*, IRC and Tampa Electric.

[41] *E.g.*, Arizona Public Service, EEI, Progress Energy, SoCal, TEC, Duke, ReliabilityFirst and National Grid.

[42] *E.g.*, EEI and Progress Energy.

must have wide latitude if a company is to be managed properly and efficiently and that it is not in the interest of shareholders to create incentives for officers and directors to be overly cautious.[43] Courts have noted that shareholders voluntarily undertake the risk of bad business judgments and investors who are adverse to such risk have alternative investment opportunities available to them.[44] In the context of section 215, however, these principles do not apply. The issue under section 215 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.

64. It is also notable that the business judgment rule is invoked, in the corporate governance context, only in extreme circumstances. Generally, to find an officer or director liable there must be evidence establishing that he or she acted fraudulently, in bad faith, or with gross or culpable negligence.[45] Some cases refer to unconscionable conduct, illegal or oppressive acts, willful abuse of discretionary power or neglect of duty, and recklessness as situations that fall outside reasonable business judgment.[46] While the FAQ document does not explain this point clearly, it does allude to it when it notes that the ''[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*.'' (Emphasis supplied).

65. These criteria are plainly inappropriate for mandatory CIP Reliability Standards. For example, if an inadequate cyber plan caused a grid-wide disturbance or blackout, a violation could be established only in ''extreme circumstances'' where there was ''unconscionable conduct'' or ''recklessness'' or, as discussed above, where the entity's plan was not consistent with its ''own business interest.'' These highly deferential legal standards are not compatible with a mandatory reliability regime under section 215 of the FPA. We therefore propose to direct NERC to delete references to ''reasonable business judgment'' from the CIP Reliability Standards.

66. We wish to stress, however, that, even though we propose to delete the business judgment rule, we believe flexibility in the application of the CIP Reliability Standards remains appropriate. First, as discussed throughout this NOPR, the CIP Reliability Standards contain specific provisions that explicitly permit various alternative courses of action. More importantly, however, the CIP Reliability Standards do not simply allow the exercise of flexibility and discretion, they require it. Even with the various revisions and additions that the Commission is proposing in this NOPR, the CIP Reliability Standards constitute a relatively brief document, and the Requirements it contains are largely performance based. These Requirements for the most part are quite general and do not dictate specific solutions to cyber-security problems. Responsible entities therefore must interpret and apply them to their specific circumstances. The CIP Assessment explained:

> The task of balancing technical options comes into play as one selects and combines the various available technologies into a comprehensive architecture to protect the specific computer environment. The key to success is possessing cyber security standards that provide reliable direction on how to choose among alternatives to achieve an adequate level of security.[47]

67. Based on our careful consideration of this issue as discussed above, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations, the Commission proposes to direct that the ERO modify each of the proposed CIP Reliability Standards to remove references to the ''reasonable business judgment'' language before compliance audits start in 2009.

b. ''Technical Feasibility'' and ''Acceptance of Risk''

68. Two CIP Reliability Standards contain language that provides exceptions from compliance with a Requirement. This language takes two forms: one focuses on technical feasibility, and the other focuses on acceptance of risk.

69. Some provisions require a responsible entity to take action ''where technically feasible.''[48] The NERC glossary does not define the term ''technically feasible,'' and the Reliability Standards themselves do not 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.[49]

Technical feasibility is here related to reasonable business judgment, but only in a situation where equipment is being replaced. Otherwise, the FAQ document treats technical feasibility in terms of objective engineering judgments regarding what is possible with existing equipment.

70. 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.''[50] The Reliability Standards do not provide explicit guidance on the circumstances in which it is appropriate to accept the risk of non-compliance.

CIP Assessment

71. In the discussion of specific Reliability Standards, the CIP Assessment expressed concern about the need to reference technical feasibility, either because the action in question appeared to be clearly technically feasible or because of the extremely limited number of situations in which technical feasibility could become an issue.[51]

72. The CIP Assessment noted that acceptance of risk raised special concern in a cyber environment. Where there are interconnected control systems, an acceptance of a cyber risk by one entity would actually be tantamount to an acceptance of risk on behalf of all entities connected with it because the first entity can serve as a gateway to the others as noted above. The entity that initially accepts the risk

[43] *Cramer* v. *General Telephone and Electronics Corp.*, 582 F.2d 259 (3d Cir. 1978); *Joy* v. *North*, 692 F.2d 880 (2d Cir. 1982).

[44] *Joy* v. *North*, 692 F.2d 880 (2d Cir. 1982).

[45] *In Re Bal Harbour Club, Inc.*, 316 F.3d 1192 (11th Cir. 2003) (*Bal Harbour*); *Froelich* v. *Senior Campus Living LLC*, 355 F.3d 802 (4th Cir. 2004); *Poth* v. *Rassey*, 281 F. Supp. 2d (E.D. Va. 2003) (*Poth* v. *Rassey*).

[46] *Bal Harbour; Poth* v. *Rassey*; *Gray* v. *Manhattan Medical Center, Inc.*, (18 P.3d 291 (Kan. 2001); *G & N Aircraft, Inc.* v. *Boehm*, 743 N.E.2d 227 (Ind. 2001).

[47] CIP Assessment at 8.

[48] 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.

[49] FAQ Document at 1.

[50] *See* CIP–007–1, Requirements R2.3, R3.2, and R4.1.

[51] *See, e.g.*, CIP Assessment at 26–27, 32–33.

becomes a ''weak link'' in the chain. The CIP Assessment noted that there is no provision in the proposed CIP Reliability Standards for oversight or consideration of the broader impacts of risk acceptance in individual cases. It sought comment on the appropriateness of risk acceptance and suggested that, if this concept is appropriate, clear guidance is needed to explain the limited circumstances in which it is appropriate.

Comments

73. NERC states that the term ''technical feasibility'' is intended to be very limited in scope. It defines the term as the physical ability of in-place equipment or software to conform directly to some Requirement in the Reliability Standards or the ability of in-place equipment or software to perform its required function if modified in a way that would most directly conform to some Requirement. The term is used to prevent penalizing responsible entities unnecessarily in situations where they cannot change immediately or prudently to comply with a Requirement. NERC states that where the concept of technical feasibility applies, the responsible entity should document the technical issue and its mitigation plans or strategies.

74. Many commenters [52] emphasize that the phrase ''where technically feasible'' is intended to permit flexibility, to permit the application of the Reliability Standards to a wide variety of situations, and to allow compliance with the Reliability Standards to evolve over time as technologies change. Some commenters note that in many cases it is not feasible to enhance equipment without replacing it. In some cases, off-the-shelf solutions are not available for various parts of the system.

75. ISA Group states that the phrase ''where technically feasible'' could be eliminated entirely from the CIP Reliability Standards and replaced with an exception mechanism that requires a decision to invoke technical feasibility to be explicit and reviewable. The exception mechanism should require that there be alternative mitigation that provides the level of security that would otherwise have been achieved. California PUC argues that the phrase ''technically feasible'' should be removed unless there is a serious question about the actual feasibility of a requirement being imposed.

76. Most commenters support the ''acceptance of risk'' terminology with certain qualifications. NERC states that the concept of risk acceptance recognizes that flexibility and judgment are required to make prudent decisions, but does not allow an entity to do nothing. It also contends that acceptance of risk is a fundamental tenet of an audit process, which recognizes that not all systems or implementations can be perfect. Other commenters state that acceptance of risk is needed to allow for flexibility and that it can be workable if decisions to accept risk are documented, compensating or mitigating action is taken, and decisions to accept risk are transparent and subject to review and oversight.[53] Some commenters state that any invocation of the risk acceptance provision should be subject to a sunset date or plan to achieve compliance.[54] In contrast, Wisconsin Electric states that acceptance of risk could seriously endanger reliability and supports removal of the option to accept risk.

Commission Proposal

77. For the reasons discussed below, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations, the Commission proposes to direct that the ERO: (1) interpret the term ''technical feasibility'' narrowly as applying to the technical characteristics of existing assets and having no relation to the considerations of business judgment discussed above; (2) treat instances where technical feasibility is invoked as exceptions that require certain alternative courses of action; (3) eliminate the ''acceptance of risk'' option from the CIP Reliability Standards; and (4) develop an annual report that quantifies, on a wide-area basis, the frequency with which responsible entities invoke ''technical feasibility'' or other provisions that produce the same outcome. The reason the Commission believes these proposed safeguards are necessary, as well as additional details regarding these proposals, are provided below.

Technical Feasibility

78. The Commission acknowledges that, in the near term, exceptions from compliance based on the concept of ''technical feasibility'' may be appropriate in a limited set of circumstances.[55] However, responsible entities should not be permitted to invoke technical feasibility on the basis of ''reasonable business judgment,'' as NERC's FAQ suggests. We have already discussed the concerns that reasonable business judgment can create for effective cyber security. Nor should a responsible entity be able to except itself unilaterally from a Requirement of a mandatory Reliability Standard with no oversight. Unless invocation of the technical feasibility exception is carefully circumscribed, substantial opportunity for abuse, difficulty in enforcement and the continued allowance of unacceptable reliability risks could result.

79. Therefore, the Commission proposes to require the ERO to establish a structure to require accountability from those who rely on ''technical feasibility'' as the basis for an exception. Such a 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 as provided in CIP–003–1, Requirement R2. 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 proposes 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 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.

80. 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 provision as well as other provisions that function as an exception to the CIP Reliability Standards. The Commission,

[52] *E.g.*, National Grid; ISO/RTO Council; PJM, Ontario IESO, SPP, and ISO–NE.

[53] *E.g.*, Allegheny, MidAmerican and National Grid.

[54] *E.g.*, MidAmerican and Allegheny.

[55] For example, it is understandable that some older ''legacy'' systems are not capable of utilizing certain cyber protection strategies needed to fully comply with the Requirements of these CIP Reliability Standards. In such a case, the responsible entity could be granted an exception upon the satisfactory submittal of a mitigation plan leading to compliance, by a date certain.

therefore, proposes 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. The Commission expects that the report would not provide a level of detail so as to contain critical energy infrastructure information, but would include sufficient information such that it is clear that the mitigation measures have addressed the interim vulnerabilities and the milestone schedules will be sufficient to bring the entities into compliance by a date certain in a timely manner. The report should include aggregated information with sufficient detail for the Commission to understand the frequency in which specific provisions are being invoked as well as mitigation and remediation plans over time and by region. Such information would allow the Commission to evaluate whether to initiate the development of additional Reliability Standards or require new Reliability Standards and/or modifications to existing Reliability Standards.

81. The Commission also seeks 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.

82. The Commission proposes 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 NERC's glossary, pursuant to the prior clarifications, without any reference to reasonable business judgment.

Acceptance of Risk

83. The Commission has several concerns regarding the references to ''acceptance of risk'' that appear in the CIP Reliability Standards. As proposed by NERC, there are no controls or limits on a responsible entity's use of this exception. For example, a responsible entity may invoke the ''acceptance of risk'' exception without any explanation, mitigation efforts, evaluation of the potential ramifications of accepting the risk, or other accountability. In essence, the phrase ''or an acceptance of risk'' allows a responsible Entity to opt out of certain provisions of a mandatory Reliability Standard at its discretion.

84. Further, there is no requirement that a responsible entity communicate to a responsible authority information related to the potential vulnerabilities created by a decision to accept risk and how they could affect Bulk-Power System reliability. The resulting uncertainty concerning who had invoked ''acceptance of risk'' and in what connection would mean that neither the ERO, Regional Entities nor others would know whether adequate cyber security precautions are in place to protect critical assets. The possibility that appropriate security measures for critical assets have not been implemented due to acceptance of risk and that no corresponding compensating or mitigating steps have been taken presents an undue and unacceptable risk to Bulk-Power System reliability.

85. Moreover, the Commission believes the acceptance of risk language does not serve any justifiable purpose. To the extent that an entity would invoke this exception because compliance is not technically feasible, it should rely on that exception, which with the Commission's proposal would have specific safeguards and limitations. To the extent that a responsible entity would invoke the acceptance of risk language because its business preference is not to expend resources on cyber vulnerability, we believe that is inappropriate for all the reasons discussed previously. A responsible entity should not be able to jeopardize critical assets of others, and create a significant and unknown risk to Bulk-Power System reliability, simply because it is willing to ''accept the risk'' that its own assets may be compromised.

86. Accordingly, the Commission proposes to direct that the ERO remove the ''acceptance of risk'' language from the CIP Reliability Standards.

6. Guidance for Improving CIP Reliability Standards

87. Several commenters discussed the proposed CIP Reliability Standards in relation to other standards that exist for governmental and industrial cyber security. MITRE and NIST suggest that more advanced cyber security standards have been developed that could provide a model in future improvements to the CIP Reliability Standards. In particular, they point to NIST Special Publication 800–53 Revision 1, Recommended Security Controls for Federal Information Systems (SP 800–53). MITRE believes that the relevant NIST publications, including Federal Information Processing Standards (FIPS) 199, FIPS 200, and SP 800–53, constitute a comprehensive and coherent basis for cyber security in the electric power sector. NIST recommends that the Commission consider a planned transition to cyber security standards that are identical to, consistent with, or based on SP 800–53 and related NIST standards and guidelines.

Commission Proposal

88. The Commission declines to propose at this time that NERC incorporate any provisions of the NIST standards into the CIP Reliability Standards. However, the Commission expects NERC to monitor the development and implementation of the NIST standards to determine if they contain provisions that will better protect the Bulk-Power System.[56] Several federal entities, such as the Tennessee Valley Authority and Western Area Power Administration, are subject to both the NIST standards and the Reliability Standards, and therefore are likely to have unique insights into the NIST standards. The Commission expects the ERO to seek and consider comments from those federal entities on the effectiveness of the NIST standards and on any implementation issues. Any provisions that will better protect the Bulk-Power System should be addressed in the ERO'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 Reliability Standards, or as part of assessing NERC's performance of its responsibilities as the ERO.[57]

B. Discussion of Each CIP Reliability Standard

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

89. 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

[56] The Commission is also aware that the Instrumentation, Systems, and Automation Society (ISA) is developing cyber security standards, referred to as ISA SP–99, and that other infrastructure sectors are considering adopting the ISA standards for their control systems.

[57] *See* Order No. 672 at P 186–91.

affect the reliability or operability of the Bulk Electric System.'' [58]

90. 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.

91. The CIP Assessment emphasized that, while CIP–002–1 through CIP–009–1 function as an integrated whole, CIP–002–1 is a key to the success of the cyber security framework that these Reliability Standards seek to create.[59] The CIP Assessment also stressed that, because CIP–002–1 addresses the assessment methodology and process for identifying critical assets and critical cyber assets, it represents the critical first step that can fundamentally affect the chances for successful implementation of the remaining CIP Reliability Standards. The methodology and process used by a responsible entity must be stringent and rigorous. Otherwise, a responsible entity may fail to identify some facilities that are critical to effective cyber protection and, as a consequence, leave them vulnerable to an attack that could threaten the reliability of the Bulk-Power System.

92. The Commission proposes to approve Reliability Standard CIP–002–1 as mandatory and enforceable. In addition, the Commission proposes to direct the ERO to develop modifications to this Reliability Standard. In our discussion below, the Commission addresses its concerns in the following topic areas regarding CIP–002–1: (1) The proper risk-based assessment methodology for identifying critical assets and associated critical cyber assets; (2) internal approval of the risk assessment; (3) oversight of critical asset identification; and (4) interdependency analysis.

a. Risk-Based Assessment Methodology

93. As mentioned above, CIP–002–1 requires each responsible entity to develop a risk-based assessment methodology to identify critical assets.

CIP Assessment

94. The CIP Assessment noted that, while CIP–002–1 requires use of a risk-based assessment methodology, it does not provide direction on the nature and scope of that methodology, its basic features or the issues it should address. The CIP Assessment expressed concern that the absence of such direction could result in the Requirement being unevenly executed, which could result in inconsistency and inefficiency. It stated that, due to this lack of direction, the Reliability Standard does not provide a basis for evaluating whether the risk-based assessment methodology adopted by a particular entity will permit effective identification of all critical assets.

95. The CIP Assessment explained that proper risk-based assessment methodology is essential to achieve sufficient scope and implementation of critical infrastructure protection. Requirement R4 specifically contemplates the circumstance that a ''Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets,'' and correspondingly requires that a signed and dated record of management approval of the list of critical assets and critical cyber assets be kept ''even if such lists are null.'' The CIP Assessment pointed out, however, that a small entity whose operations may not have a major, day-to-day operational impact on the Bulk-Power System can have critical importance from a cyber security perspective, especially as a gateway to larger entities or when attacked simultaneously with other entities. The absence of adequate direction on what constitutes a proper risk-based assessment methodology may potentially result in entities improperly identifying a limited or ''null set'' of critical assets and critical cyber assets. This result could have serious adverse effects for Bulk-Power System reliability.

Comments

96. Commenters generally agree that CIP–002–1 plays a crucial role because whether a responsible entity must comply with the substance of the remaining CIP Reliability Standards depends on whether it identifies critical cyber assets pursuant to CIP–002–1. Commenters also agree that the risk assessment methodology is the key to a responsible entity accurately identifying its critical assets and critical cyber security assets.

97. While some commenters agree with the CIP Assessment that the Requirement for the risk-based assessment methodology would benefit from additional guidance or specificity, the majority disagree. Among those who support the need for more specificity, Arizona Public Service expresses concern that CIP–002–1, as proposed, may place a responsible entity in the position of not having enough guidance on whether its risk-based methodology will result in the identification of all critical assets.

98. Ontario IESO agrees that the CIP Assessment's reasons for concern are valid, which stem from the fact that many assessments will be performed by entities not previously subject to compliance with NERC Reliability Standards, and from the potential disagreement between entities on what constitutes a critical asset. It also shares the concern that some entities may avoid declaring critical assets to avoid further compliance obligations with the CIP Reliability Standards. Ontario IESO emphasizes that an essential feature of a good assessment is the quality of the judgments that necessarily must be applied. Rather than making modifications to provide more explicit direction, Ontario IESO suggests that much of the concern associated with critical asset identification could be addressed by modifying the Reliability Standard to require that the responsible entity consult with its reliability coordinator, and granting the reliability coordinator the authority to make the final determination of critical assets within its territory.

99. NERC and others oppose including additional specificity, claiming that CIP–002–1 is specifically written to allow each responsible entity the flexibility to implement it as it applies to the specific circumstances within each organization, and at each location containing critical cyber assets.[60] These commenters are concerned that a Commission directive to include additional guidance would restrict the needed flexibility. For example, APPA argues that the proposed provisions provide an adequate basis for evaluating the methodology, stating that prescribing a national-level ''one size fits all'' risk-based assessment methodology would

[58] ''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 cybersecurity incident, or unanticipated failure of system elements.'' EPAct 2005, section 215(a)(4).

[59] CIP Assessment at 16–17.

[60] E.g., ReliabilityFirst, EEI, EPSA, and APPA.

require a costly effort to comply, but would not result in measurable cyber security improvements. APPA adds that every entity's risk-based assessment will be subject to challenge by an audit team from time-to-time, which will include review by peer technical experts who share the goal of preventing any successful attack on critical assets. AMP-Ohio suggests that it would be inappropriate to divide the Bulk Electric System into a large number of small, discrete and in some cases rather isolated pieces and then to assign responsibility to each of these small pieces to determine what is or is not critical to the reliable operation of the Bulk Electric System.

Commission Proposal

100. Most commenters on the CIP Assessment acknowledge the importance of CIP–002–1 in ensuring that an appropriate set of critical assets is identified. However, many commenters oppose any modification to CIP–002–1 to provide additional specificity regarding the risk assessment methodology for identifying critical assets, based on concerns that such specificity will impede the needed flexibility that is currently provided by the Reliability Standard.

101. The Commission recognizes the commenters' concerns and is mindful of the need for flexibility in the risk assessment process to take into account the individual circumstances of a responsible entity. Yet, the Commission is concerned that, without some additional guidance, each responsible entity will have to devise its own assessment methodology without sufficient assurance that the methodology is adequate to identify the types of assets necessary to protect the reliability of the Bulk-Power System. As explained by Ontario IESO, many responsible entities performing the risk assessment have not previously been subject to compliance with NERC's Reliability Standards. Further, there is a potential for disagreement among responsible entities regarding what constitutes a critical asset.

102. The Commission also is concerned that the risk assessment methodologies required by CIP–002–1 must place the proper emphasis on the possible consequences from an outage of a particular asset. Generically, risk assessments include consideration of both consequence (in this case, the effect of loss of availability of an asset on the reliable operation of the Bulk-Power System) and threat (the likelihood that an outage will occur, naturally or by malicious act). However, in this context we believe that the consequence of an outage should be the controlling factor. We note that the definition of ''critical assets'' is focused on the criticality of the assets, not the likelihood of an outage.

103. Accordingly, the Commission proposes to direct NERC to develop modifications to CIP–002–1 to provide some basic guidance on the content or considerations to be applied in a risk assessment methodology. We are not proposing that NERC develop specific details of a methodology that must be applied in all circumstances. However, the Commission believes that responsible entities would benefit from NERC providing some common understanding regarding the scope, purpose and basic direction of the risk assessment methodology. For example, the Reliability Standard should indicate that a proper risk-based assessment methodology to identify critical assets should examine (1) the consequences of the loss of the asset to the Bulk-Power System and (2) the consequence to the Bulk-Power System if an adversary gains control of the asset for intentional misuse. Such guidance could also address how a generation owner, or even a partial owner of generation, without a wide-area reliability perspective, should approach a risk-based assessment.

104. Further, we are concerned that relatively smaller registered entities, such as some resources, load-serving entities, and demand side aggregators, may have difficulty in determining whether a particular asset is ''critical'' for Bulk-Power System reliability, since, for example, the impact of their facilities may be dependent on their connection with a transmission owner or operator. We believe that such an entity may want to perform an accurate assessment but lack the regional view to make a determination on its own. Thus, we propose that the ERO and Regional Entities provide reasonable technical support to such entities that would assist them in determining whether their assets are critical to the Bulk-Power System.

105. Accordingly, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations, the Commission proposes to direct that the ERO develop modifications to CIP–002–1 through its Reliability Standards development process to provide additional guidance as to the features and functionality of an adequate risk-based assessment methodology, as discussed above.

b. Internal Approval of Risk Assessment

106. 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. The CIP Assessment suggested that that this senior management involvement should be extended to approving the risk-based assessment methodology developed pursuant to Requirement R1.[61] Several commenters disagree,[62] stating that this approval is implied by the requirement for senior management approval of the critical asset list and the critical cyber asset list. Other commenters generally believe that senior management approval of the risk-based assessment methodology would be a benefit.[63]

Commission Proposal

107. The Commission believes that senior management approval of the risk-based assessment methodology has clear benefits that exceed any additional burden placed on the responsible entities, and the rigor that the senior management approval would encourage is worth the effort. As explained in the CIP Assessment, since a poor methodology will likely result in an inadequate identification of critical assets and critical cyber assets, senior management awareness and approval of the chosen risk-based assessment methodology is of critical importance.[64] It is not clear to the Commission that, as some commenters suggest, senior management approval of the risk-based assessment methodology is implicit in the requirement that senior management approve the critical asset list and critical cyber asset list. Commenters did not object to the concept, but only believed that it might be redundant. We believe this additional layer of oversight is important and should be made explicit. The Commission also notes that requiring this senior management approval helps to implement the Blackout Report's Recommendation 43, which calls for establishing ''clear authority and ownership for physical and cyber security.'' [65]

108. Thus, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations, the Commission proposes to direct that the ERO develop a modification to CIP–002–1 through its Reliability Standards development process to include a requirement that a senior manager annually review and approve the risk-based assessment methodology.

---

[61] CIP Assessment at 17–18.

[62] NERC, ReliabilityFirst, and Santa Clara.

[63] *E.g.,* APPA/LPPC, FirstEnergy, National Grid, Progress Energy, and Xcel.

[64] CIP Assessment at 18.

[65] *See* Blackout Report at 169, Recommendation 43.

c. Oversight of Critical Assets Identification

109. The CIP Assessment emphasized the underlying importance that each responsible entity develop accurate lists of critical assets and critical cyber assets. Several commenters note that responsible entities currently lack a wide-area view that would enable them to better assess the risks associated with certain assets.[66] They suggest that guidance or oversight from an external organization could help ensure that responsible entities have properly identified critical assets from a regional perspective. Cleveland Public Power suggests that the Regional Entities should assume this role. Similarly, AMP-Ohio recommends that the Regional Entities should be responsible for identifying critical assets, with input from reliability coordinators and transmission planners. EPSA indicates that independent system operators (ISOs) and regional transmission organizations (RTOs) could provide guidance to individual companies in assessing critical assets and their vulnerability, in coordination with NERC and the Commission.

110. NERC, however, opposes regional oversight, stating that ''[i]t is not the function of the standards to implement an oversight or hierarchical organization for determining risks or vulnerabilities.'' [67] NERC suggests that regional perspective is gained through information sharing forums such as the Electricity Sector Information Sharing and Analysis Center (ESISAC) [68] and NERC's Critical Infrastructure Protection Committee.

Commission Proposal

111. The Commission disagrees with commenters that suggest that the responsibility for identifying critical assets should be placed on the Regional Entities or another organization instead of the categories of applicable entities currently identified in CIP–002–1. Such an approach would shift primary responsibility away from the asset owner or operator. We believe that such a shift would not improve the identification of critical assets, but more likely overwhelm the Regional Entities.

112. On the other hand, the Commission believes that a formal or systematic approach to external oversight of the identification of critical assets would assure a wide-area view. Such an approach, on a regional basis, would better ensure that responsible entities are identifying similar assets. Even taking into account the individual circumstances of a responsible entity, we would expect certain trends in critical asset identification within a class of responsible entities, such as generator owners or transmission owners. If the vast majority of transmission owners, for example, identified a certain asset as critical, and a few did not, this result could be due to the unique circumstances of those transmission owners or from a flawed risk-based assessment methodology. However, without external oversight using a wide-area view, such trends or deviations would never be identified prior to an incident or audit, perhaps precluding a necessary adjustment to a particular critical asset list. In addition, 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.

113. NERC suggests that such issues can be addressed through existing forums for the voluntary exchange of information on cyber security issues. The Commission believes that this matter is too important to leave to voluntary mechanisms. Accordingly, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations, the Commission proposes to direct that the ERO develop a modification to CIP–002–1 through its Reliability Standards development process to include a mechanism for the external review and approval of critical asset lists based on a regional perspective. While we propose that the Regional Entities should be responsible for this function, we will not exclude the possibility of a critical asset review process that allows for participation of other organizations, such as transmission planners and reliability coordinators.

114. Moreover, we note that the definition of ''critical cyber assets'' encompasses data.[69] Thus, marketing or other data essential to the proper operation of a critical asset, and possibly the computer systems that produce or process that data, would be considered critical cyber assets subject to the CIP Reliability Standards. Therefore, the Commission proposes 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.

115. The Commission is concerned that all critical assets are identified, and interprets 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, based on the risk-based assessment methodology used, why specific assets were or were not chosen as critical assets. The Commission is also concerned that sufficient rigor is applied in examining whether control systems are determined to be critical assets. While it seems obvious that an evaluation of a control system for critical asset status would consider the potential loss of operability of the control center due to power or communications failure, we also believe that such an evaluation should include an examination of any misuse of the control system, the impact this misuse could have on any electric facilities that the responsible entity controls, and the combined impact of such facilities. Therefore, the Commission proposes to direct the ERO to modify Requirement R1.2 to clarify the requirement to show why specific assets were or were not chosen as critical assets, and to require the consideration of misuse of control systems.

d. Interdependency

116. The CIP Assessment noted that CIP–002–1 does not address the issue of interdependency with other infrastructures and explained that there may be occasions where an electric sector asset, while not critical to Bulk-Power System reliability, may be crucial to the operation of another critical infrastructure.[70] The CIP Assessment asked (1) whether this issue is appropriate for inclusion in CIP–002–1 and (2) whether this topic is an area for future coordination and collaboration with other industries and government agencies.

117. Commenters generally agree that this issue is worthy of consideration and coordination and cooperation could be

[66] *E.g.,* AMP-Ohio, EPSA, and Cleveland Public Power.

[67] NERC Comments, Attachment 1 at 17 (in response to a CIP Assessment suggestion regarding the need for regional perspective in CIP–003–1).

[68] The Electric Sector Information Sharing and Analysis Center was created based on a recommendation of Presidential Decision Directive 63, which defined specific infrastructures critical to the national economy and public well-being. ESISAC serves the Electricity Sector by facilitating communications between electricity sector participants, governmental entities, and other critical infrastructures. It is the job of the ESISAC to promptly disseminate threat indications, analyses, and warnings, together with interpretations, to assist electricity sector participants to take protective actions. NERC is functioning as the operator of the ESISAC.

[69] The NERC Glossary defines ''Critical Cyber Assets'' as ''Cyber Assets essential to the reliable operation of critical assets.'' It defines ''Cyber Assets'' as ''programmable electronic devices and communication networks including hardware, software, and data.'' Therefore, marketing data or other system data that are essential to the proper operation of the critical asset may confer critical cyber asset status to those data and the computer systems that process them.

[70] CIP Assessment at 17.

advantageous. However, most commenters consider the topic outside the scope of CIP–002–1.[71] By contrast, one commenter posits that there is a clear need to articulate that this type of interdependency analysis should be part of the responsible entity's determination of critical assets.[72]

Commission Proposal

118. Reliability Standard CIP–002–1 pertains to the identification of assets critical to Bulk-Power System reliability. While broader interdependency issues cannot be ignored, the Commission intends to revisit this matter through future proceedings and with other agencies. This work will help to 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.

e. Commission Proposal Summary

119. In summary,[73] the Commission proposes to approve Reliability Standard CIP–002–1 as mandatory and enforceable. In addition, the Commission proposes to direct the ERO, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations, to develop modifications to CIP–002–1 through its Reliability Standards development process that: (1) Provide some basic guidance on the content or considerations to be applied in a risk-based assessment methodology; (2) include a requirement that a senior manager annually review and approve the risk-based assessment methodology; (3) include a mechanism for the external review and approval of critical asset lists based on a regional perspective; and (4) modify Requirement R1.2 to (a) clarify the requirement to show why specific assets were or were not chosen as critical assets and (b) require the consideration of misuse of control systems.

2. CIP–003–1—Security Management Controls

120. Reliability Standard CIP–003–1 seeks to ensure that each responsible entity has minimum security management controls in place to protect critical cyber assets identified pursuant to CIP–002–1. To achieve this goal, a responsible entity first must develop a cyber security policy that represents management's commitment and ability to secure its critical cyber assets. The responsible entity must designate a senior manager to lead and direct the responsible entity's cyber security program. This senior manager will also be the person authorized to approve any exception set out in the entity's cyber security policy.

121. Further, a responsible entity must 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, the responsible entity must establish a change control and configuration management program to oversee changes made to the critical cyber assets' hardware or software.

122. The Commission proposes to approve Reliability Standard CIP–003–1 as mandatory and enforceable. In addition, we propose to direct the ERO to develop modifications to this Reliability Standard. In our discussion below, the Commission addresses its concerns in the following topic areas regarding CIP–003–1: (1) 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

123. Requirement R1 of Reliability Standard CIP–003–1 directs the 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 ''addresses the Requirements in CIP–002–1 through CIP–009–1, including the provisions for emergency situations.'' The Requirement also requires that a senior manager annually review and approve the policy.

124. The CIP Assessment stated that senior management involvement should improve the prioritization of control system security within the entity, including allocation of resources.[74] It explained that, since many of the Requirements in the CIP Reliability Standards leave considerable discretion to each responsible entity, the scope and thoroughness of the cyber security policies could vary widely. Thus, the CIP Assessment expressed concern that, because Requirement R1 does not address the policy's adequacy, this Requirement could actually mask certain security vulnerabilities.

125. APPA/LPPC are not convinced that the variation allowed in cyber security policies means that plans lack a sufficient level of protection. They believe that the Reliability Standard allows an appropriate level of variation as to how specific requirements will be met. Likewise, Georgia System does not share the CIP Assessment's concern that Requirement R1 could allow responsible entities to mask vulnerabilities, positing that it is in a utility's self-interest to take actions that improve reliability. Thus, it does not see a need for any additional guarantee that the involvement of senior management will result in improvements to the responsible entity's cyber security policy.

Commission Proposal

126. The Commission acknowledges that details of particular security policies will vary due to the different cyber architectures and equipment used by the responsible entities. However, in addition to consideration of every Requirement in Reliability Standards CIP–002–1 through CIP–009–1, the Commission expects that responsible entities' security policies will address issues that are not currently reflected in the CIP Reliability Standards, but are important to the security of the control system. For instance, currently data networks and communication networks are not covered by any CIP Reliability Standard. Yet these networks play an important role in the proper functioning of the control systems. The Commission would expect a security policy for control systems to address the responsible entity's actions to protect communication networks. Other possible topics for guidance here are 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 equipment for critical cyber assets. We note that Recommendation 34 of the Blackout Report states that ''grid-related organizations should have a planned and documented security strategy, governance model, and architecture for EMS [energy management systems] automation systems.'' [75]

127. The Commission proposes to 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 to ensure that the responsible entity

[71] *E.g.,* APPA/LPPC, Duke, EEI, Georgia System, National Grid, NERC, ReliabilityFirst, SPP, Xcel, SoCal Edison, Progress Energy, and MidAmerican.

[72] ISA Group.

[73] This summary should be read in conjunction with the discussion above.

[74] CIP Assessment at 19.

[75] *See* Blackout Report at 165, Recommendation 34.

reasonably protects its critical cyber assets.

b. Discretion to Grant Exceptions

128. Requirement R3 of CIP–003–1 provides that a responsible entity must document as an exception, with senior manager authorization, each instance where a responsible entity cannot conform to its security policy developed pursuant to Requirement R1. Documentation of the exception 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.

129. The CIP Assessment expressed concern that this provision allows for broad discretion and may serve as a disincentive for upgrading to control systems that fully comply with cyber security Reliability Standards.[76] With regard to a responsible entity's option to ''accept the risk,'' it pointed out that, for interconnected control systems of various entities, acceptance of risk by one entity is actually an acceptance of risk for all those that are interconnected. Yet, other entities may not be aware of the vulnerability, particularly absent any oversight or regional perspective of the risks or vulnerabilities that may exist.

130. Most commenters believe that it is appropriate to provide latitude for management to document exceptions to the responsible entity's established policies, select alternative and mitigating solutions, and ultimately accept residual risk. APPA/LPPC expect that the exercise of discretion will be one of the areas that will draw the most attention from auditors.

131. Others, such as California PUC agree with the CIP Assessment's concern that the broad discretion allowed for exceptions could act as a disincentive for upgrading control systems. California PUC also agrees that acceptance of the risk in a cyber environment is actually an acceptance of risk for all connected entities because the entity that initially accepts the risk becomes the ''weak link'' in the chain. Santa Clara suggests that a responsible entity that makes exceptions and ''accepts risks'' is responsible for communicating such exceptions to its Regional Entity, which can then evaluate the overall ''risk,'' if any, to the bulk electric system. The Regional Entity, in turn, can then communicate appropriately to any interconnected entities so that they might take any necessary action.

Commission Proposal

132. The Commission is concerned that CIP–003–1 allows a responsible entity too much latitude in excusing itself from compliance with its cyber security policy. While there may be valid reasons for exceptions to a cyber security policy, and it is helpful that exceptions must be explained in writing and approved by a designated senior manager, the Commission does not believe that the ''exceptions'' provision provides sufficient rigor or external accountability regarding the decision of a responsible entity to except itself from the cyber security policy. Accordingly, the Commission proposes to direct that NERC develop a modification to Requirement R3 of CIP–003–1 to require a responsible entity to periodically submit to the Regional Entity the documentation of exceptions to the cyber security policy. The Commission believes that the external review of this documentation will provide added assurance that each responsible entity adequately justifies the exceptions to its cyber security policy.

133. In addition, the Commission believes that there is a distinction between situations where a responsible entity excepts itself from its cyber security policy, rather than from specific Requirements of the CIP Reliability Standards based on technical feasibility. An exception to a cyber security policy provision does not also excuse compliance with a Requirement of a CIP Reliability Standard. Generally, a responsible entity has no authority to excuse itself from compliance with a mandatory Reliability Standard. As discussed above in section II.B.1.6, the CIP Reliability Standards do include several Requirements that allow an exception based on technical feasibility. However, the Commission has proposed to direct NERC to modify such provisions so that a responsible entity can only invoke the technical feasibility exception after fulfilling specific conditions including receiving approval from the ERO or the relevant Regional Entity. In contrast, an exception to a cyber security policy would require only senior manager approval and after-the-fact reporting to the Regional Entity. Accordingly, the Commission proposes to direct NERC to clarify that the exceptions mentioned in Reliability Standard CIP–003–1, Requirements R2.3 and R3, do not except responsible entities from the requirements of the CIP Reliability Standards.

c. Leadership

134. The CIP Assessment notes that senior management involvement in security issues is important to ensure that responsible entities achieve compliance as quickly as possible and to ensure that it exercises any necessary discretion in an appropriate manner.[77]

135. While National Grid concurs with the CIP Assessment, it also suggests that given the wide variety of critical assets, critical cyber assets and physical security requirements, no single senior manager has the expertise or authority to ensure compliance with all of the CIP Reliability Standards.

Commission Proposal

136. The Commission's view is that Requirement R2 of CIP–003–1 should be interpreted to require the designation of a single manager who has direct and comprehensive responsibility for the implementation and ongoing compliance with the CIP Reliability Standards. While this senior manager must have authority to delegate tasks and responsibilities within the entity's management structure, we believe that the senior manager must remain accountable for the responsible entity's compliance with the CIP Reliability Standards. In our view, it is essential to make clear both the ''authority and ownership'' for security, as Recommendation 43 of the Blackout Report states.[78] Therefore, the Commission proposes to direct the ERO to modify CIP–003–1, to make clear the senior manager's ultimate responsibility.

d. Access Authorization

137. Requirement R5 of CIP–003–1 directs the responsible entity to implement a program for managing access to protected critical cyber asset information. The CIP Assessment suggested that an annual review of personnel access to this information appears insufficient and could result in unnecessary vulnerability, especially since there is no requirement that a responsible entity revise access privileges to such protected information upon employee termination or job reassignment.

138. Many commenters agree with the CIP Assessment's concern that an employee who leaves the company or who no longer performs job functions that require access to critical cyber assets should have that access revoked

[76] CIP Assessment at 20.

[77] CIP Assessment at 20.

[78] *See* Blackout Report at 169, Recommendation 43.

promptly.[79] NERC, Xcel, FirstEnergy and ReliabilityFirst note that this Requirement seeks establishment of ''a program for managing access to protected critical cyber asset information.'' They stress that CIP–003–1, Requirement R5 relates to the governance and approval process, not the implementation and review of individual access (the oversight responsibility of which lies with the senior manager of the responsible entity). NERC asserts that the three requirements work together. The implementation provisions are in Requirement R5 of CIP–007–1, the revocation requirements are in Requirement R4 of CIP–004–1, and the management review and approval requirements are in Requirement R5 of CIP–003–1. NERC argues that, together, these provisions serve as a check that the CIP–004–1 revocation provision has been implemented.

Commission Proposal

139. The Commission believes that the language of CIP–007–1, Requirement R5, CIP–004–1, Requirement R4, and CIP–003–1, Requirement R5 does not interlink these related provisions as clearly as some commenters assert. We are not persuaded by commenters who claim these Requirements adequately address the access issues related to employee turnover. We believe that the interrelationship among these provisions must be made clearer. We note that CIP–007–1, Requirement R5.1.3, which specifically refers to CIP–003–1, Requirement R5, addresses ''user accounts.'' Likewise, CIP–004–1, Requirement R4 addresses authorization for unescorted physical or cyber access to ''critical cyber assets.'' However, the information for which Requirement R4 of CIP–003–1 requires protection appears to be broader than ''user accounts'' and ''critical cyber assets.'' According to CIP–003–1, Requirement R4, protected information includes lists of critical cyber assets, floor plans, and security configuration information. While the concept of access authorization is similar across these provisions, there is no explicit mention in them of revoking access to ''information'' about critical cyber assets. While the priority must be on granting and revoking access to the critical cyber assets themselves, access to information concerning the critical cyber assets should also be adequately protected, and revocations always should be made promptly. We also note that Recommendation 44 of the Blackout Report stresses the need to prevent inappropriate disclosure of information.[80] Thus, the Commission proposes to direct the ERO to modify Reliability Standards CIP–003–1, CIP–004–1, and/or CIP–007–1, to ensure and make clear that access to protected information is revoked promptly.

e. Change Control and Configuration Management

140. Requirement R6 requires the responsible entity to establish a process of change control and configuration management for adding, modifying, replacing, or removing critical cyber asset hardware or software.

141. The CIP Assessment noted that entities often rely on commercial vendors to test and certify that electronic security patches they provide will not adversely affect other electronic systems already in place. It is not clear how a responsible entity could otherwise verify that a problem does not exist without burdensome testing each time a patch is implemented. Such a testing requirement may also inhibit or delay the use of security patches and thereby prolong vulnerabilities that would otherwise be relatively easy to fix.

142. Santa Clara submits that electric utilities, like all ''cyber users,'' must rely on information technology vendors for accurate and reliable ''emergency or normal modifications.'' It suggests that it is not only unrealistic, but unnecessary, to expect that all responsible entities under the CIP Reliability Standards should, or could, possess the technical expertise to understand an IT vendor's code in enough detail to ensure that any modifications made by the IT vendor are accurate and reliable.

143. SPP believes that the purpose of the change management program is to ensure the entity is aware of all changes being made to a critical cyber asset and, in being aware, readily recognizes when an unapproved change is made. An unapproved change could be an indication of a cyber attack in progress. SPP comments that Requirement R6 may fall short because it does not specify the need for detection and monitoring controls to determine when changes occur. SPP also asserts that a proper change management program includes provisions for routine, planned changes and emergency, unplanned changes.

Commission Proposal

144. While Requirement R6 of Reliability Standard CIP–003–1 captures the essence of managing changes intentionally made to critical cyber assets, it fails to address accidental consequences or malicious actions by individuals. Thus, the Commission believes that this Requirement needs to go further and we propose to direct the ERO to make two changes. First, we propose additional wording to require verification that authorized changes made to critical cyber assets, which include software and data, only affect processes that are intended. Our concern here includes both accidental consequences and malicious actions by individuals performing the changes. Second, we propose a requirement for responsible entities to take actions to detect unauthorized changes to critical cyber assets. Such changes could result from malicious actions originating either outside or inside the responsible entity. No electronic security perimeter is 100 percent effective, especially when a malicious action is performed by an insider, and detection must be part of a good cyber security program. Therefore, the Commission proposes, as suggested by SPP, to direct the ERO to modify Requirement R6 of Reliability Standard CIP–003–1 to include in the process of change control and configuration management a requirement for detection and monitoring controls to determine if changes are made as intended and to investigate whether any unintended or unplanned changes have been made.

f. Interconnected Networks

145. The CIP Assessment also raised a concern that interconnected control system networks are more susceptible to infiltration by a cyber intruder. Georgia Operators responds that every responsible entity must protect its critical cyber assets by guarding its electronic access points against the spread of harm from external interconnected entities. This task can only be accomplished by assuming that such external entities are themselves unprotected.

146. NERC and ReliabilityFirst claim that the purpose of establishing policy and procedure is for a responsible entity to protect itself from the ''outside world'' wherever that ''outside world'' might exist. It does not matter if the ''outside'' is an internally connected corporate network, or a completely separate entity. These commenters explain that the CIP Reliability Standards address a responsible entity's area of responsibility—the equipment it owns and controls. All interconnected control system network communications will traverse through electronic access points; therefore, there exists a need for ''security'' on the

[79] *E.g.,* APPA/LPPC and California PUC.

[80] *See* Blackout Report at 169, Recommendation 44.

interconnection points. Both commenters state that the electronic security perimeter effectively implements a model of mutual distrust between any collection of critical cyber assets within an electronic security perimeter, and any and all other cyber assets.

Commission Proposal

147. The Commission agrees with commenters who caution that a responsible entity should protect itself from whatever is outside its control system. The phrase ''mutual distrust'' has been used to denote how these ''outside world'' systems are treated by those inside the control system. However, there is very little guidance for how a responsible entity would configure an architecture under a ''mutual distrust'' posture to handle both interactive login-type connectivity between the outside world and the control system as well as direct application communications (data shared between programs) that also occur between the control system and the outside world (both internal and external to the responsible entity). In addition, the Commission notes that, in our earlier discussion regarding the applicability of the CIP Reliability Standards to small entities, we relied in part upon the expectation that the responsible entities would adopt ''mutual distrust'' postures when receiving communications from others that impact the functioning of control systems. Therefore, the Commission proposes to direct the ERO to modify Reliability Standard CIP–003–1 to provide direction regarding the issues and concerns that a ''mutual distrust'' posture must address to protect the control system from the ''outside world.'' [81]

g. Commission Proposal Summary

148. In summary, the Commission proposes to approve Reliability Standard CIP–003–1 as mandatory and enforceable. In addition, the Commission proposes to direct the ERO, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations, to develop modifications to CIP–003–1 through its Reliability Standards development process that (1) provide additional guidance for the topics and processes that should be addressed by the required cyber security policy in order to ensure that the responsible entity reasonably protects its critical cyber assets; (2) require a responsible entity to submit periodically to the Regional Entity the documentation of exceptions to the cyber security policy; (3) 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; (4) make clear that the senior manager ultimately remains responsible for the responsible entity's compliance with the CIP Reliability Standards; (5) ensure and make clear that access to protected critical cyber asset information is revoked promptly (and make parallel modifications to CIP–004–1 and CIP–007–1 as needed); (6) include in the process of change control and configuration management a requirement for detection and monitoring controls to determine if changes were made as intended and to investigate whether any unintended or unplanned changes have occurred; and (7) provide direction 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

149. Reliability 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.

150. The Commission proposes to approve Reliability Standard CIP–004–1 as mandatory and enforceable. In addition, we propose to direct the ERO to develop modifications to this Reliability Standard. In our discussion below, the Commission addresses its concerns in the following topic areas regarding CIP–004–1: (1) Training; (2) personnel risk assessments; (3) access; and (4) jointly owned facilities.

a. Training

151. The CIP Assessment noted that the training requirements 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.[82] It then expressed concern that this requirement does not clearly address the interconnectivity of systems; *i.e.*, the required training programs should address not only the critical cyber assets themselves, but also any networking hardware or software linking them. It noted that the importance of network support to overall security environment may not be understood by personnel if the training does not encompass the related non-critical cyber assets, such as switches and routers that can impact the security of the critical cyber assets. Moreover, it pointed out that while this requirement specifies the minimum topics that training should cover, it does not provide criteria for assessing the quality and adequacy of the training. With regard to both the awareness program of Requirement R1 and the training program of Requirement R2, the CIP Assessment noted that certain NIST publications provide guidance on training of personnel and practices that enhance the security posture of information systems.[83]

152. NERC states that a subset of networking hardware and software is included in Requirement R2 to the extent active communications hardware and software reside within the defined electronic security perimeter, and because hardware and software acts as an electronic access control, defining the electronic security perimeter. NERC draws attention to the fact that communication networks and data communication links between discrete electronic security perimeters are specifically excluded by Applicability section 4.2.2 of this Reliability Standard.

153. APPA/LPPC believe that most, if not all, networking hardware and software will be essential to the operation and control of critical cyber assets and therefore will be subject to the Reliability Standard and encompassed by the security training requirement. FirstEnergy notes the Measures and Compliance provisions currently require only documentation of

[81] 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.

[82] CIP Assessment at 23.

[83] *See* NIST Special Publication 800–16, Information Technology Security Training Requirements: A Role- and Performance-Based Model (1998); and NIST Special Publication 800–50, Building an Information Technology Security Awareness Training Program (2003), *available* at: *http://csrc.nist.gov/publications/nistpubs/.*

the requirements and states that NERC should focus on developing Reliability Standards to maintain the quality of personnel training in this area. FirstEnergy states that training requirements should be appropriate to each employee's experience and access level.

154. The CIP Assessment also questioned whether it is appropriate to allow personnel to have access to critical cyber assets for up to 90 days prior to receiving any cyber security training, as Requirement R2.1 allows. It suggested that personnel should receive the training prior to such access.

155. NERC and ReliabilityFirst state that the sub-requirements of Requirement R2 list specific expected outcomes from the training. NERC and ReliabilityFirst state that the 90-day period is based on the belief that certain conditions may require that personnel receive access prior to specific additional training in cyber security processes and procedures in order to maintain or restore the reliable operation of the Bulk-Power System. They explain that standard industry practice ensures anyone with access to sensitive systems has had adequate training, but that such training may not have been specific to the systems or environment to which they receive access, such as when, in an emergency restoration, personnel with specialized knowledge may be required to access systems outside their normal assignments.[84]

156. APPA/LPPC agree with the CIP Assessment that, whenever possible, personnel should receive their cyber security training and undergo the required personnel risk assessment before being allowed access to critical cyber assets. However, APPA/LPPC favor retention of the 90-day period for conducting training so that responsible entities will not risk a technical violation of the Reliability Standard when emergency conditions require that personnel obtain access before they are trained or authorized with access.

157. ISA Group agrees with the CIP Assessment that training in critical security practices should occur prior to an individual having the corresponding access and suggests making a distinction between the training that is needed before access is granted and the remaining training that is not critical for access but still significant. The ISA Group also states that training and awareness programs should be specific to the critical cyber assets to be protected and that persons who provide the training should be adequately trained to address the cyber security of the systems. SPP and ISO–NE agree with the CIP Assessment that allowing unescorted access to critical cyber assets prior to security training introduces an unnecessary risk. SPP suggests that, under normal circumstances, training prior to access should be the requirement with provisions made for emergency conditions.

Commission Proposal

158. Training is clearly integral to the protection of critical cyber assets. Allowing personnel to access critical cyber assets prior to receiving training increases the vulnerability of and risk to such assets. Thus, such access should not be the norm under the Reliability Standard. Accordingly, we propose to direct the ERO to modify this provision 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 allowing limited exceptions, such as during emergencies, subject to documentation and mitigation.

159. Alternate provisions for emergencies and certain other conditions could be designed, such as requiring documentation of all personnel who received access to particular equipment during the emergency and whether they received a briefing or any other training prior to their access concerning the specific facilities; the extent to which people needed for the emergency had received general training and possessed appropriate specialized expertise for the circumstance; and any risk mitigation steps taken during the emergency access, as discussed by commenters in this proceeding. To facilitate communications in emergency situations, the Commission proposes 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 other contingency situations where full training prior to access will not best serve the reliability of the Bulk-Power System. We note that during ''emergency conditions,'' the Bulk-Power System could be particularly vulnerable to mischief or mistakes, and we propose to require the ERO to consider this when developing the modification. We also propose to direct the ERO to consider what, if any, modifications to CIP–004–1 should be made to address the concern raised by the ISA Group that security trainers be adequately trained themselves.

160. In addition, we propose to direct the ERO to modify the 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. As indicated by the comments, it is not clear whether interconnectivity issues are already included in the proposed language of the training requirement of CIP–004–1. One method of clarification the ERO should consider is the addition of a provision such as that contained in CIP–005–1, Requirement R1.4, which specifically subjects any non-critical cyber asset within a defined electronic security perimeter to the Reliability Standard. 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.

161. Finally, we propose to direct the ERO to increase the guidance in the Reliability Standard as to the scope and quality of training. We note that part of the goal for training, in conjunction with awareness programs, is to keep security practices on the minds of employees, contractors, and vendors. Examples of some areas where the inclusion of guidance can be considered are: control of electronic devices (such as laptop computers), the appropriate audiences for the training, delivery methods, and updates of training materials. In our view, the awareness and training programs, addressed separately by Requirements R1 and R2, complement each other and work in tandem. In parallel with the security awareness program, we expect the ERO to consider relevant aspects of the cited NIST Special Publications, as well as other relevant models, to improve CIP–004–1 and prevent a lowest common denominator result.

b. Personnel Risk Assessment

162. 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 check, be conducted within 30 days after a person receives cyber access or unescorted physical access to critical cyber assets. The CIP Assessment noted that Requirement R3 would allow access to critical cyber assets while investigation is still underway, and even before an investigation has started.

[84] APPA/LPPC, SPP and Xcel agree that this flexibility is needed in emergency situations, and comment that training beforehand would not always be practical.

163. NERC and ReliabilityFirst assert that certain conditions affecting the reliable operation of the Bulk-Power System may require that personnel be allowed to access the critical cyber assets prior to completing the personnel risk assessment process, although they may be subject to escort and review during the investigative period.

164. Several commenters agree with the CIP Assessment that an appropriate personnel risk assessment should be completed before an employee (especially a newly hired employee or vendor) is granted access to critical cyber assets. SPP states that emergency contingency procedures can be developed to handle situations where access must be granted prior to completing the required background check.

165. However, NERC and other commenters have concerns about existing personnel. NERC and ReliabilityFirst assert that certain conditions affecting the reliable operation of the Bulk-Power System may require that personnel be allowed to access the critical cyber assets prior to the completion of the personnel risk assessment process, although they may be subject to escort and review during the investigative period. National Grid expresses concern that, since the Requirement appears to apply to a significant portion of existing utility workforce, any attempt to revoke access to such employees while completing their personnel risk assessments would create more reliability concerns than simply allowing such employees to remain on the job. FirstEnergy states that the 30-day window may be appropriate for employees and vendors with which the responsible entity has had a working relationship. FirstEnergy comments that Requirement R3 does not provide sufficient detail on what constitutes an adequate personnel risk assessment, which could cause variable interpretations of this Requirement. ISO–NE agrees with the CIP Assessment that the Reliability Standard provides insufficient direction regarding the elements of an appropriate awareness program.

Commission Proposal

166. Similar to our concerns regarding the training provisions of Requirement R2, we believe 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. We also observe that Recommendation 41 of the Blackout Report emphasizes the need for guidance on implementing background checks.[85] At the same time, we believe that commenters have 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, we propose that the ERO 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. The ERO should determine the parameters of such exceptional circumstances in developing the proposed modification through its Reliability Standards development process. However, to avoid disruptions, we propose that the 30-day window allowing access before the personnel risk assessment is completed 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. We propose to direct 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.

c. Access

167. Requirement R4 directs the responsible entity to maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to critical cyber assets. The CIP Assessment observed that the lists do not serve to deny personnel access from critical cyber assets prior to completion of a personnel risk assessment. However, Requirement R4.2 requires that 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.

168. NERC states that while the access list itself does not prevent access, it does provide for identification of personnel for which additional levels of review and escort may be assigned. California PUC suggests amending the Reliability Standard to require immediate updates when an employee is transferred, retires, or is terminated.

[85] *See* Blackout Report at 167–168, Recommendation 41, where the Blackout Report recommends that NERC provide guidance on background checks to be completed on contractor and sub-contractor employees in advance of allowing access to secure facilities.

Commission Proposal

169. Timely system updates to access rights are important. Employee, contractor, or vendor access to critical cyber assets when the employee, contractor, or vendor no longer has a need for such access, due for example to a transfer or termination, represents a gap in security. Moreover, while Requirement R4 of CIP–004–1 requires a responsible entity to maintain a list of authorized personnel, it does not indicate what the responsible entity must do with the list. Accordingly, the Commission proposes to direct that NERC 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). Because an organization is typically aware in advance of personnel action dates, timely updating of the authorization list should not be unduly burdensome. Further, we propose to direct that NERC modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list.

d. Question of Jointly Owned Facilities

170. APPA/LPPC request that the Commission direct NERC to consider clarifications for entities with facilities governed by existing joint use or joint ownership agreements. They explain that most of there members have joint facilities with neighboring entities (*e.g.*, a transmission substation at a point of interconnection with an adjacent system), and that joint facility agreements often prohibit individual co-owners from blocking the other co-owners' use of, or access to, such facilities. APPA/LPPC state that CIP–004–1 obligates individual responsible entities to block certain persons from their facilities, possibly including persons with existing contractual rights of access. APPA/LPPC believe that one joint facility owner should not be able to block another unaffiliated entity's existing contractual rights of access. APPA/LPPC also ask that entities with joint facilities not be subject to sanctions solely because an unaffiliated entity that is a party to one of its joint facility agreements failed to comply with CIP–004–1 when acting independently.

Commission Proposal

171. The Commission views joint owners of critical cyber assets as being

equally subject to the CIP Reliability Standards as other responsible entities. If an asset is designated as a critical cyber asset by one joint owner, it must be treated likewise by the other owner(s). Thus, each entity that possesses an interest in a jointly-owned facility would be responsible to develop a list of its authorized personnel and to respect each other joint owner's corresponding list.

172. APPA/LPPC also raise the issue of ''joint use'' arrangements. For example, an owner of a critical cyber asset substation may well house electronic or other equipment on its premises that belongs to another entity that may or may not be subject to these Reliability Standards. The Commission believes that, in principle, the owner of a critical cyber asset is responsible under the Reliability Standards for ensuring that all persons having access to the critical cyber asset meet the requirements of these Reliability Standards, much as the owner is responsible to ensure that vendor personnel have the required levels of security training, awareness and background checks.

173. Nevertheless, we can appreciate that even with this general guidance, further clarification regarding how ''joint use'' arrangements should be addressed. Therefore, we propose to direct the ERO to address the ''joint use'' concerns expressed by APPA/LPPC while developing any modifications to these Reliability Standards directed in a final rule. Regardless of whether a facility subject to CIP–004–1 is jointly owned or not, all entities that have access to it must comply with CIP–004–1. Each entity, however, is responsible for only its compliance and may not attempt to block or limit another's access on the basis of its perception that the other entity has not complied with CIP–004–1. In the event non-compliance is suspected, it must be promptly reported to the Regional Entity or ERO.

e. Commission Proposal Summary

174. In summary, the Commission proposes to approve Reliability Standard CIP–004–1 as mandatory and enforceable. In addition, the Commission proposes to direct the ERO, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations, to develop modifications to CIP–004–1 through its Reliability Standards development process that: (1) Require affected personnel, with limited exceptions, to receive required training before obtaining access to critical cyber assets (rather than within 90 days of access authorization); (2) require responsible entities to identify ''core training'' elements to ensure that essential training elements will not go unheeded in an emergency and other contingency situations where full training prior to access will not best serve the reliability of the Bulk-Power System; (3) clarify that the cyber security training programs required by Requirement R2 are intended to encompass training on networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets; (4) provide increased guidance on the scope and quality of training; (5) make 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; (6) 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; and (7) require immediate revocation of both physical and electronic access privileges when an employee, for any reason (including disciplinary action, transfer, termination, or retirement), no longer performs a function that requires access to critical cyber assets.

175. In addition, the Commission proposes to direct the ERO to (1) consider what, if any, modifications to CIP–004–1 should be made to address the concern raised by the ISA Group that security trainers be adequately trained; (2) consider relevant aspects of certain NIST Special Publications, as well as other relevant models, to improve CIP–004–1; and (3) address the ''joint use'' concerns expressed by APPA/LPPC and discussed herein by the Commission when developing modifications to the Reliability Standards that the Commission may direct when we issue our final rule.

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

176. Reliability 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 risk-based assessment methodology required by Reliability 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. Once each electronic security perimeter has been established, the responsible entity must develop mechanisms to control and monitor electronic access to all electronic access points. Furthermore, the responsible entity must assess the electronic security perimeter's cyber vulnerability and test every electronic access point at least annually.

177. The Commission proposes to approve Reliability Standard CIP–005–1 as mandatory and enforceable. In addition, we propose to direct the ERO to develop modifications to this Reliability Standard. Further, the Commission also proposes to require the ERO to consider various other matters of clarification, guidance, and modification. In our discussion below, the Commission addresses its concerns in the following topic areas regarding CIP–005–1: (1) Adequacy of electronic security perimeters; (2) protecting access points and controls; (3) monitoring access logs; (4) vulnerability assessments; and (5) document updates.

a. Adequacy of Electronic Security Perimeters

178. Requirement R1 of CIP–005–1 addresses the identification of electronic security perimeters to ensure that every critical cyber asset resides within one. The CIP Assessment explained that the electronic security perimeter constitutes the appropriate first line of defense. However, a responsible entity should use a cyber security protection program that contains additional security measures to detect and stop intrusions that penetrate the outer shell of the defense (*i.e.*, a defense in depth approach).

179. APPA/LPPC and Xcel agree with the CIP Assessment's concept of defense in depth and when possible, securing the non-critical cyber assets outside the electronic security perimeter. However, APPA/LPPC state that the use of ''defense in depth'' may not be practical for all critical cyber assets, such as assets supplied by vendors that are no longer in business.

180. Xcel notes that a line needs to be drawn in order to avoid responsible entities taking expensive precautions that are not cost-effective. It further adds that CIP–005–1 should not be extended to equipment and systems beyond the electronic security perimeter.

Commission Proposal

181. The Commission recognizes that there is a point at which having multiple defense layers would not be cost effective. However, the effectiveness of any one defense measure is often dependent upon the quality of active human maintenance, and there is no one perfect defense measure that will guarantee the

protection of the Bulk-Power System. Therefore, we believe that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter. Thus, the Commission proposes to direct the ERO to develop a requirement to implement a defensive security approach including two or more defensive measures in a defense in depth posture. This approach should not inhibit, but instead supplement the establishment of an electronic security perimeter. While such layers/measures are generally integrated within and constitute part of a system or program, many are also effectively, and more feasibly, placed ''in front of'' a system, such as an older, legacy system.

b. Protecting Access Points and Controls

182. 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.''

183. The CIP Assessment raised concerns regarding the qualifier ''where technically feasible'' in Requirement R2.4. The CIP Assessment also cautioned that keeping pace with advances in cyber security is a necessary part of the defense strategy needed to protect against intrusion by an adversary. The CIP Assessment noted that implementation and maintenance of strong controls to ensure authenticity of the accessing party is not a question of technical feasibility. It represents that the technology currently exists and that every responsible entity identifying critical cyber assets should be able to implement such controls. Balancing an appropriate mix of protections and technology is part of achieving effective cyber security. The CIP Assessment also expressed the view that Requirement R2.4 should not allow a responsible entity to fail to implement rudimentary procedural and technical access controls.

184. California PUC states that electronic access from outside the electronic security perimeter should require strong verification, such as digital certificates or two-factor authentication. It suggests that such a system is virtually impenetrable and that it, or some similar system, should be required in the CIP Reliability Standards.

185. California PUC comments that access controls should be implemented at all access points to the network and that the caveat of ''technical feasibility'' in the NERC-proposed Reliability Standard is inappropriate. California PUC further states that Requirement R2.0 prescribes, *inter alia,* that only those ports and services required for normal or emergency operations should be enabled, while all others should be disabled. Furthermore, it notes that access control, including the authorization process and authentication method for each access point, should be documented. Access should be monitored twenty-four hours a day, seven days a week, and disturbances and unauthorized access attempts should be identified. All responsible entities should conduct vulnerability assessments of their access points, scanning to verify that only the proper ports and services are enabled. California PUC agrees with the CIP Assessment assertion that ''such (strong access control) technology currently exists'' and implementation by every entity is feasible.

186. NERC disagrees with the CIP Assessment comment that a ''technical feasibility'' caveat is not needed in Requirement R2.4, particularly for legacy implementations and substation environments. NERC agrees that the CIP Assessment statement may be applicable in a modern control center environment, where common IT systems have migrated into the control environment. However, NERC states that this is not the case for many existing field systems. The technical feasibility clause, NERC claims, is needed to accommodate the vast majority of legacy systems that cannot be upgraded due to the age and nature of their system configurations.[86]

187. Given the numerous scenarios surrounding access control, APPA/LPPC believe that removing the ''technically feasibility'' caveat will not provide a solution in every situation. They assert that Requirement R2.4 is appropriate as currently written. APPA/LPPC note that some access control solutions, such as biometric ones, are still subject to failure and may grant access to unauthorized people.

Commission Proposal

188. Requirement R2.4 of CIP–005–1 calls for the implementation of ''strong procedural or technical controls'' at access points to ensure authenticity of the accessing party. While we agree with the goal of Requirement R2.4, we are concerned that requiring ''strong'' controls does not provide sufficient guidance and possibly sets subjective criteria. Thus, we believe that Requirement R2.4 should 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. The Commission agrees with California PUC that strong verification includes technologies such as digital certificates and two-factor authentication. We also note that Recommendation 32 of the Blackout Report emphasizes the need ''to ensure access is granted only to users who have corresponding job responsibilities.'' [87] We propose to direct the ERO to modify this Reliability Standard accordingly.

189. The Commission believes that providing such basic security measures as access control can be accomplished using/placing measures ''in front of'' systems as opposed to ''inside'' systems. Such an approach can be used to secure even older, yet functioning, legacy systems. The Commission proposes to direct the ERO to evaluate the issue and provide specific guidance to responsible entities that must face such issues.

190. The Commission is persuaded by commenters that maintain that, due to the variety of equipment and systems, some discretion must be preserved that would allow responsible entities to control access points. Further, in our general discussion of ''technical feasibility'' in section II.A.5.b above, we explained that, while we have concerns regarding the broad discretion currently allowed in the use of the technical feasibility language, we would not propose to eliminate the provision but, rather, propose to require specific controls and accountability when a responsible entity chooses to invoke the provision. Specifically, a responsible entity invoking a technical feasibility exception would have 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 responsible for leading and managing compliance with the CIP Reliability Standards. As discussed previously, the Commission proposes that a responsible entity invoking a

[86] Progress Energy, ReliabilityFirst, and Santa Clara agree with NERC.

[87] *See* Blackout Report at 164–165, Recommendation 32.

technical feasibility exception must have 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 proposes to require a responsible entity to report and justify to the ERO and the Regional Entity for approval each exception and its expected duration.

191. Consistent with our earlier discussion, we will not propose the removal of the ''technical feasibility'' language from Requirement R2.4 of CIP–005–1. However, such discretion will not lie solely with the responsible entities. We propose to direct 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.

c. Monitoring Access Logs

192. 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.

193. The CIP Assessment noted that frequent reviews of access logs are necessary to look for security breaches that automated alerts do not detect. It cautioned that the ''technical feasibility'' caveat in Requirement R3.2 can allow a 90-day lapse in review of access logs when it is commonplace in the IT industry for logs to be reviewed every one or two days. The CIP Assessment also advised that the use of discretion to address ''technical feasibility'' permitted in Requirement R3.2 should not be a basis for failing to implement a process that detects attempts to access or actual unauthorized access. Such monitoring technology is available [88] and no responsible entity should be excepted due to technical infeasibility.

194. NERC agrees with the CIP Assessment that logs should be reviewed frequently. However, NERC believes that a strict requirement for the review period cannot be specified because of the varied methods and technologies used to gather and review the logs. NERC asserts that automated alert technology can detect many attempts and breaches, and leave a much smaller set of ''questionable'' events which can readily be analyzed manually.[89]

Commission Proposal

195. The Commission is persuaded by the commenters that varied technologies and locations make setting a ''one size fits all'' frequency of access log review requirement difficult. However, the Commission believes 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. Thus, regular manual review is beneficial.

196. The Commission believes that frequent reviews of access logs are necessary to detect breaches that automated alerts do not detect. Moreover, where automated alerts are not used, frequent monitoring takes on even greater importance. The Commission recognizes that accessibility of an access log may affect the review interval. For instance, logs that are readily available, 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. However, 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.

197. For the reasons discussed above, the Commission believes that more frequent review of access logs is important and therefore proposes 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 believes such review should be performed at least weekly. As part of developing this bifurcated review requirement, the ERO must 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.

d. Vulnerability Assessments

198. The CIP Assessment stated that Requirement R4 fails to specify whether a live vulnerability assessment is required, as opposed to a paper assessment.[90] It recommends performing a ''live'' cyber vulnerability assessment at least annually and developing an action plan to remediate any weaknesses identified. It also notes that permitting a one year window, without any specificity regarding updates, could be inadequate.

199. NERC, Progress Energy and ReliabilityFirst state that Requirement R4 intentionally allows for either vulnerability assessment approach, live or paper-based, to allow a responsible entity to determine the approach best suited to its own level of sophistication and tolerance for risk. NERC acknowledges that some responsible entities already perform live testing but notes that such testing is limited to specific systems and circumstances of the responsible entity.

200. Georgia System argues that the existing Requirement R4 is well-designed. It suggests, however, that annual testing of each electronic access point should not be imposed, because such wide-spread ''live'' testing could have adverse impacts on system reliability. APPA/LPPC disagree with the CIP Assessment and insist that an annual testing requirement is sufficient, as long as the responsible entity does not make changes to any border devices. APPA/LPPC argue that, if changes occur to the perimeter, then the entity should, as a good business practice, reassess the vulnerability of that portion of the perimeter.

Commission Proposal

201. The Commission believes that annual vulnerability assessments are sufficient, provided that no modifications are made to the electronic security perimeter during the year. However, 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. Thus, the Commission proposes 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

[88] Technology that is currently available for monitoring access (*e.g.,* network servers, firewalls, Intrusion Detection Systems, Intrusion Prevention Systems) has alarm capability built into it.

[89] FirstEnergy, ReliabilityFirst, ISO/RTO Council, Georgia System, Xcel, and Santa Clara agree with NERC.

[90] A live vulnerability assessment typically involves the use of specialized software or hardware to scan electronic access points to determine which communications each access point allows to pass through.

modifications to the electronic security perimeter or defense in depth strategy.

202. In addition, the Commission proposes that Requirement R4 should provide for the conduct of live vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years. If such live vulnerability assessments are not ''technically feasible,'' consistent with the Commission's earlier determination, a responsible entity may seek to be excused from full compliance via an application to the Regional Entity fully documenting the necessary interim actions, milestone schedule, and mitigation plan.

e. Commission Proposal Summary

203. In summary, the Commission proposes to approve Reliability Standard CIP–005–1 as mandatory and enforceable. In addition, the Commission proposes to direct the ERO, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations, to develop modifications to CIP–005–1 through its Reliability Standards development process that (1) require implementation of a defensive security approach, including two or more defensive measures in a defense in depth posture; (2) add guidance to Requirement R2 by identifying examples of specific verification technologies that would satisfy compliance with the ''strong controls'' in Requirement R2.4, such as digital certificates and two-factor authentication, while also allowing compliance by means of technically equivalent measures; (3) evaluates and provides guidance regarding the use of access security measures ''in front of'' as opposed to ''inside of'' older systems; (4) require additional controls and accountability when a responsible entity invokes the ''technical feasibility'' exception in Requirement R2.4 consistent with the proposal discussion in section II.A.5.b of the NOPR; (5) provide a bifurcated review requirement of access logs at electronic access points in which readily available logs are reviewed more frequently than 90 days including guidance on which assets should be designated ''readily accessible;'' (6) require a vulnerability assessment of electronic access points as part of, or contemporaneously with, any modifications to an electronic security perimeter or defense in depth strategy; and (7) provide for the conduct of live vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years.

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

204. 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.[91] 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.

205. 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.

206. The Commission proposes to approve Reliability Standard CIP–006–1 as mandatory and enforceable. In addition, we propose to direct the ERO to develop modifications to this Reliability Standard. Further, the Commission also proposes to require the ERO to consider various other matters of clarification, guidance, and modification. In our discussion below, we address our concerns in the following topic areas regarding CIP–006–1: (1) Physical security plan; (2) physical access controls and monitoring physical access controls; (3) physical security breach; and (4) maintenance and testing.

a. Physical Security Plan

207. 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.

208. SPP recognizes the CIP Assessment concern with Requirement R1.1, but disagrees that the language of the Requirement needs revision. SPP maintains that while the Reliability Standard prescribes what must be done, it does not and should not prescribe how a particular Requirement is to be implemented. SPP states that NERC's FAQ document offers suggestions on how to physically secure critical cyber assets when they cannot be enclosed within a restricted access six-wall boundary. Progress Energy agrees with the CIP Assessment that NERC should provide guidance on how an alternative measure would be identified or determined adequate. However, Progress Energy contends that this guidance should not be in the Reliability Standard itself, but rather in an interpretive document like a FAQ document.

Commission Proposal

209. The Commission's current view is that the phrase ''alternative measures'' as referenced in Requirement R1.1 should be interpreted to be a Requirement exception.[92] 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, the Requirements do not provide guidance on how an alternative measure should be identified or determined to be adequate. Therefore, the Commission proposes 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.

[91] 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 * * *.''

[92] The Commission's discussion elsewhere in this NOPR, relating to discretion to make exceptions to a Requirement based on technical feasibility applies here.

b. Physical Access Controls and Monitoring Physical Access Controls

210. The CIP Assessment noted that Requirement R2 of the 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.[93] 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. The CIP Assessment suggested that, consistent with a defense in depth strategy, a layered approach would increase the complexity of an intrusion by requiring that multiple security provisions be circumvented. The CIP Assessment further suggested that such an approach would provide redundancy in case one system requires maintenance or unexpectedly fails to function as expected.

211. Xcel, FirstEnergy and others agree that redundancy and the number of layers should be a function of a reasonable risk assessment and good utility practice, which provide an objective basis for measuring compliance. They also state that unnecessary redundancy would take funds and resources away from the assets that need the elaborate redundancy.

212. Xcel agrees with the CIP Assessment that defense in depth is an optimal strategy, but states that it is not always practical. For example, Xcel notes that where a substation has cyber security equipment inside a control building surrounded by a fence, it may not be worth the cost or administrative burden to install fence detection equipment at a remote substation.

213. FirstEnergy agrees with the CIP Assessment that Requirement R2 should include a process for identifying the criticality of critical cyber assets and a process for applying an appropriate number of layers based on criticality. NERC and ReliabilityFirst point out that, throughout the Reliability Standards, assets are classified as either critical or non-critical, with no subjectivity involved in determining their ''level'' of criticality. They suggest that all assets classified as critical must be afforded the same level of protection, regardless of their location or perceived level of criticality. Consequently, they believe the specific implementation of protection must be functionally equivalent and sufficient at all locations.

Commission Proposal

214. We do not believe that the proposal to require a minimum of two different security procedures creates an unreasonable burden. We believe that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter. Use of a minimum of two different security procedures will, 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 recognizes that there is a point at which implementing multiple layers of defense becomes an unreasonable burden to responsible entities, the Commission proposes to direct the ERO to modify this 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.

c. Physical Security Breach

215. The CIP Assessment noted that Reliability Standard CIP–006–1 does not include actions to be taken in response to a physical security breach. Thus, the CIP Assessment suggested that the physical security plan specify responsibilities and required communication in such an event.

216. California PUC states that CIP–006–1 is sound, except that it does not require a plan in the contingency of a physical security breach. California PUC suggests that a guideline for such a plan should be incorporated into this Reliability Standard.

Commission Proposal

217. Below, the Commission proposes, in CIP–008–1, to direct the ERO to develop and include (in CIP–008–1) language regarding what should be included in the term ''reportable incident.'' The Commission proposes to direct the ERO, when it develops its language in Reliability Standard CIP–008–1 on the term ''reportable incident,'' to include a breach that may occur through cyber or physical means. Thus, the Commission expects that the issue of a physical security breach will be fully addressed through that proposed modification and no revision of CIP–006–1 is needed to address this issue.

d. Maintenance and Testing

218. Requirement R6, which requires a maintenance and testing program, to ensure that all physical security systems under Requirements R2, R3, and R4 function properly, is critical for the overall success of CIP–006–1. The CIP Assessment explained that, if the system's outer physical security perimeter fails to secure critical assets, the electronic access controls may be rendered ineffective. The CIP Assessment questioned whether consideration should be given to testing the more important physical security mechanisms and systems more frequently, with testing and maintenance records maintained for the full three-year testing cycle.

219. NERC and ReliabilityFirst reiterate that the Reliability Standards do not make a distinction between levels of criticality. These commenters assert that testing of more important systems cannot be performed, because all critical assets have the same level of criticality. Xcel states that a more frequent testing of the physical security perimeter is not needed because most of the equipment will be used on a weekly basis. Xcel maintains that since the equipment will be in regular use, a Requirement for additional testing of the equipment appears redundant.

220. SPP agrees with the CIP Assessment, stating that a three-year inspection cycle of physical access control is too infrequent if a critical asset has high potential impact on reliability and where such testing is not inconvenient. SPP argues that, while it may be appropriate to test the physical access controls at a remote substation once every three years, the physical access controls at a generating plant and a control center can and should be tested far more frequently. FirstEnergy also agrees with the CIP Assessment, stating that more frequent testing should be required for critical facilities, but that the Requirement should specify the form of testing that will be considered adequate.

Commission Proposal

221. Currently, Requirement R6 of CIP–006–1 requires that responsible entities 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 cycle. In addition, Requirement R6 requires retention of outage records of certain physical security systems for a

[93] CIP Assessment at 29.

minimum of one year. The Commission agrees with SPP that maintenance and testing of physical security systems should occur more frequently than once every three years. However, the Commission also agrees with SPP that such testing at remote substations should be allowed less frequently. Therefore, the Commission proposes 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 believes that this approach provides an appropriate assurance that security measures for geographically dispersed physical assets are functioning properly.

e. Commission Proposal Summary

222. In summary, the Commission proposes to approve Reliability Standard CIP–006–1 as mandatory and enforceable. In addition, the Commission proposes to direct the ERO, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations, to develop modifications to CIP–006–1 through its Reliability Standards development process that require that: (1) The ERO treats the allowance of ''alternative measures'' referenced in Requirement R1.1 as ''interim actions'' developed and implemented as part of a mitigation plan under a ''technical feasibility'' exception; (2) a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets; (3) the ERO, when it develops its language in Reliability Standard CIP–008–1 on the term ''reportable incident,'' include a breach that may occur through cyber or physical means; (4) a readily accessible critical cyber asset be tested every year with a one-year requirement for the retention of testing, maintenance, and outage records; and (5) a non-readily accessible critical cyber asset be tested in a three-year cycle with a three-year record retention requirement.

6. CIP–007–1—Systems Security Management

223. The Purpose statement in Reliability Standard 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).

224. The CIP Assessment explained that this Reliability Standard deals primarily with changes made to the operating control system [94] and verification that such changes will not inadvertently have adverse effects.[95] The CIP Assessment noted that the operating control system is vulnerable during the testing process for an indeterminate period of time prior to the installation of a patch, and an attacker could exploit the vulnerability. It explained that contracts with vendors present another security challenge. Service contracts typically provide that the vendor will test patches before allowing an entity to install them on its operating control system. The contracts also typically prohibit installation before the vendor verifies the patch, at risk of voiding the warranty. It explained that the time involved in the testing and installation of a patch may provide an attacker a window of opportunity to exploit the vulnerability that the patch is designed to prevent.

225. Another challenge the CIP Assessment identified is ensuring that the test environment accurately approximates and mirrors the operating control system. It noted that an inaccurate test environment can allow potential failures of the new product to go undetected. It noted that some entities may not have the resources to maintain a backup system, let alone a duplicate of their operating control system.

226. The Commission proposes to approve Reliability Standard CIP–007–1 as mandatory and enforceable. In addition, we propose to direct the ERO to develop modifications to this Reliability Standard. In our discussion below, the Commission addresses its concerns in the following topic areas regarding CIP–007–1: (1) Test procedures; (2) ports and services; (3) security patch management; (4) malicious software prevention; (5) security status Monitoring; (6) disposal or redeployment; (7) cyber vulnerability assessment; and (8) documentation review and maintenance.

a. Test Procedures

227. 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 or its operation. They must document that testing is performed in a manner that reflects the production environment and must document test results.

228. The CIP Assessment suggested that Requirement R1.2 should require the responsible entity to document how each significant difference between the operation and testing environments is considered and addressed.[96]

229. NERC and ReliabilityFirst comment that any test environment that has a ''significant difference'' from the production environment is not a true ''reflection'' of the production requirement, as required by the Reliability Standard. National Grid states that the need for and amount of testing will depend on the nature of the change that needs to be implemented. Flexibility to assess each situation is necessary to determine the type of testing required. National Grid states that it may not be possible to establish an isolated testing environment for all security upgrades because cyber assets in production operate continuously. A responsible entity therefore may need to take substantial steps to configure a test environment, such as taking an entire substation out of service.

Commission Proposal

230. If a testing environment does not accurately reflect the operational 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 acknowledges that this is not always possible. When it is not, any differences between the test environment and the production system should be documented. In addition, the Commission believes that responsible entities should address to the satisfaction of senior management these differences and how they propose to mitigate the impact of any differences between the testing environment and the production system. Therefore, the Commission proposes 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.

[94] The term ''operating control system'' is used in this NOPR to represent the control system used to control critical assets in real time, as opposed to backup, training, or duplicate control systems.

[95] CIP Assessment at 31.

[96] CIP Assessment at 32.

b. Ports and Services

231. Requirement R2 of CIP–007–1 requires a responsible entity to establish a process to ensure that only those ports and services required for normal and emergency operations are enabled and all others are disabled.

232. The CIP Assessment stressed that the requirement to ''disable other ports and services'' is a basic building block of a cyber security program, and that it is a generally recognized security practice to assume a ''deny all'' stance (*i.e.*, disabling all ports and services first) before opening the various ports that are needed only for operations. The CIP Assessment expressed concern that 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.'' This Requirement specifies that the responsible entity must either document (1) compensating measures to mitigate exposure or (2) an ''acceptance of risk.'' The CIP Assessment noted that in situations where technical limitations prevent unused ports and services from being disabled and risk can at best be mitigated, acceptance of risk appears to mean acceptance of vulnerabilities without further action. The CIP Assessment suggested that clear guidance is needed to explain limited circumstances for its use, and warned that accepting risk could potentially become an exception from compliance that permits unacceptable risks.

233. NERC and ReliabilityFirst comment that many situations exist where ports and services must be left open due to operating system requirements, the requirements of equipment manufacturers or vendors or the lack of information from vendors that is necessary to determine if a port or service can be disabled. APPA/LPPC agree with the CIP Assessment that closing unused ports is generally a good business practice, but they disagree that it should be mandated. They state that in some cases there may be sound technical reasons why an unused port cannot be closed. They further comment that this Requirement is acceptable as written because it allows the responsible entity to use reasonable business judgment.

Commission Proposal

234. In section II.A.5.b above, the Commission discusses the problems presented by acceptance of risk. For the reasons discussed there, the Commission proposes to direct the ERO to eliminate the acceptance of risk language from Requirement R2.3. At the same time, the Commission proposes to leave intact the exception for ''technical limitations.'' However, the Commission believes that the ''technical limitations'' language of Requirement R2.3 raises the same concerns here as the ''technical feasibility'' language referenced in section II.A.5.b. While an exception for ''technical limitations'' may be appropriate, it must include the same conditions as discussed in the context of ''technical feasibility.'' Accordingly, we propose that the same conditions and reporting requirements should apply here. Thus, the Commission proposes to direct the ERO to revise Requirement R2 and its subparts to reflect our determinations discussed above to remove the ''acceptance of risk'' language and to impose the same conditions and reporting requirements here for ''technical limitations'' as imposed elsewhere in this NOPR regarding ''technical feasibility.''

c. Security Patch Management

235. 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 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.

236. The CIP Assessment acknowledged that compensating measures are necessary at times, especially when patches require vendor support, but also expressed concern that Requirement R3.2 permits a wide variation of processes for patching a system when it allows an ''acceptance of risk'' in lieu of mitigating risk exposure through a patching program. The CIP Assessment asserted that an effective Reliability Standard cannot simply offer a responsible entity a choice between installing a patch or accepting the risk of not doing so, and that at least some form of mitigation should always be possible.

237. NERC and ReliabilityFirst believe that ''acceptance of risk'' is not a permanent solution but would be used during a period where testing and other required upgrades may be accomplished. In addition, they and other commenters are concerned about implementing language in the Reliability Standard that would seem to require installation of patches on platforms where patches cannot be implemented due to architecture, operating environment or warranty issues. Allegheny states that if patches were not applied, it is highly unlikely there would not be some form of mitigation available such as physical protection and/or firewalls. It also states that compensating measures should be in place before there is an acceptance of risk. SoCal Edison states that acceptance of the risk of non-compliance should be clearly documented so that an auditor can see the rationale for this decision.

238. PG&E comments that older devices have a limited modification capability, and as a result the responsible entity must balance the risk of replacing devices that currently operate with new, untested, and potentially inadequate devices.

Commission Proposal

239. The Commission has discussed acceptance of risk above and, because those remarks and proposals apply equally here, we propose that the ''acceptance of risk'' language must be removed here also.[97] With the exception of references to acceptance of risk, the Commission considers the provisions of Requirement R3 to be acceptable and appropriate. Patch management must be weighed in light of the risks involved, with senior management involved in the decision. As discussed under Recommendation 33 of the Blackout Report,[98] using the most 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.

d. Malicious Software Prevention

240. Requirement R4 of CIP–007–1 requires responsible entities to use anti-virus and other malicious software prevention tools. The CIP Assessment noted that Reliability Standard CIP–007–1 does not provide any direction on how to implement this type of protection or where it should be deployed, and that care must be taken to implement and test malicious code protection in order to avoid harm to the operating control system. The CIP Assessment pointed out that the Reliability Standard could suggest the use of a multi-layer, defense in depth strategy, to forestall or detect an attacker's penetration of the electronic security.[99]

[97] *See supra* discussion in section II.A.5.b.

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

[99] CIP Assessment at 33.

241. Requirement R4 requires the responsible entity to use anti-virus software and malicious software prevention tools where ''technically feasible.'' The CIP Assessment questioned this phrase as allowing unnecessary discretion to opt out of Requirement R4. It noted that Requirement R4.1 raises the same concerns regarding the phrase ''acceptance of risk'' as in Requirement R3.2, this time in connection with cases where anti-virus software and malicious software prevention tools are not installed. The CIP Assessment noted a lack of direction in the Reliability Standard and sought comment on what types of compensating measures are available and what would be an adequate justification for accepting risk.

242. In response to the CIP Assessment observation that Requirement R4 does not provide any direction on how to implement anti-virus protection or where it should be deployed, NERC and ReliabilityFirst comment that the Reliability Standards are performance based; that they do not specify how to perform a function, only that the Requirement must be met. This comment is similar to the suggestion addressed in Order No. 672,[100] that, ''in general, a Reliability Standard should address the 'what' and not the 'how' of reliability and that the actual implementation of a Reliability Standard should be left to entities such as control area operators and system planners * * *.'' [101] NERC and ReliabilityFirst conclude that, while the responsible entity must implement a solution that meets the Requirement, it should not be restricted with regard to how to do so. Thus, they argue the Reliability Standard should remain silent as to whether the anti-virus solution is implemented at the electronic security perimeter border, on an in-line device, or on the critical cyber asset itself, so long as the implemented solution meets the stated requirement.

243. In response to the CIP Assessment comment that the Reliability Standard does not suggest the use of a multi-layered, defense in depth strategy through the use of various products from multiple vendors, NERC and ReliabilityFirst state that a multi-layered defense may be appropriate in a best practice document, but not in a mandatory Reliability Standard.

Commission Proposal

244. The Commission has discussed the issues of defense in depth, technical feasibility, and risk acceptance elsewhere above in this NOPR. The remarks and proposals there apply equally to the issue of malicious software prevention. Therefore, the ''acceptance of risk'' language must be removed here, and the same conditions and reporting requirements regarding ''technical feasibility'' that apply elsewhere are applicable here. In addition, the Commission proposes to direct the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software in to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means.

e. Security Status Monitoring

245. 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.

246. The CIP Assessment questioned the need to limit Requirement R6.3, which requires logs of system events related to cyber security to support incident reporting, as specified in CIP–008–1, to situations where this is ''technically feasible.'' The CIP Assessment also raised concerns about the record retention requirements for Requirements R6.3 and R6.4, which pertain to logs of cyber security-related system events used to identify reportable incidents and to support incident response, as required in CIP–008–1. It noted that, depending upon the frequency of log review, the 90-day period specified may be inadequate and that frequent review of logs would facilitate the early detection of reportable incidents. It also would ensure that current data are available for forensics. The CIP Assessment sought comment on whether the Reliability Standard should address the frequency and scope of the review of system event logs related to cyber security that is required by Requirement R6.5. It also noted the lack of guidance on how data should be saved, backed up and stored where computerized cyber incident monitoring and logging is performed.

247. Several commenters state that all devices of interest do not have the capability to create logs or that they may not provide the capability to capture ''security related'' information. They state that many installed devices in power plants and substations do not have log generation capability. If there is no capacity to generate logs, then it is technically infeasible to maintain logs.

248. NERC and ReliabilityFirst comment that generated logs from remote locations may not be readily collected for frequent review. In many cases, the telecommunications infrastructure connecting these remote locations cannot support the rapid and frequent collection of log data, especially if it is voluminous. The remote location of some sites makes frequent visits to collect and store log data impractical.

249. SPP recommends that logs be transferred in real time to a separate logging system to mitigate the risk of a successful attack destroying evidence of the intrusion. Where possible, the log should be readable separately from the device that created it or the device should be able to continue logging while in playback mode. Wisconsin Electric submits that cyber security logs should be reviewed with the frequency necessary to identify a cyber security incident within the timeframe established in the entity's cyber security incident response plan. The cyber security logs should be stored in a manner that assures that information is protected as required in CIP–003–1 and that it is available through the 90-day retention period.

Commission Proposal

250. We have discussed the issue of technical feasibility. Our remarks and proposals there apply equally to the technical feasibility of monitoring and logging of system events related to cyber security.

251. The Commission agrees with the CIP Assessment and Wisconsin Electric that logs should be reviewed with the frequency necessary to ensure timely identification of a cyber security incident. Simply reviewing logs at the end of the retention period will not ensure an appropriate level of security because it does not permit effective response to all incidents. We note that

[100] FERC Stats. & Regs. ¶ 31,204 at P 260.

[101] In Order No. 672, the Commission immediately followed this general statement with the caution that, ''in other situations, however, the 'how' may be inextricably linked to the Reliability Standard and may need to be specified by the ERO to ensure the enforcement of the Reliability Standard.'' Order No. 672 at P 265.

this issue of log review touches on Blackout Report Recommendation 35, which addresses network monitoring, and Recommendation 37 which addresses diagnostic capabilities.[102] The Commission therefore proposes 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. This direction should be completed consistent with our discussion above regarding ''readily accessible'' assets.[103] Accessibility should take into account both physical remoteness and available communications channels. We would expect control centers to fall within the ''readily accessible'' category.

252. The Commission also proposes 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. 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.

f. Disposal or Redeployment

253. Requirement R7 of CIP–007–1 requires the responsible entity to establish formal methods, processes and procedures for disposal or redeployment of cyber assets. The CIP Assessment noted that erasing alone 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 quality degaussing.[104]

254. Allegheny and SPP agree with the CIP Assessment that erasing alone may be inadequate because technology currently exists that allows retrieval of ''erased'' data from storage devices. SPP also states that if the magnetic media is being disposed of, physical destruction of the media is also an appropriate technique to render it unreadable.

255. NERC and ReliabilityFirst state that any method that fails to ''prevent unauthorized retrieval of sensitive cyber security or reliability data'' does not satisfy the Requirement. Likewise, APPA/LPPC believe that it is clear from the Requirement that ''erase'' means that there is no opportunity for unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it. They caution against being overly prescriptive regarding the exact process that responsible entities must use to meet this Requirement.

Commission Proposal

256. The Commission agrees with commenters that degaussing is not the sole means for achieving the goal of the requirement. As noted by commenters, the issue is less one of erasure, which is as much a method as it is a goal, than of assuring that there is no opportunity for unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it. The Commission therefore proposes to direct the ERO to modify this Requirement to clarify this point.

g. Cyber Vulnerability Assessment

257. 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. The CIP Assessment noted that this Requirement provides little direction on what features, functionality, and vulnerabilities responsible entities should focus on in a vulnerability assessment. The CIP Assessment pointed out that a poorly chosen vulnerability assessment process could result in a false sense of security. The CIP Assessment also noted that while Requirement R8.4 requires development of an action plan to remediate or mitigate vulnerabilities identified in the assessment, it does not provide a timeframe for completion of the action plan.[105]

258. Several commenters state that a responsible entity must determine the approach it will implement based on its own level of sophistication and its internal tolerance for risk. These commenters state that every environment and implementation is different, and any additional specificity would be impossible to describe for all possible situations, and, consequently, would not be productive. NERC and ReliabilityFirst state that requiring a specific timeframe for completion of an action regardless of its complexity serves no useful purpose because the timeframe will depend on the actions required. They maintain that the requirement to document the ''execution status'' of the action plan serves to keep the action plan on track.

259. ISA Group states that experience shows that most companies do not know what devices have actually been installed in the field. It maintains that a requirement for a detailed walk-down of all critical cyber assets should be mandatory for an acceptable vulnerability assessment. Progress and Xcel comment that the scope of the vulnerability test should be clearly defined.

Commission Proposal

260. The Commission believes 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. The Blackout Report recognized the importance of vulnerability assessments in Recommendation 38 that called for vulnerability assessment activities to identify weaknesses and mitigating actions.[106] The Commission believes, as noted by NERC and ReliabilityFirst, that execution status is a good means to keep the action plan on track. Therefore, the Commission proposes to require that the ERO 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.

h. Documentation Review and Maintenance

261. 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. The CIP Assessment expressed the view that the 90-day timeframe for updating documentation appears excessively long, especially when one considers that this Reliability Standard establishes a line of defense for protecting critical cyber assets and that up-to-date documentation is essential in case of an emergency.

262. NERC and ReliabilityFirst state that the 90-day time period is appropriate, given the nature and type of facilities and their locations,

[102] *See* Blackout Report at 165–166, Recommendations 35 and 37.

[103] *See* section II.B.4.c (Monitoring Access Logs) in this NOPR.

[104] CIP Assessment at 34–35. To degauss is to demagnetize. Degaussing a magnetic storage medium removes all data stored on it.

[105] CIP Assessment at 35.

[106] *See* Blackout Report at 167, Recommendation 38.

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. ReliabilityFirst adds that the 90-day period also takes into account possible management changes or extended time out of the office.

Commission Proposal

263. The Commission proposes 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 believe 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.

i. Commission Proposal Summary

264. In summary, the Commission proposes to approve Reliability Standard CIP–007–1 as mandatory and enforceable. In addition, the Commission proposes to direct the ERO, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations to develop modifications to CIP–007–1 through its Reliability Standards development process that: (1) 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; (2) revise Requirement R2 and its subparts to remove the ''acceptance of risk'' language and apply the same conditions and reporting requirements here for ''technical limitations'' as imposed elsewhere in this NOPR for ''technical feasibility;'' (3) remove the ''acceptance of risk'' provision from Requirement R3 and R4; (4) 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; (5) ensure that references to ''technical feasibility'' in CIP–007–1 are subject to the same conditions and reporting requirements discussed elsewhere; (6) 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; (7) 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; (8) revise Requirement R7 of the Reliability Standard to clarify that the issue is less one of erasure than of assuring that there is no opportunity for unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying; (9) provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments; (10) revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan; and (11) revise Requirement R9 to state that the changes resulting from modifications to the system or controls shall be documented in within 30 days.

7. CIP–008–1—Incident Reporting and Response Planning

265. 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 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.

266. The Commission proposes to approve Reliability Standard CIP–008–1 as mandatory and enforceable. In addition, we propose to direct the ERO to develop modifications to this Reliability Standard. In our discussion below, the Commission addresses its concerns in the following topic areas 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

267. The CIP Assessment noted that Requirement R1 of CIP–008–1 makes reference to reportable cyber security incidents, but it does not provide a definition of a ''reportable incident.'' Consequently, cyber security incidents may go unreported depending upon a responsible entity's interpretation of a ''reportable incident.'' [107]

268. NERC and ReliabilityFirst affirm the CIP Assessment concern, stating that each responsible entity is required to develop the required procedures for the determination of a reportable incident. They add that the definition of a reportable incident is currently undergoing extensive industry debate.

269. A number of commenters state that FERC should require NERC to clarify what types of cyber security incidents are ''reportable incidents.'' National Grid points out that the Commission should seek to ensure that any further interpretation of what is considered a reportable incident be consistent with the reporting obligations of utilities under the DOE Form 417. Allegheny suggests that, in order to maintain consistency, the DOE Form 417 reporting requirements should be referenced as part of the Reliability Standard. Progress Energy, on the other hand, states that such increased specificity is not possible and would be subject to constant revision in response to ever-changing incidents or threats to cyber systems.

Commission Proposal

270. The Commission believes that guidance regarding what should be included in the term ''reportable incident'' can be provided. The Blackout Report pointed out the need for ''uniform standards for the reporting and sharing of physical and cyber security incident information'' in Recommendation 42.[108] As NERC and ReliabilityFirst state, the definition of a ''reportable incident'' is currently undergoing extensive industry debate.

[107] CIP Assessment at 36. The CIP Assessment recognized that 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) Cyber Security Standards CIP–002–1 through CIP–009–1, March 6, 2006, page 27, question 1.

[108] *See* also Blackout Report at 168, Recommendation 42.

This debate can be a catalyst for developing an appropriate level of guidance. As noted in the NERC Glossary, a ''cyber security incident'' is defined as a compromise, or an attempt to compromise, the electronic security perimeter or physical security perimeter of a critical asset. The Commission proposes 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; [109] (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form 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.

b. Reporting

271. CIP–008–1, Requirement R1.3, requires that each responsible entity 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.

272. 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 (IAW) Standard Operating Procedure (SOP) is voluntary. The CIP Assessment noted the importance of other responsible entities receiving timely information regarding a reportable cyber security incident, so they can take precautions against being the target of a similar incident. The CIP Assessment stated that, depending upon the nature of the incident, timelines of incident reporting may be critical. It expressed concern with regard to the voluntary nature of the one-hour reporting requirement associated with ESISAC's IAW SOP. Therefore, the CIP Assessment requested comment on 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.

273. NERC and ReliabilityFirst agree that rapid reporting is desirable. However, they state that imposing a specific time period is not advisable because, when an event occurs, the need to meet a reporting deadline should not be the entity's primary concern, rather restoration of operations must take precedence. NERC and ReliabilityFirst state that ESISAC's IAW SOP is intentionally not a part of this Reliability Standard, and is classified as a guideline, because it has not been through the ERO standards development process. These commenters believe the requirement is to report incidents to the ESISAC, with the implication that an established ESISAC reporting protocol is to be used.

274. APPA/LPPC do not believe that incorporating the ESISAC one-hour reporting limit or any other deadline would provide adequate time for another responsible entity to take meaningful precautions to prevent a cyber attack. Cyber attacks are designed to occur nearly simultaneously in more than one location. Thus, even an extremely short deadline, such as one minute, is unlikely to provide other responsible entities time to take precautions. Nonetheless, APPA/LPPC suggest that, if a deadline is prescribed, it should run from the discovery of the incident by the responsible entity, and not from the occurrence of the incident.

275. Several commenters argue against any time limit for reporting security incidents. They believe the requirement to report such incidents to the ESISAC is sufficient. Wisconsin Electric notes that using the same one-hour limit in CIP 008–1 as in the ESISAC IAW SOP would not represent a new performance threshold to the industry.

Commission Proposal

276. The Commission believes that the ESISAC one-hour reporting limit is reasonable and proposes that it be incorporated into CIP 008–1. We reach this conclusion for several reasons. First, although it is true that cyber attacks against different entities could occur simultaneously, it would still be extremely useful to those attempting to defend against those attacks to know what kind of threat they are dealing with. The fact that simultaneous attacks are directed at other entities would be important information about the nature of the attacks.

277. Second, 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.

278. Third, the Commission disagrees with commenters that believe that a reporting limit will not provide others with time for responsive action to mitigate other potential Cyber Security Incidents. While a reporting time limit may not allow such mitigation in every situation, it very well could allow such mitigation in many situations.

279. Fourth, although ESISAC's time limit is voluntary, a one hour NERC reporting time limit would match up with the ESISAC reporting time limit and, thus, would avoid conflicting requirements and would not cause any new reporting burden.

280. Thus, the Commission proposes to direct the ERO to modify CIP–008–1 to require a 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. While we leave development of the details to NERC, the Commission agrees with APPA/LPPC that the reporting timeframe should run from the discovery of the incident by the responsible entity, and not the occurrence of the incident.

c. Full Operational Exercises and Lessons Learned

281. The CIP Assessment stated that the annual testing of the Incident Response Plan should require full operational exercises due to the potential for such exercises to uncover unforeseen complications.[110] In addition, it indicated that 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.

282. NERC and ReliabilityFirst state that there are many instances in substations or power plants where backup or fully functional test systems do not exist, making a full operational exercise an extremely risky proposition. Because of this, NERC and ReliabilityFirst believe that a universal requirement for a full operational exercise may be unduly disruptive and burdensome to reliable operations, and represent a threat to the overall reliability of the Bulk-Power System. NERC and ReliabilityFirst believe that table-top exercises are sufficient to test the effectiveness of an Incident Response Plan. Several commenters agree. Ontario IESO posits that there is no evidence that a paper drill would be materially inferior to an operational exercise.

[109] The Commission emphasizes that a cyber security incident that does not result in a material loss of physical assets should not prevent the incident from being reported.

[110] CIP Assessment at 37.

283. A number of commenters believe that requiring a full operational exercise during the three-year documentation cycle and paper drills during the other two years should provide the desired benefits of testing the Incident Response Plan. An actual incident response would satisfy the need for a full operational exercise during a three-year cycle. One commenter, the ISA Group, believes that full operational exercises should be mandated at least yearly. Wisconsin Electric states that, if full drills become a requirement, they should be conducted every five years, with paper drills only when the process or procedure is created or changed.

284. Several commenters note that there may be a significant benefit in executing an operational exercise over a paper drill, but note that an operational exercise also can require expensive back-up systems and may unnecessarily risk damaging system functionality in case of an error or unforeseen system effect. Georgia System believes each responsible entity has to determine whether the incremental benefit from a yearly exercise is worth the costs and reliability risks associated with the exercise. MidAmerican states it could support full operational exercises for a limited number of critical assets, with paper exercises for the remaining facilities. National Grid suggests that operational drills are more appropriate for actual recovery plans under CIP–009–1, and paper drills are more than adequate to assess whether the response plans under CIP–008–1 identify and alert the right responders. Xcel Energy is concerned that operational drills (like vulnerability tests) could cause an inadvertent disruption to EMS and SCADA systems.

285. NERC and ReliabilityFirst state that collection and maintenance of lessons learned, and plan improvement are included in the ''update'' language of Requirement R1.4. Allegheny states that documentation and implementation of lessons learned is a critical part of any incident response or drill. As such, Allegheny believes the need to maintain a collection of lessons learned as a result of testing the Incident Response Plan and to apply them to plan improvements is necessary to ensure response plans remain viable. Wisconsin Electric submits that lessons learned from incident response exercises should be documented as well as audited for completion of any enhancements to the process.

Commission Proposal

286. We understand from commenters that annual testing may be costly and disruptive. Nonetheless, periodic operational drills are important because they may reveal weaknesses, vulnerabilities, and opportunity for improvement that a paper drill would not identify. The Commission agrees with the commenters that suggest 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. We believe this strikes an appropriate balance between the benefits of executing an operational exercise and the associated costs and potential risks of misoperations. Therefore, the Commission proposes 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 technical feasibility parameters discussed earlier in section II.A.5.b. Further, the Commission proposes to direct the ERO to provide guidance on the meaning of the term ''full operational exercise.'' [111]

287. The Commission believes that industry will benefit from a requirement to document and implement lessons learned from testing or responses to actual cyber security incidents. Although NERC and ReliabilityFirst suggest that this is included in the ''update'' language of Requirement R1.4, we believe that the Reliability Standard would be improved by making a ''lessons learned'' requirement explicit. Therefore, the Commission proposes to direct that the ERO 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 proposes to direct the ERO to include language to require revisions to the Incident Response Plan to address these lessons learned.

d. Commission Proposal Summary

288. In summary, the Commission proposes to approve Reliability Standard CIP–008–1 as mandatory and enforceable. In addition, the Commission proposes to direct the ERO, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations to develop modifications to CIP–008–1 through its Reliability Standards development process that: (1) Develop and include language regarding the term ''reportable incident'' 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 417; (3) recognize that the term ''reportable incident'' should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced; (5) require a responsible entity to contact appropriate government authorities and industry participants in the event of a Cyber Security Incident as soon as possible, but at least within one hour of the event, even if it is a preliminary report; (6) 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 technical feasibility parameters discussed earlier herein and provide guidance on the meaning of the term ''full operational exercise;'' (7) refine 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; and (8) require revisions to the Incident Response Plan to address the lessons learned.

8. CIP–009–1—Recovery Plans for Critical Cyber Assets

289. 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 establishes required development, updating, and testing of recovery plans, as well as storage and testing of associated backup data and backup media.

290. The Commission proposes to approve Reliability Standard CIP–009–1 as mandatory and enforceable. In addition, we propose to direct the ERO to develop modifications to this Reliability Standard. Further, the Commission also proposes to require the ERO to consider various other matters of clarification, guidance, and modification. In our discussion below, the Commission addresses its concerns in the following topic areas regarding CIP–009–1: (1) Recovery plans; (2) forensic data collection; (3) operational exercises; (4) recovery plan updates; (5) backup and storage of restoration data and (6) testing of backup media.

[111] We address the meaning of the term ''full operational exercise'' in section II.B.8.c below.

a. Recovery Plans

291. Requirement R1 of CIP–009–1 requires the responsible entity to create and annually review recovery plans for critical cyber assets. The CIP Assessment expressed concern that the ''events or conditions of varying duration and severity that would activate the recovery plan(s)'' 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.

292. NERC, MidAmerican, Xcel, and Allegheny comment that providing additional detail will limit the scope of potential ''precipitating events'' addressed by recovery plans, and will not provide for the needed flexibility. NERC states that the determination of which events warrant a recovery plan is intentionally left to the discretion of responsible entities. Wisconsin Electric and others agree with the CIP Assessment that additional clarification should be added to this Requirement.

Commission Proposal

293. The Commission shares the concern that ''precipitating events'' are readily recognized by responsible entities so that recovery plans are promptly implemented. While we do not propose to require modifications regarding the ''events and conditions'' language at this time, we do note that Requirement R1 fails to state that the plans it requires must be implemented when needed. That is, it requires that recovery plans must be ''created and reviewed'' but does not explicitly require actual implementation when the ''events or conditions of varying duration and severity'' occur. We propose to direct the ERO to modify to CIP–009–1 to include this requirement. 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.

b. Forensic Data Collection

294. The CIP Assessment pointed out that Requirement R1 does not provide guidance on whether and how the recovery plans should preserve data for forensics purposes. In particular, Requirement R1 does not specify whether forensics collection should occur prior to, contemporaneously with, or after recovery of the critical cyber assets.

295. NERC, ReliabilityFirst, and PG&E assert that there are no Bulk-Power System reliability issues associated with forensic data collection, and that there is a possibility that collection of forensic data could impede the restoration of cyber assets, which in turn could affect the reliable operation of the Bulk-Power System. NERC comments that each entity must consider the balance between data collection and actions required to rapidly restore the electric power transmission. NERC states that after-the-fact recovery of incident data cannot be assumed to be technically possible on legacy equipment and that, therefore, it cannot be a requirement. Georgia System stresses that restoring the Bulk-Power System should remain the foremost objective of all immediate efforts, over issues of data collection.

296. Allegheny comments that forensics collection should also be addressed within this range of plans. Noting again that one size does not fit all in regards to scenarios for recovery planning, Allegheny says that forensic collection should be addressed in each of the plans that addresses the various scenarios.

Commission Proposal

297. The Commission is concerned that Requirement R1 of CIP–009–1 does not require the collection of forensics data and does not address how such collection activities relate to restoration of service efforts. The Commission believes that concern for the reliability of the Bulk-Power System requires attention to forensics data collection. The Blackout Report also emphasized the need to improve forensics and diagnostic capabilities in Recommendation 37.[112] 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. 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. Technical capabilities to do so will likely vary with the facility, and many legacy systems present considerable technical limitations in this regard. In the interest of ''raising the bar'' above what the least capable equipment can do to collect forensic data, the Commission proposes to direct the ERO to modify CIP–009–1 to incorporate use of good forensic data collection practices into this CIP Reliability Standard.

298. In addition, we agree with commenters 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. Nonetheless, 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 data may not be ''technically feasible'' for all situations due to equipment limitations, such as older substation installations with little electronic monitoring. Therefore, we suggest that forensic data collection is an appropriate candidate for the ''where technically feasible'' exception clause, where, if invoked, the responsible entity would be required to propose interim actions, milestone schedules, and a mitigation plan, as described elsewhere in this NOPR. We agree with commenters that the recovery plans should include forensic data collection procedures. Therefore, we propose 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.

c. Operational Exercises

299. 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, to recovery from an actual incident. The CIP Assessment asked whether full operational exercises should be required to aid in identifying potential problems and in realizing opportunities for improving recovery plans.[113]

300. NERC and others believe that table-top exercises (or paper drills) are sufficient, and consistent with accepted practice used to test blackstart procedures. NERC cautions that full operational exercises may be extremely risky because many substations or power plants do not have backup or fully functional test systems. NERC, therefore, believes that a universal requirement for full operational

[112] *See* Blackout Report at 166, Recommendation 37.

[113] CIP Assessment at 38.

exercises may be unduly disruptive and burdensome to reliable operations.

301. ISA Group and others support required periodic operational testing of restoration plans. California PUC recommends annual testing through a full operational exercise; and Allegheny supports operational exercises on a three-year cycle. Wisconsin Electric suggests that a one-time full operational test of the process would be beneficial. Georgia Operators supports periodic operational testing, with the caveat that each entity should determine whether the benefit is worth the costs and reliability risks associated with such an exercise. MidAmerican states that it could support full operational exercises for a limited number of critical assets.

Commission Proposal

302. The Commission agrees with the commenters that stress the benefits of operational exercises; *i.e.*, that potential problems, some of which could significantly impair reliability, will not be found without them. We do not believe that table-top exercises alone, on an ongoing basis, will suffice, given the increasing complexity and interconnection of control systems. Some commenters acknowledge the benefits of operational exercises, but believe they should occur only on a limited basis. We agree with this approach, with the cautionary note that technical feasibility and risks must be carefully weighed with the possible benefits. We acknowledge that some infrastructure facilities exist for which even limited operational exercises present unsuitable reliability risks. However, we conclude 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.

303. Accordingly, the Commission proposes to direct the ERO to develop modifications to the Reliability Standard through its Reliability Standards development process 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. Further, we propose, in conjunction with the above proposed modification, that the ERO consider the appropriateness of a ''technical feasibility'' option, in the limited fashion proposed earlier in this NOPR.[114] For example, 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 with the requisite interim actions, milestone schedules, and a mitigation plan, as described elsewhere in this NOPR.

304. We note that NERC points out a lack of clarity of the term ''full operational exercise.'' The Commission agrees and therefore proposes to direct the ERO, in conjunction with making the above modifications, 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. As NERC and ReliabilityFirst note, many operational exercise practices include table-top components in significant proportions.

d. Recovery Plan Updates

305. Requirement R3 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 event. It requires plan updates to be communicated to the personnel responsible for activating or implementing the recovery plan within 90 days of the change. The CIP Assessment noted that individuals responsible for activation and implementation of process changes in the recovery plans must have the most current information available, and questions whether a 90-day time lag is consistent with this objective.

306. NERC comments that a shorter time frame is impractical due to the number, kind and location of assets, especially field assets. Santa Clara agrees with the CIP Assessment that recovery plans must be updated as soon as possible after an event, but also states that 90 days is reasonable for completion of training for all affected personnel. Santa Clara notes that it may not be feasible to include all shift schedules of personnel in training sessions in a timeline shorter than 90 days.

307. ISO/RTO Council agrees with the CIP Assessment that that updates to such documents generally can be performed sooner than 90 days. ISO/RTO Council suggests that timely updating should be a formal component of any assessment or review process, especially with regard to after-the-fact analyses and timely application of lessons learned. ISA Group states that a 90-day time lag to activate or implement process changes in recovery plans after deficiencies are discovered is not acceptable. ISA Group suggests up to one week to identify any process workarounds and 30 days to modify equipment as necessary.

Commission Proposal

308. Requirement R3 of CIP–009–1 requires that updates to a recovery plan be communicated within 90 days to the personnel responsible for activating or implementing the recovery plan. The Commission is concerned that individuals responsible for activating and implementing the recovery plan must have the most current information available, and believes 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. Failure for such 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 proposes 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 believe a 30 day requirement for updating the recovery plans will promote timely incorporation of lessons learned during exercises and actual events. While key personnel should be informed as soon as possible, we agree with SPP and others that 90 days is reasonable for the completion of personnel training sessions, due to varied shifts schedules and other feasibility issues with regard to facility and organization.

e. Backup and Storage of Restoration Data

309. Requirement R4 requires that a recovery plan include processes and procedures for the backup and storage of information necessary to successfully restore critical cyber assets. The CIP Assessment asserted that the Requirement should specify that, when significant changes are made to the operational control system, a backup should be made for recovery purposes and that it should be tested as part of the system change before it is stored and assumed to be operational.

310. NERC and ReliabilityFirst state that this concern is mitigated by the generally accepted practice of maintaining multiple generations of backup. NERC states that ''backup made for recovery purposes'' is contained in the ''supporting configuration management activities'' clause of CIP–003–1, Requirement R6.

[114] *See* section II.A.5.b (Technical Feasibility and Acceptance of Risk).

311. Progress Energy agrees with the CIP Assessment that a backup should be tested before it is stored, but believes that the frequency of testing should be left to the discretion of the responsible entity. SPP asserts that backups should be routinely and regularly backed up, not just upon a significant change to the configuration. SPP notes that a properly configured backup and restoration testing process obviates the need to make special backups upon occurrence of the significant changes to existing critical assets defined by CIP–007–1, Requirement R1.

Commission Proposal

312. The Commission proposes to instruct the ERO to modify this Reliability Standard 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.

313. The Commission agrees with NERC that preserving multiple generations of restoration backups is common practice, and believes that competent and complete implementation of the CIP Reliability Standards would tend to include testing of recovery backups as they are created, also as a matter of good, efficient practice. However, we disagree with NERC that exercising these good practices is contained in, implied by, or readily understood from Requirement R6 of CIP–003–1. Adding language, 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. As stated above, in our discussion of the change control processes required by Requirement R6 of CIP–003–1, the Commission reiterates its position, that there is a need for enhanced direction in issues related to proper change control. The CIP Reliability Standards should specifically state that a change control process should include procedures for a tested backup. No backups of any kind are mentioned in CIP–003–1, Requirement R6.

f. Testing of Backup Media

314. Requirement R5 requires annual testing of information stored on backup media to ensure information essential to recovery is available. The CIP Assessment noted the criticality of such information being accessible in the event of an actual incident, noted 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.

315. NERC and ReliabilityFirst comment that, since the Reliability Standards cannot predict what technology will be used, they should not specify actions in response to testing. They believe that routine use of backups will serve to exercise the media more often than the specified one-year test. Likewise, Georgia System states that annual testing is more than adequate, even unnecessary, if no significant changes were made to the system; and more prescriptive Reliability Standards should be developed only if experience shows that discretion exercised in implementation of the Reliability Standards is abused.

316. Santa Clara agrees with the CIP Assessment that testing of information stored on backup media is crucial to the integrity of those backup systems. It submits that such testing could be done on a periodic basis, and in an ''off-line'' mode if necessary. Santa Clara has found it beneficial to maintain more than one set of backups so that, if the latest backup fails, the previous backup has been tested and validated, leaving a ''Plan B'' restoration solution available until the latest backup system is corrected.

317. Constellation adds that review of the backup and recovery plans is implicit if the annual review of the Cyber Security Policy already required by the CIP Reliability Standards is performed competently. SPP agrees that restoration testing is only one part of a more comprehensive backup plan, noting that the entity needs to have procedures to verify backups are successfully completed every cycle, and procedures for when the backup fails. SPP points out that failure to notice that a backup process has failed poses a far greater risk than infrequency of testing, as long as the backup process is properly managed.

Commission Proposal

318. The Commission agrees with commenters that, if these CIP Reliability Standards are implemented in a full and competent manner, then adequate backup verification measures will probably be in place. Reliability Standards, however, demand a higher degree of certainty. The proposed Reliability Standards do not provide the guidance that SPP offers—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. The Commission agrees with SPP on this point.

319. The Commission proposes to direct the ERO to modify this Reliability Standard 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. 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 agree that inability to recognize the failure of a backup process poses a great risk, and that the annual restoration testing in this Requirement is adequate as long as the backup process is properly managed.

g. Commission Proposal Summary

320. In summary, the Commission proposes to approve Reliability Standard CIP–009–1 as mandatory and enforceable. In addition, the Commission proposes to direct the ERO, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations to develop modifications to CIP–009–1 through its Reliability Standards development process that: (1) Clarify Requirement R1 to make clear that the required recovery plans must be implemented when the ''events or conditions of varying duration and severity'' occur; (2) incorporate use of good forensic data collection practices, and 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 with the parameters discussed above; (3) define in the NERC glossary the term ''full operational exercise'' or provide more direction directly in the Reliability Standard as to the parameters of the term; (4) 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 and consider the appropriateness of a technical feasibility option in connection with modified operational exercises; (5) shorten the timeline to updating recovery plans to 30 days, while continuing to allow up to 90 days to communicate those updates to responsible and affected personnel; (6) 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; and (7) provide direction that backup practices include regular procedures to ensure verification that backups are successful and available for future use.

C. Violation Risk Factors

1. Background

321. In a separate filing, NERC submitted over 1,000 Violation Risk Factors, including 162 that correspond to Requirements of the proposed CIP Reliability Standards.[115] While the Commission has addressed the Violation Risk Factors that correspond to the Requirements of the Commission-approved Reliability Standards, NERC requested that the Commission take action on the Violation Risk Factors when it takes actions on the associated Reliability Standards.[116] Accordingly, the Commission will address the Violation Risk Factors that correspond to the CIP Reliability Standards in this proceeding.

322. As part of its compliance and enforcement program, the ERO will use a three-step process to determine a monetary penalty for a standard violation. In the first of these steps, the ERO or Regional Entity will set an initial range for the base penalty amount for the violation. In order to accomplish this, the ERO or the Regional Entity will consider the applicable Violation Risk Factor [117] and Violation Severity Level [118] in the ''base penalty amount table'' in Appendix A to NERC's Sanction Guidelines. According to NERC, the base penalty amount table adds a measure of certainty for those subject to penalties and assists the ERO in executing its penalty authority.

323. NERC states that a Violation Risk Factor has been assigned to each Requirement of the Version 1 Reliability Standards to delineate the relative risk to the Bulk-Power System associated with the violation of each Requirement, and the Violation Risk Factors do not change the meaning or intent of the Reliability Standards. NERC explains that it has defined the following three levels of Violation Risk Factors: (1) High risk requirement; (2) medium risk requirement; and (3) lower risk requirement.[119]

2. Commission Proposal

324. In reviewing the proposed Violation Risk Factor assignments, the Commission has used the same guidelines it applied when evaluating NERC's submission of Violation Risk Factors as discussed in the May 18 Order. Specifically, to determine whether the proposed Violation Risk Factor assignments appropriately indicate the potential or expected impact to the reliability of the Bulk-Power System, the Commission considered: (1) Consistency with the conclusions of the Final Report on the August 14, 2003 Blackout in the United States and Canada, (2) consistency within a Reliability Standard, *i.e.*, among sub- and main Requirements of the same Reliability Standard, (3) consistency among Reliability Standards with similar Requirements, (4) consistency with NERC's proposed definition of the Violation Risk Factor level, and (5) assignment of a Violation Risk Factor level to those Requirements in certain Reliability Standards that co-mingle a higher risk reliability objective and a lesser risk reliability objective.[120]

325. Based on the application of these guidelines, and for the reasons explained below, the Commission proposes to approve the 162 proposed Violation Risk Factor assignments that correspond to the Requirements of the CIP Reliability Standards and direct NERC to revise 43 of them. In addition, the Commission notes that NERC did not assign Violation Risk Factors to the following nine Requirements and proposes to direct NERC to make these Violation Risk Factor assignments and file them for Commission approval:

CIP–002–1 Requirement R3.1
CIP–003–1 Requirement R4.1
CIP–003–1 Requirement R5.1.2
CIP–004–1 Requirement R2.2.2
CIP–004–1 Requirement R2.2.3
CIP–005–1 Requirement R1.5
CIP–007–1 Requirement R5.1
CIP–007–1 Requirement R5.3.3
CIP–007–1 Requirement R7

326. NERC has assigned a ''lower'' designation to almost 85 per cent of the Violation Risk Factors corresponding to the Requirements of the CIP Reliability Standards. No Requirements received a ''higher'' Violation Risk Factor assignment. By definition, a ''lower'' Violation Risk Factor assignment means that the Requirement is administrative in nature where a violation of the Requirement would not be expected to affect the electrical state, capability, monitoring or control of the Bulk-Power System. The Commission believes that NERC has mischaracterized many of the Requirements as ''administrative,'' resulting in a ''lower'' Violation Risk Factor assignment, where in fact a ''medium'' or ''high'' designation is more appropriate.

327. 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, 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. If an asset is critical and is not identified as such, the remaining CIP Reliability Standards will not be applied. Depending on the asset that is overlooked, and consequently not protected by the standards, a ''higher'' level of Bulk-Power System failure is possible. Thus, by NERC's definition, this Requirement should have a ''higher'' Violation Risk Factor assignment. In addition, the recommendations related to physical and cyber security contained in the Blackout Report,[121] while largely addressed by the proposed CIP Reliability Standards, would essentially be thwarted if a responsible entity does not comply with Requirements R2 and R3 of CIP–002–1. Accordingly, we are proposing to direct NERC to modify this Requirement to denote a ''higher'' Violation Risk Factor assignment.

328. 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

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

[116] *See North American Electric Reliability Corporation,* 119 FERC ¶ 61,145 (2007) (May 18 Order) (approving and modifying Violation Risk Factors).

[117] A Violation Risk Factor of lower, medium, or high is assigned to each Requirement of each mandatory Reliability Standard to associate a violation of the Requirement with its potential impact on the reliability of the Bulk-Power System.

[118] For each Requirement of a Reliability Standard, NERC will define up to four Violation Severity Levels-lower, moderate, high, and severe—as measurements of the degree to which a Requirement is violated. In a June 7, 2007 order, the Commission approved NERC's proposal to apply the current Levels of Non-Compliance in lieu of Violation Severity Levels, while NERC develops a comprehensive set of Violation Severity Levels by March 1, 2008. *North American Electric Reliability Corp.,* 119 FERC ¶ 61,248 (2007).

[119] *See May 18 Order* at P 9 (providing the complete definition of each level of Violation Risk Factor).

[120] *See* May 18 Order at P 16–36. We also note that the May 18 Order explained that this list is not necessarily comprehensive. The Commission retains the flexibility to consider additional guidelines in the future. *Id.* at n.12.

[121] Blackout Report at 163–169, Recommendations 32–44.

emergency, abnormal, or restoration conditions to lead to Bulk-Power System instability, separation, or cascading failures, nor 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, 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.[122] Thus, by NERC's definition this Requirement should have a ''higher'' Violation Risk Factor assignment. Accordingly, we are proposing to direct NERC to modify this Requirement to denote a ''higher'' Violation Risk Factor assignment.

329. The other modifications that the Commission is proposing to direct NERC to move the Violation Risk Factor from a ''lower'' to a ''medium'' assignment. The Commission's primary reason for directing these changes is 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.

330. The Commission proposes to approve the proposed Violation Risk Factor assignments filed by NERC and proposes to direct NERC to modify the Violation Risk Factors corresponding to the Requirements as illustrated in the attached list of proposed disposition actions for the proposed Violation Risk Factors.

331. We propose to direct NERC to submit a filing containing these modifications within 60 days of the date of the Final Rule. We also propose to direct NERC to include in its filing a complete Violation Risk Factor matrix. The matrix should also include assignments for the missing Violation Risk Factor assignments discussed above.

III. Information Collection Statement

332. The Office of Management and Budget (OMB) Regulations require that OMB approve certain reporting and recordkeeping (collections of information) imposed by an agency.[123] The information collection requirements proposed in this NOPR are 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.[124] In addition, OMB regulations require OMB to approve certain reporting and recordkeeping requirements imposed by agency rule.[125]

333. The ''public protection'' provisions of the Paperwork Reduction of 1995 requires 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**.

334. *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. For example, each responsible entity must develop and document a risk-based assessment methodology to identify critical assets, which is then used to develop a list of critical cyber assets (CIP–002–1). A responsible entity that identifies any critical cyber assets must also document: a cyber security policy (CIP–003–1); a security awareness program (CIP–004–1, Requirement R1); a personnel risk assessment program (CIP–004–1, Requirement R3); an electronic security perimeter and processes for control of electronic access to all electronic access points to the perimeter (CIP–005–1, Requirements R1 and R2); a physical security plan (CIP–006–1); procedures for securing certain cyber assets (CIP–007–1); and recovery plans for critical cyber assets (CIP–008–1). The above is not an exhaustive list and, in addition, the CIP Reliability Standards require responsible entities to maintain various lists and access logs.

335. 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, 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.

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 security 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

[122] *Id.*

[123] 5 CFR 1320.11.

[124] 44 U.S.C. 3507(d).

[125] 5 CFR 1320.11.

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 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 CIP Reliability Standards were approved by the NERC board in May 2006, with a designated effective date of June 1, 2006.[126] 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 CIP 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 seeks comments on the costs to comply with these requirements. It has projected 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.[127]

Title: Mandatory Reliability Standards for Critical Infrastructure Protection.

Action: Proposed collection.

OMB Control Number: To be determined.

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 proposes in this NOPR to approve eight Critical Infrastructure Protection (CIP) Reliability Standards submitted to the Commission for approval by 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. The information collections proposed in this NOPR 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.

336. *Internal Review:* The Commission has reviewed the CIP Reliability Standards proposed for approval in this NOPR and has made a preliminary determination that the proposed CIP Reliability Standards are necessary to safeguard the integrity of the nation's Bulk-Power System. The Commission has assured itself, by means of its internal review, that there is specific, objective support for the burden estimate associated with the information requirements (FERC–725B ''Mandatory Reliability Standards for Critical Infrastructure Protection'') proposed to be imposed by this NOPR.

337. Interested persons may obtain information on the reporting requirements by contacting the following: Federal Energy Regulatory Commission, 888 First Street, NE., Washington, DC 20426 (Attention: Michael Miller, Office of the Executive Director, 202–502–8415) or from the Office of Management and Budget (*Attention:* Desk Officer for the Federal Energy Regulatory Commission, fax: 202–395–7285, e-mail: *oira_submission@omb.eop.gov*).

338. Comments concerning the collection of information(s) and the associated burden estimate(s), should be sent to the contact listed above and to the Office of Management and Budget, Office of Information and Regulatory Affairs, Washington, DC 20503 [Attention: Desk Officer for the Federal Energy Regulatory Commission, phone: (202) 395–7856, fax: (202) 395–7285].

[126] 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.

[127] *See http://www.bls.gov/oes/current/naics2_22.htm.*

IV. Environmental Analysis

339. 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.[128] The Commission has categorically excluded certain actions from these requirements as not having a significant effect on the human environment.[129] 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.[130] Therefore, an environmental assessment is unnecessary and has not been prepared in this NOPR.

V. Regulatory Flexibility Act Certification

340. The Regulatory Flexibility Act of 1980 (RFA) [131] generally requires a description and analysis of final rules that will have significant economic impact on a substantial number of small entities. In a NOPR, an agency must either include an initial regulatory flexibility analysis or certify that the proposed rule will not have a ''significant impact on a substantial number of small entities.'' The Small Business Administration defines a small electric utility as one that has a total electric output of less than four million MWh in the proceeding year.

341. The RFA requires agencies in drafting a proposed rule: (1) To assess the affect that their regulation will have on small entities; (2) to analyze effective alternatives that may minimize a regulation's impact; and (3) to make their analyses available for public comment.[132] In its notice of proposed rule making (NOPR), the agency must either include an initial regulatory flexibility analysis (Initial RFA) [133] or certify that the proposed rule will not have a ''significant impact on a substantial number of small entities.'' [134]

Affect on small entities

342. Our analysis shows that the DOE's Energy Information Administration (EIA) reports that there were 3,284 electric utility companies in the United States in 2005,[135] and 3,029 of these electric utilities qualify as small entities under the 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; [136] (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.

343. As explained above, the Commission is relying on NERC's compliance registry, applying the NERC Statement of Registry Criteria, to identify entities that must comply with the CIP Reliability Standards. 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. 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 estimates that approximately 1,000 registered entities will be responsible for compliance with the CIP Reliability Standards. Of these, 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 municipal and cooperatives.

344. The Commission believes that the CIP Reliability Standards will not have a significant economic impact on a substantial number of small entities. The majority of small entities are not required to comply with mandatory Reliability Standards based on the application of the NERC Registry Criteria. Moreover, as explained above, 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 believes that the economic impact of such compliance will 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.

345. In addition, as discussed further below, while not required or proposed by this NOPR, small entities can, if they choose, collectively select a single consultant to develop model software and programs to comply with the proposals in this NOPR on their behalf. Such an approach could significantly reduce the costs that would be incurred if each company would address these issues independently.

346. While there will be some portion of small entities that will have to expend significant amounts of resources on labor and technology to comply with the CIP Reliability Standards, the Commission believes that this will be a significant minority. Further, in such circumstances, the economic impact is justified as necessary to protect cyber security assets that support Bulk-Power System reliability.

Alternatives

347. In Order No. 693, which approved 83 Reliability Standard for the Bulk-Power System, the Commission discussed several alternatives that are also applicable to the CIP Reliability Standards.[137] Several of these have already been implemented such as the approval of the NERC definition of bulk electric system, which reduces significantly the number of small entities responsible for compliance with mandatory Reliability Standards.[138] Further, the Commission adopted the NERC compliance registry process to identify the entities responsible for compliance with mandatory Reliability Standards.

348. Another significant alternative is the ability for a small entity to join a joint action agency or similar organization. Such an organization may accept responsibility for compliance with mandatory Reliability Standards on behalf of its members and also may divide the responsibility for compliance with its members. The Commission generally approved the concept of joint action agencies in Order No. 693 and directed NERC to submit implementing

[128] Order No. 486, Regulations Implementing the National Environmental Policy Act, 52 FR 47897 (Dec. 17, 1987), FERC Stats. & Regs. Preambles 1986–1990 ¶ 30,783 (1987).

[129] 18 CFR 380.4.

[130] *See* 18 CFR 380.4(a)(2)(ii), 380.4(a)(5), 380.4(a)(27).

[131] 5 U.S.C. 601–612 (2006).

[132] 5 U.S.C. 601–604 (2006).

[133] 5 U.S.C. 603(a) (2006).

[134] 5 U.S.C. 605(b) (2006).

[135] *See* Energy Information Administration Database, Form EIA–861, Dept. of Energy (2005), *available at http://www.eia.doe.gov/cneaf/electricity/page/eia861.html.*

[136] 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.

[137] *See* Order No. 693 at P 1945.

[138] *Id.* at P 75, 1945.

procedures.[139] NERC submitted revisions to its Rules of Procedure to allow for joint action agencies and similar organizations and, in an order issuing concurrently with this NOPR, the Commission approves NERC's joint action agency rules. These rules, supported by APPA, NRECA and others, will provide significant flexibility for small entities on how they will achieve compliance with the CIP Reliability Standards or to assign compliance responsibility to a central organization.

Certification

349. Based on the above analysis, the Commission certifies that the proposed rulemaking will not have a significant impact on a substantial number of small entities.

VI. Comment Procedures

350. The Commission invites interested persons to submit comments on the matters and issues proposed in this notice to be adopted, including any related matters or alternative proposals that commenters may wish to discuss. Comments are due October 5, 2007. Comments must refer to Docket No. RM06–22–000, and must include the commenter's name, the organization they represent, if applicable, and their address in their comments. Comments may be filed either in electronic or paper format.

351. Comments may be filed electronically via the eFiling link on the Commission's Web site at *http://www.ferc.gov.* The Commission accepts most standard word processing formats and requests commenters to submit comments in a text-searchable format rather than a scanned image format. Commenters filing electronically do not need to make a paper filing. Commenters that are not able to file comments electronically must send an original and 14 copies of their comments to: Federal Energy Regulatory Commission, Office of the Secretary, 888 First Street, NE., Washington, DC 20426.

352. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability section below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

VII. Document Availability

353. 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.

354. 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.

355. User assistance is available for eLibrary and the FERC's Web site during normal business hours from FERC Online Support at (202) 502–6652 (toll-free at 1–866–208–3676) or 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.*

List of Subjects in 18 CFR Part 39

Administrative practice and procedure, Electric power, Penalties, Reporting and recordkeeping requirements.

By direction of the Commission.

Kimberly D. Bose,

Secretary.

[**Note:** The following appendices will not be published in the *Code of Federal Regulations.*]

APPENDIX A

List of Commenters	
Allegheny	Allegheny Power and Allegheny Energy Supply Company.
AMP–Ohio	American Municipal Power—Ohio, Inc.
APPA/LPPC	American Public Power Association and Large Public Power Council.
ATC	American Transmission Company, LLC.
Arizona Public Service	Arizona Public Service Company.
California PUC	California Public Utilities Commission.
Cleveland Public Power	City of Cleveland, Division of Public Power.
Constellation	Constellation Energy Group, Inc.
Dominion	Dominion Resources, Inc.
Duke	Duke Energy Corporation.
EEI	Edison Electric Institute.
EPSA	Electric Power Supply Association.
FirstEnergy	FirstEnergy Service Company.
Georgia System	Georgia System Operations Corporation.
ISA Group	Three members of the ISA–SP99.05 Leadership Group (Instrument Society of America).
ISO/RTO Council	ISO/RTO Council.
ISO–NE	ISO New England Inc.
MEAG Power	MEAG Power Motion to Intervene.
MidAmerican	MidAmerican Electric Operating Companies.
MITRE	MITRE Corporation.
National Grid	National Grid USA.
NERC	North American Electric Reliability Corporation.
NIST	National Institute of Standards and Technology.
Northeast Utilities	Northeast Utilities Service Company (on behalf of its transmission owning affiliates, the NU Companies).
NRECA	National Rural Electric Cooperative Association.
Ontario IESO	Ontario Independent Electricity System Operator.
PG&E	Pacific Gas and Electric Company.
PJM	PJM Interconnection, LLC.

[139] *Id.* at P 107.

APPENDIX A—Continued

List of Commenters	
Progress Energy	Progress Energy, Inc.
ReliabilityFirst	ReliabilityFirst Corporation.
Santa Clara	City of Santa Clara, for its municipal Silicon Valley Power.
SoCal Edison	Southern California Edison Company.
Southern	Southern Company Services, Inc.
Southwest TDUs	Southwest Transmission Dependent Utility Group.
SPP	Southwest Power Pool, Inc.
Tampa Electric	Tampa Electric Company.
Wisconsin Electric	Wisconsin Electric Power Company.
Xcel	Xcel Energy Services, Inc.

APPENDIX B.—VIOLATION RISK FACTORS: PROPOSED DISPOSITIONS

Standard No.	Requirement No.	Text of requirement	Violation risk factor		Guideline
			NERC proposal	Commission determination	
CIP–002–1	R1	Critical Asset Identification Method—The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	LOWER	MEDIUM	1, 3, 4
CIP–002–1	R1.2	The risk-based assessment shall consider the following assets:	LOWER	MEDIUM	2
CIP–002–1	R2	Critical Asset Identification—The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary	LOWER	HIGH	1, 3, 4
CIP–002–1	R3	Critical Cyber Asset Identification—Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Reliability Standard CIP–002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	MEDIUM	HIGH	1, 3, 4
CIP–003–1	R1	Cyber Security Policy—The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	LOWER	MEDIUM	1
CIP–003–1	R2	Leadership—The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Reliability Standards CIP–002 through CIP–009.	LOWER	MEDIUM	1
CIP–003–1	R4	Information Protection—The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	LOWER	MEDIUM	1
CIP–004–1	R2.1	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within 90 calendar days of such authorization.	LOWER	MEDIUM	1
CIP–004–1	R2.2	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP–004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	LOWER	MEDIUM	1, 2

APPENDIX B.—VIOLATION RISK FACTORS: PROPOSED DISPOSITIONS—Continued

Standard No.	Requirement No.	Text of requirement	Violation risk factor		Guideline
			NERC proposal	Commission determination	
CIP–004–1	R2.2.4	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	LOWER	MEDIUM	1, 4
CIP–004–1	R3	Personnel Risk Assessment—The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within 30 days of such personnel being granted such access. Such program shall at a minimum include:	LOWER	MEDIUM	1, 3, 4
CIP–004–1	R4.2	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	LOWER	MEDIUM	1, 3, 4
CIP–005–1	R1.1	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	LOWER	MEDIUM	1, 2, 4
CIP–005–1	R1.2	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	LOWER	MEDIUM	1, 2, 4
CIP–005–1	R1.3	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	LOWER	MEDIUM	1, 2, 4
CIP–005–1	R1.4	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Reliability Standard CIP–005.	LOWER	MEDIUM	1, 2, 4
CIP–005–1	R2	Electronic Access Controls—The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	LOWER	MEDIUM	1, 2, 4
CIP–005–1	R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	LOWER	MEDIUM	1, 2
CIP–005–1	R3	Monitoring Electronic Access—The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	LOWER	MEDIUM	1, 2
CIP–005–1	R3.1	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	LOWER	MEDIUM	1
CIP–005–1	R3.2	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every 90 calendar days.	LOWER	MEDIUM	1

APPENDIX B.—VIOLATION RISK FACTORS: PROPOSED DISPOSITIONS—Continued

Standard No.	Requirement No.	Text of requirement	Violation risk factor		Guideline
			NERC proposal	Commission determination	
CIP–005–1	R4	Cyber Vulnerability Assessment—The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	LOWER	MEDIUM	1, 2
CIP–005–1	R4.2	A review to verify that only ports and services required for operations at these access points are enabled.	LOWER	MEDIUM	1, 2
CIP–005–1	R4.3	The discovery of all access points to the Electronic Security Perimeter;	LOWER	MEDIUM	1, 2
CIP–005–1	R4.4	A review of controls for default accounts, passwords, and network management community strings; and	LOWER	MEDIUM	1, 2
CIP–005–1	R4.5	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	LOWER	MEDIUM	1, 4
CIP–006–1	R1.5	Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP–004 Requirement R4.	LOWER	MEDIUM	1, 3
CIP–006–1	R6.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	LOWER	MEDIUM	2
CIP–007–1	R1.1	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	LOWER	MEDIUM	1, 2
CIP–007–1	R2	Ports and Services—The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	LOWER	MEDIUM	1, 2
CIP–007–1	R2.3	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	LOWER	MEDIUM	1, 2
CIP–007–1	R4	Malicious Software Prevention—The Responsible Entity shall use anti-virus software and other malicious software (''malware'') prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	LOWER	MEDIUM	1, 2
CIP–007–1	R4.1	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	LOWER	MEDIUM	1, 2
CIP–007–1	R4.2	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention ''signatures.'' The process must address testing and installing the signatures.	LOWER	MEDIUM	1, 2
CIP–007–1	R5.1.3	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Reliability Standard CIP–003 Requirement R5 and Reliability Standard CIP–004 Requirement R4.	LOWER	MEDIUM	1, 2
CIP–007–1	R5.2.1	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	LOWER	MEDIUM	1, 2
CIP–007–1	R5.2.3	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	LOWER	MEDIUM	1, 2

APPENDIX B.—VIOLATION RISK FACTORS: PROPOSED DISPOSITIONS—Continued

Standard No.	Requirement No.	Text of requirement	Violation risk factor		Guideline
			NERC proposal	Commission determination	
CIP–007–1	R6.1	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	LOWER	MEDIUM	1, 2
CIP–007–1	R6.2	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	LOWER	MEDIUM	1, 2
CIP–007–1	R6.3	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Reliability Standard CIP–008.	LOWER	MEDIUM	1, 2
CIP–007–1	R8.2	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	LOWER	MEDIUM	1, 3
CIP–007–1	R8.3	A review of controls for default accounts; and	LOWER	MEDIUM	1, 3
CIP–007–1	R8.4	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	LOWER	MEDIUM	1, 2, 3

[FR Doc. E7–14710 Filed 8–3–07; 8:45 am]
BILLING CODE 6717–01–P