Supporting Statement for

FERC-725B, Mandatory Reliability Standards for Critical Infrastructure Protection

As Proposed in Docket No. RM06-22-000
(A Final Rule Issued January 18, 2008)

The Federal Energy Regulatory Commission (Commission) (FERC) requests that the Office of Management and Budget (OMB) review and approve **FERC-725B, Mandatory Reliability Standards for Critical Infrastructure Protection**, for a three year period. FERC-725B (Control No. 1902-0248) is a new Commission data collection, (filing requirements), as contained in 18 Code of Federal Regulations, Part 40.

FERC-725B implements standards that were previously part of a voluntary program. The Commission requests that OMB approve the projected estimates reported in this submission. There are no changes to what the Commission proposed when it submitted the NOPR for review and approval. The Commission's estimates are based on the potential number of entities who will have to come into compliance with the mandatory standards. The Commission will revise these estimates for these requirements as the ERO completes its registration process and as mandatory standards are updated and enforced.

Compliance with these Reliability Standards will be mandatory and enforceable for the applicable categories of entities identified in each Reliability Standard. The Reliability Standards approved in this Final Rule are necessary for the reliable operation of the nation's interconnected Bulk-Power System.

Background

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.[1] 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.[2]

In the aftermath of the 1965 Blackout in the northeast United States, the electric industry established the North American Electric Reliability Council (NERC), a voluntary reliability organization. Since its inception, NERC has developed Operating Policies and Planning Standards that provide voluntary guidelines for operating and planning the North American bulk-power system. In April 2005, NERC adopted "Version O" reliability standards that translated the NERC Operating Policies, Planning Standards and compliance requirements into a comprehensible set of measurable standards. While NERC has developed a compliance

1 Energy Policy Act of 2005, Pub. L. No. 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005), 16 U.S.C. 824o.
2 16 U.S.C. 824o(e)(3).

enforcement program to ensure compliance with the reliability standards it developed, industry compliance has been voluntary and not subject to mandatory enforcement penalties. Although NERC's efforts have been important in maintaining the reliability of the nation's bulk-power system, NERC itself has recognized the need for mandatory, enforceable reliability standards and has been a proponent of legislation to establish a FERC-jurisdictional ERO that would propose and enforce mandatory reliability standards.

On February 3, 2006, the Commission issued Order No. 672, implementing section 215 of the FPA.[3] Pursuant to Order No. 672, the Commission certified one organization, NERC, as the ERO.[4] 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.

RM06-22-000 NOPR

On July 20, 2007 the Commission issued a NOPR proposing to approve eight Critical Infrastructure Protection (CIP) Reliability Standards submitted by the North American Electric Reliability Corporation (NERC) for Commission approval. 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, in accordance with section 215(d)(5) of the FPA, the Commission proposed 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.

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.[5] Only Reliability Standards approved by the Commission will become mandatory and enforceable.

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, see Attachment A. Glossary of Terms of this submission), transmission owners and operators, and generation owners and operators that perform defined functions. Specifically, it established a self-certification process relating to the

3 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).

4 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).

5 Section 215(d)(5) of the FPA.

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.

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

- **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.

6 The Reliability Standards are not to be codified in the CFR and are not attached to the Final Rule. They are, however, available on the Commission's eLibrary document retrieval system in Docket No. RM06-22-000 and are available on the ERO's website, http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection.

- **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.

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

Each 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.

RM06-22-000 Final Rule

On January 18, 2008 the Commission issued a Final Rule approving the eight Critical Infrastructure Protection (CIP) Reliability Standards submitted by the NERC for the Commission's approval. In addition, the Commission is approving NERC's implementation plan that sets milestones for responsible entities to achieve full compliance with the CIP Reliability Standards. The Commission is also directing NERC to develop modifications to the CIP Reliability Standards through its Reliability Standards development process to address specific concerns identified by the Commission. Similar to the Commission's approach in Order No. 693, it views such directives as a separate action from approval, consistent with the Commission's authority in section 215(d) (5) of the FPA to direct the ERO to develop a modification to a Reliability Standard.

Other determinations in the Final Rule include:

- A directive that the ERO must develop modifications to the CIP Reliability Standards to remove the "reasonable business judgment" language. (See item no. 8)

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

- The ERO is directed to develop specific conditions that a responsible entity must satisfy to invoke the "technical

feasibility" exception. This structure for use of the technical feasibility exception allows flexibility and customization of implementation of the CIP Reliability Standards in a controlled manner.

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

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

A. Justification

1. CIRCUMSTANCES THAT MAKE THE COLLECTION OF INFORMATION NECESSARY

EPAct 2005 added a new section 215 to the FPA, which provides for a system of mandatory and enforceable Reliability Standards. Section 215(d)(1) of the FPA provides that the ERO must file each Reliability Standard or modification to a Reliability Standard that it proposes to be made effective, i.e., mandatory and enforceable, with the Commission. As mentioned above, on April 4, 2006, and as later modified and supplemented, the ERO submitted 107 Reliability Standards for Commission approval pursuant to section 215(d) of the FPA.

Section 215(d)(2) of the FPA provides that the Commission may approve, by rule or order, a proposed Reliability Standard or modification to a proposed Reliability Standard if it meets the statutory standard for approval, giving due weight to the technical expertise of the ERO. Alternatively, the Commission may remand a Reliability Standard pursuant to section 215(d)(4) of the FPA. Further, the Commission may order the ERO to submit to the Commission a proposed Reliability Standard or a modification to a Reliability Standard that addresses a specific matter if the Commission considers such a new or modified Reliability Standard appropriate to "carry out" section 215 of the FPA.[7] The Commission's action in this Proposed Rule is based on its authority pursuant to section 215 of the FPA.

Recent Events

A common cause of past major regional blackouts was violation of NERC's then Operating Policies and Planning Standards. During July and August 1996, the west coast of the United States experienced two cascading blackouts caused by violations of voluntary Operating Policies.[8] In response to the outages, the Secretary of Energy convened a task force to advise

7 See 16 U.S.C. 824o(d)(5) (2006).

8 The Electric Power Outages in the Western United States, July 2-3, 1996, at 76

the Department of Energy (DOE) on issues needed to be addressed to maintain the reliability of the bulk-power system. In a September 1998 report, the task force recommended, among other things, that federal legislation should grant more explicit authority for FERC to approve and oversee an organization having responsibility for bulk-power reliability standards.[9] Further, the task force recommended that such legislation provide for Commission jurisdiction for reliability of the bulk-power system and FERC implementation of mandatory, enforceable reliability standards.

Electric reliability legislation was first proposed after issuance of the September 1998 task force report and was a common feature of comprehensive electricity bills since that time. A stand-alone electric reliability bill was passed by the Senate unanimously in 2000. In 2001, President Bush proposed making electric Reliability Standards mandatory and enforceable as part of the National Energy Policy.[10]

Under the new electric power reliability system enacted by the Congress, the United States will no longer rely on voluntary compliance by participants in the electric industry with industry reliability requirements for operating and planning the Bulk-Power System. Congress directed the development of mandatory, Commission-approved, enforceable electricity Reliability Standards. The Commission believes that, to achieve this goal, it is necessary to have a strong ERO that promotes excellence in the development and enforcement of Reliability Standards.

A mandatory Reliability Standard should not reflect the "lowest common denominator" in order to achieve a consensus among participants in the ERO's Reliability Standard development process. Therefore, the Commission will carefully review each Reliability Standard submitted and, where appropriate, later remand if necessary, an inadequate Reliability Standard to ensure that it protects reliability, has no undue adverse effect on competition, and can be enforced in a clear and even-handed manner.

A key to the successful cyber protection of the Bulk-Power System is 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,

---

(ftp://www.nerc.com/pub/sys/all_updl/docs/pubs/doerept.pdf) and WSCC Disturbance Report, For the Power System outage that Occurred on the Western Interconnection August 10, 1996, at 4 (ftp://www.nerc.com/pub/sys/all_updl/docs/pubs/AUG10FIN.pdf).

9 Maintaining Reliability in a Competitive U.S. Electricity Industry, Final report of the Task Force on Electric System Reliability, Secretary of Energy Advisory Board, U.S. Department of Energy (September 1998), at 25-27, 65-67.

10 Report of the National Energy Policy Development Group, May 2001, at p. 7-6.

developed specific recommendations for the improving the then-current voluntary standards and development of new Reliability Standards.[11]

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.[12] The CIP Reliability Standards address these and related topics.

CIP Assessment

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.

As the Commission 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.[13] Likewise, in this Final Rule, 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.

The Commission recognizes 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 has evaluated the CIP Reliability Standards in the context of the above over-arching considerations.

11 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.

12 See Blackout Report at 163-169, Recommendations 32-44.

13 See Order No. 693 at P 234.

2. HOW, BY WHOM, AND FOR WHAT PURPOSE THE INFORMATION IS TO BE USED AND THE CONSEQUENCES OF NOT COLLECTING THE INFORMATION

Prior to enactment of section 215, FERC had acted primarily as an economic regulator of wholesale power markets and the interstate transmission grid. In this regard, the Commission acted to promote a more reliable electric system by promoting regional coordination and planning of the interstate grid through regional independent system operators (ISOs) and regional transmission organizations (RTOs), adopting transmission pricing policies that provide price signals for the most reliable and efficient operation and expansion of the grid, and providing pricing incentives at the wholesale level for investment in grid improvements and assuring recovery of costs in wholesale transmission rates.

As part of FERC's efforts to promote grid reliability, the Commission created a new Division of Reliability within the Office of Markets, Tariffs and Rates. On September 20, 2007, the Division became a full fledged Directorate within the Commission. The Office of Electric Reliability (OER) is continuing to focus on the development and implementation of mandatory and enforceable reliability standards for the users, owners, and operators of the nation's bulk power system. One task of this office has been to participate in NERC's Reliability readiness reviews of balancing authorities, transmission operators and reliability coordinators in North America to determine their readiness to maintain safe and reliable operations. FERC's OER has also engaged in studies and other activities to assess the longer-term and strategic needs and issues related to power grid reliability.

Sufficient supplies of energy and a reliable way to transport those supplies to customers are necessary to assure reliable energy availability and to enable competitive markets. The Commission assists in creating a more reliable electric system by:

- Fostering regional coordination and planning of the interstate grid through independent system operators and regional transmission organizations;
- Adopting transmission policies that provide price signals for the most reliable and efficient operation and expansion of the grid; and
- Providing pricing incentives at the wholesale level for investment in grid improvements and ensuring opportunities for cost recovery in wholesale transmission rates.

The passage of the Electricity Modernization Act of 2005 added to the Commission's efforts identified above, by giving it the authority to strengthen the reliability of the interstate grid through the grant of new authority pursuant to section 215 of the FPA which provides for a system of mandatory Reliability Standards developed by the ERO, established by FERC, and enforced by the ERO and Regional Entities.

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.

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.

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.

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.

3. DESCRIBE ANY CONSIDERATION OF THE USE OF IMPROVED TECHNOLOGY TO REDUCE BURDEN AND TECHNICAL OR LEGAL OBSTACLES TO REDUCING BURDEN.

In order that the Commission is able to perform its oversight function with regard to Reliability Standards that are proposed by the ERO and established by the Commission, it is essential that the Commission receive timely information regarding all or potential violations of Reliability Standards. While section 215 of the FPA contemplates the filing of the record of an ERO or Regional Entity enforcement action, FERC needs information regarding violations and potential violations at or near the time of occurrence. Therefore, it will work with the ERO and regional reliability organizations to be able to use the electronic filing of information so the Commission receives timely information.

The new regulations also require that each Reliability Standard that is approved by the Commission will be maintained on the ERO's Internet website for public inspection.

4. DESCRIBE EFFORTS TO IDENTIFY DUPLICATION AND SHOW SPECIFICALLY WHY ANY SIMILAR INFORMATION ALREADY

AVAILABLE CANNOT BE USED OR MODIFIED FOR USE FOR THE PURPOSE(S) DESCRIBED IN INSTRUCTION NO. 2

Filing requirements are periodically reviewed as OMB review dates arise or as the Commission may deem necessary in carrying out its responsibilities under the FPA in order to eliminate duplication and ensure that filing burden is minimized. There are no similar sources of information available that can be used or modified for these reporting purposes. The filing requirements in FERC-725B will incorporate NERC's requirements. However, all reliability requirements will be subject to FERC approval along with the requirements developed by Regional Entities, Regional Advisory Bodies and the ERO.

5. METHODS USED TO MINIMIZE BURDEN IN COLLECTION OF INFORMATION INVOLVING SMALL ENTITIES

FERC-725B is a filing requirement concerning the implementation of reliability standards by the Electric Reliability Organization and its responsibilities as well as those of Regional Entities and Regional Advisory Bodies in the development of Reliability Standards. The Electricity Modernization Act specifies that the ERO and Regional Entities are not departments, agencies or instrumentalities of the United States government and will not be like most other businesses, profit or not-for–profit. Congress created the concept of the ERO and Regional Entities as select, special purpose entities that will transition the oversight of the Bulk-Power System reliability from voluntary, industry organizations to independent organizations subject to Commission jurisdiction.

Section 215(b) of the FPA requires all users, owners and operators of the Bulk-Power System to comply with Commission-approved Reliability Standards. Each proposed Reliability Standard submitted for approval by NERC applies to some subset of users, owners and operators.

In the CIP NOPR, the Commission analyzed the affect of the proposed rule on small entities.[14] The Commission's analysis found that the DOE's Energy Information Administration (EIA) reports that there were 3,284 electric utility companies in the United States in 2005,[15] and 3,029 of these electric utilities qualify as small entities under the Small Business Administration (SBA) definition. Of these 3,284 electric utility companies, the EIA subdivides them as follows: (1) 883 cooperatives of which 852 are small entity cooperatives; (2) 1,862 municipal utilities, of which 1842 are small entity municipal utilities; (3) 127 political subdivisions, of which 114 are small entity political subdivisions; (4) 159 power marketers, of which 97 individually could be considered small entity power marketers;[16] (5) 219 privately owned utilities, of which 104 could be considered small entity private utilities; (6) 25 state

14 CIP NOPR at P 342.

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

16 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.

organizations, of which 16 are small entity state organizations; and (7) nine federal organizations of which four are small entity federal organizations.

In addition, the Commission's analysis relied on NERC's compliance registry, applying the NERC Statement of Registry Criteria, to identify entities that must comply with the CIP Reliability Standards. For an entity to be included in the compliance registry, the ERO will have made a determination that a specific small entity has a material impact on the Bulk-Power System. Consequently, the compliance of such small entities is justifiable as necessary for Bulk-Power System reliability. Based on NERC's compliance registry as of June 2007, the Commission estimated that approximately 1,000 registered entities will be responsible for compliance with the CIP Reliability Standards. Of these, the Commission estimated that the CIP Reliability Standards would apply to approximately 632 small entities, consisting of 12 small investor-owned utilities and 620 small municipal and cooperatives.

The Commission's analysis concluded that the CIP Reliability Standards would not have a significant economic impact on a substantial number of small entities. The majority of small entities would not be required to comply with mandatory Reliability Standards based on the application of the NERC Registry Criteria. Moreover, the Commission explained that a small entity that is registered but does not identify critical cyber assets pursuant to CIP-002-1 will not have compliance obligations pursuant to CIP-003-1 through CIP-009-1. While a small entity that identifies only a few critical cyber assets must comply with CIP-003-1 through CIP-009-1, the Commission stated that the economic impact of such compliance would not be significant. Likewise, the housing of a limited number of critical cyber assets in a single location will lessen the economic impact of compliance.

The Commission also noted that, while not required or proposed by the CIP NOPR, small entities could choose to collectively select a single consultant to develop model software and programs to comply with the CIP Reliability Standards on their behalf. Such an approach could significantly reduce the costs that would be incurred if each company would address these issues independently.

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

The Commission also investigated possible alternatives. These included the Commission's adoption in Order No. 693 of the NERC definition of bulk electric system, which reduces significantly the number of small entities responsible for compliance with mandatory Reliability Standards.[17] The Commission also noted that small entities could join a joint action agency or similar organization, which could accept responsibility for compliance with mandatory Reliability Standards on behalf of its members and also may divide the responsibility

17 CIP NOPR at P 347.

for compliance with its members. Based on that analysis, the Commission certified that the proposed rulemaking would not have a significant impact on a substantial number of small entities.

National Rural Electric Cooperative Association (NRECA) stated that, for the most part, the CIP NOPR treats small entities in an appropriate manner. NRECA maintained that the approach of having the CIP and other Reliability Standards apply to small entities only if they have a material impact on the reliability of the Bulk-Power System is appropriate and consistent with the Commission's prior orders, the statute, and the ERO's Statement of Registry Criteria, and NRECA supports it fully, with the exception of the Commission's discussion of jointly-owned facilities, which is discussed in the Final Rule with respect to CIP-004-1.

American Public Power Association/Large Public Power Council (APPA/LPPC) stated that application of the NERC Statement of Compliance Registry Criteria has reduced the total number of public power utilities potentially subject to NERC's Reliability Standards from nearly 2,000 to approximately 326 discrete public power utilities, and APPA/LPPC agrees with the Commission that NERC's compliance registry goes a long way toward mitigating the economic impact of the proposed rules on small entities. Nonetheless, APPA/LPPC disagrees with the Commission's categorical statement that "the CIP Reliability Standards will not have a significant economic impact on a substantial number of small entities."

According to APPA/LPPC, approximately 293 of the 326 public power systems included on the NERC compliance registry meet the SBA definition of a small electric utility.[18] Therefore, APPA/LPPC argues that the proposed regulations will have an impact on a substantial number of small entities. They maintain that the question is how significant that impact will in fact be. APPA/LPPC believes that some of these small entities will incur significant economic costs to comply with the CIP Reliability Standards.[19]

Despite these reservations, APPA/ LPPC believe that the broad contour of the rule contemplated by the CIP NOPR, subject to the changes they request in comments, satisfies the requirements of the RFA. APPA/LPPC state that they recognize that CIP Reliability Standards are necessary to ensure the reliable operation of the Bulk-Power System. While NERC's proposed standards will place the burden on many small entities to identify critical assets and critical cyber assets, this approach is far superior to a top-down approach to asset classification. Assuming small entities do have critical assets and critical cyber assets, they will have to take on significant burdens and incur significant costs to protect their critical cyber assets. However,

18 The APPA/LPPC estimate is based on a comparison of public power systems listed on the NERC compliance registry as of September 2007 with Energy Information Administration Form 861 data for 2005 MWh sales to ultimate customers and sales for resale. The Commission estimates that "the CIP Reliability Standards will apply to approximately 632 small entities, consisting of 12 small investor-owned utilities and 620 small municipals and cooperatives."

19 For example, APPA/LPPC stated that many small distribution utilities with fewer than 50 employees may nonetheless own and operate 20 MVA generators. Many of these generators were constructed prior to the industry's adoption of a modern information technology infrastructure. A rigid implementation of the "technical feasibility" exception discussed in item no. 8 below may lead to directives to adopt remediation plans that bring these units up to current industry standards. However, the costs required to retrofit such facilities to meet new cyber-security requirements may well force the owners to retire many of these units instead. APPA/LPPC at 30.

APPA/LPPC stated that NERC's proposed timeline for the implementation plan appears feasible. Moreover, they state that joint action agencies and other similar organizations may form joint registration organizations that accept compliance responsibilities for their members or provide compliance services to their members.

Arkansas Electric fully supports the comments submitted in response to the CIP NOPR by NRECA. Arkansas Electric argued that, throughout the CIP NOPR, the Commission proposed significant changes to the Reliability Standards which will increase the amount of effort and expense required to comply. Arkansas Electric is concerned that the costs of these additional resources will be especially high for small entities, when viewed in a relative sense. Arkansas Electric is concerned that, even with the friendly tone that some state regulators have taken toward rate recovery for cyber security-related expenses, these dollars would still come from its members. Arkansas Electric respectfully asks the Commission to keep cooperatives and small entities in mind as it proposed changes to the CIP Reliability Standards. The resources available within such organizations to comply with the Reliability Standards are often quite limited.

California Cogeneration and Energy Producers argued that the eight cyber security Reliability Standards will impose significant new compliance costs on registered entities to the extent they identify critical cyber assets, under CIP-002-1. They suggested that the Commission should direct the ERO to develop pro forma models of protocols and methodologies to be used by entities to facilitate compliance. California Cogeneration submitted that pro forma protocols could help mitigate the costs of compliance with the requirements of Reliability Standards CIP-003-1 through CIP-009-1. California Cogeneration pointed out that the CIP NOPR suggested that groups of entities could collaborate to reduce compliance costs; California Cogeneration argued that this approach could be expanded to include a formal role for NERC.

To maximize the effectiveness and the focus of the Reliability Standards, Energy Producers argued that NERC should revisit the NERC Functional Model to include a qualifying facility (QF) category so that Reliability Standards specific to QFs can be developed to account for their unique operating characteristics. To ensure that the regulations effectively promote reliability while not imposing unreasonable costs, Energy Producers argued that the regulations should provide a rigorous definition of critical cyber assets. Such rigor would be provided, first, by retaining the definitions contained in the current draft of the regulations, and second, by providing greater specificity to the risk-based assessment required in CIP-002-1.

Iowa Association of Municipal Utilities (Iowa Municipals) was concerned about the impact that the CIP Reliability Standards will have on smaller entities. While it is true that smaller entities can provide a cyber gateway to larger entities, and many smaller entities will be excluded through the identification of critical cyber assets, it is equally true that some smaller entities will, nonetheless, be subjected to the CIP Reliability Standards. The CIP NOPR pays insufficient attention to supporting compliance by smaller entities. Iowa Municipals made some suggestions to assist the Commission to enable smaller entities to comply with the Reliability Standards.

One area in which smaller entities' compliance efforts can be supported is through the self-certification process. Iowa Municipals supported the comments filed by Mid-American Energy Company (MidAmerican) that support a semi-annual certification process. As an enhancement to this process, Iowa Municipals recommended that the Commission require NERC to provide a "lessons learned" report to entities within 30 days of the certification deadline. This report has the potential of providing invaluable guidance and assistance to smaller entities.

Iowa Municipals also urged the Commission to support smaller entities' compliance efforts by providing either a longer compliance timetable, or providing temporary waivers upon an adequate showing of work to attain compliance. Further, Iowa Municipals suggested that compliance by smaller entities can be promoted by allowing smaller entities to walk in the footsteps of larger entities and reach compliance more quickly by taking advantage of lessons learned by others. Iowa Municipals also argued that following such a better path to compliance by smaller entities should ultimately provide a higher level of system protection.

The Southwest Transmission Dependent Utility Group (Southwest TDUs) stated that the CIP NOPR seems to be of two minds on how the impact of the CIP Reliability Standards might be addressed for smaller entities. On the one hand, the Commission proposed that NERC and the Regional Entities help the small entities by providing technical support to identify critical assets. On the other, the Commission acknowledged that these Reliability Standards could be made applicable down to the smallest entity, which appears to discount the economic impact on these entities required to be analyzed by the RFA because cyber security operations may actually be managed by a control area operator or other larger entity. Southwest TDUs argued that just because a larger entity is performing compliance does not mean the costs of compliance are not being passed on to the small entities. Indeed, there is likelihood that this will be the case. Southwest TDUs maintained that it does not know how onerous a burden that small entities will face. The Commission must be ready to adjust the CIP requirements, if experience shows that the burden on small entities proves to be onerous.

Commission Response

As of October 2007, there are 1,772 registered entities, of which the Commission estimates that approximately 1,400 will be responsible for compliance with the CIP Reliability Standards. Of these, the Commission estimates that the CIP Reliability Standards would apply to approximately 632 small entities, consisting of 12 small investor-owned utilities and 620 small municipal and cooperatives.

Arkansas Electric raised concerns with the cost to small entities of the modifications directed by the Commission. These modifications will be made by the ERO through the Reliability Standards development process. Until NERC files any revised Reliability Standards, the Commission cannot estimate their burden on any user, owner or operator of the Bulk-Power System, including small entities. The Commission therefore does not believe it is appropriate to speculate on the cost of compliance with any modified Reliability Standard at this time.

The Commission does not believe it is appropriate to grant California Cogeneration's request that NERC develop pro forma models of protocols and methodologies to be used by entities to facilitate compliance. That level of detail could potentially introduce common vulnerabilities resulting from all small entities implementing the Reliability Standards using a nearly identical solution. With respect to California Cogeneration's suggestion that NERC should have a formal role in collaborating to reduce compliance costs, the Commission will not direct that at this time. However, NERC should consider providing information to such groups. Further, the Commission believes that requiring the ERO to develop guidance on how to comply with the Reliability Standards should facilitate compliance by small entities.

The Commission also declines to direct the ERO to include a QF category in the Functional Model, as requested by the Energy Producers and Users Coalition (Energy Producers). The Commission believes that this request is outside the scope of the Final Rule, which only concerns the CIP Reliability Standards proposed by NERC.

The Commission does not believe it is necessary to allow small entities a longer compliance timetable or to provide temporary waivers upon an adequate showing of work to attain compliance. As the Commission stated in the CIP NOPR, the burden to small entities is not great, but the economic impact is justified as necessary to protect cyber security assets that support Bulk-Power System reliability. Further, the Commission believes that allowing small entities to collectively select a single consultant to develop model software and programs to comply with the CIP Reliability Standard will allow the small entities to take advantage of any information known by larger entities or their consultants.

While Southwest TDUs are correct that the Commission acknowledges that the Reliability Standards could be made applicable down to the smallest entity, the Commission disagrees that this discounts the economic impact on these entities. As the Commission stated in the CIP NOPR, to be included in the compliance registry, the ERO will have made a determination that a specific small entity has a material impact on the Bulk-Power System. A small entity placed on the compliance registry could then appeal the determination to the ERO and the Commission.

Further, Southwest TDUs argued that just because a larger entity is performing compliance does not mean the costs of compliance are not being passed on to the small entities. The Commission agrees; however, in allowing small entities to pool their resources and select a single consultant to develop model software and programs, each entity need not separately fund model software and programs development. Rather, that cost can be spread over several entities.

6. CONSEQUENCE TO FEDERAL PROGRAM IF COLLECTION WERE CONDUCTED LESS FREQUENTLY

The Electric Reliability Organization will conduct periodic assessments of the reliability and adequacy of the Bulk-Power System in North America and report its findings to the Commission, the Secretary of Energy, Regional Entities, and Regional Advisory Bodies

annually or more frequently if so ordered by the Commission. The ERO and Regional Entities will report to FERC on their enforcement actions and associated penalties and to the Secretary of Energy, relevant Regional entities and relevant Regional Advisory Bodies annually or quarterly in a manner to be prescribed by the Commission. If the information were conducted less frequently or discontinued, the Commission would be placed at a disadvantage in not having the data necessary for monitoring its mandated obligations.

7. EXPLAIN ANY SPECIAL CIRCUMSTANCES RELATING TO THE INFORMATION COLLECTION

FERC-725B is a filing requirement necessary to comply with the applicable provisions of the Electricity Modernization Act of 2005 and section 215 of the Federal Power Act.

In accordance with section 39.5 of the Commission's regulations, the ERO must file each Reliability Standard or a modification to a Reliability Standard with the Commission. The filing is to include a concise statement of the basis and purpose of the proposed Reliability Standard, either a summary of the Reliability development proceedings conducted by the ERO or a summary of the Reliability Standard development proceedings conducted by a Regional Entity together with a summary of the Reliability Standard review proceedings of the ERO and a demonstration that the proposed Reliability Standard is "just, reasonable, not unduly discriminatory or preferential, and in the public interest.

The ERO must make each effective Reliability Standard available on its Internet website. Copies of the effective Reliability Standards will be available from the Commission's Public Reference Room.

The Commission requires an original and seven copies of the proposed Reliability Standard or to the modification to a proposed Reliability Standard to be filed. This exceeds the OMB guidelines in 5 CFR 1320.5(d) (2) (iii) because of the number of divisions within the Commission that must analyze the standard and corresponding reports in order to carry out the regulatory process. The original is docketed, imaged through e-Library and filed as a permanent record for the Commission. The remaining copies are distributed to the necessary offices of the Commission with one being placed immediately in the Commission's Public Reference Room for public use. Since the time frame for responses to the request is very limited, the multiple hard copies are necessary for the various offices to review, analyze and prepare the final order at the same time. The electronic filing initiative at FERC, may in the near future, allow for relief of the number of copies, but at this time, the program turn around time for docketing, imaging and retrieval does not permit sufficient time to review the filings and to prepare the necessary documents for the processing of these filings.

8. DESCRIBE EFFORTS TO CONSULT OUTSIDE THE AGENCY: SUMMARIZE PUBLIC COMMENTS AND THE AGENCY'S RESPONSE TO THESE COMMENTS

Each Commission rulemaking (both NOPRs and Final Rules) are published in the Federal Register, thereby affording all public utilities and licensees, state commissions, Federal agencies, and other interested parties an opportunity to submit data, views, comments or suggestions concerning the proposed collection of data. The notice procedures also allow for public conferences to be held as required. The Commission has held several workshops and technical conferences to address reliability issues including transition to the NERC reliability standards, operator tools, and reactive power. Comments in response to this NOPR were due by October 5, 2007.

In response to the CIP NOPR, comments were filed by 70 interested persons. The discussions below address the issues raised by these comments. Appendix A to the Final Rule lists the entities that filed comments on the CIP NOPR.

Information Collection Statement

MidAmerican stated that the Commission's information collection assessment warrants revision for significantly underestimating the cost of compliance, even after controlling for variation in the number of critical cyber security assets identified by the responsible entity. MidAmerican alone estimates its total compliance costs as a substantial fraction of the burden amount estimated by the Commission, based upon compliance with the originally proposed CIP Reliability Standards. That cost should be expected to increase by ten percent based upon the more stringent Reliability Standards and rising labor rates. Based on this actual experience to date, MidAmerican submits that the CIP NOPR burden underestimates implementation difficulties by inadequately accounting for the both the replacement costs associated with upgrading existing antiquated cyber infrastructure as well as the host of employer recruiting, hiring and training challenges responsible entities will face to demonstrate compliance. The skilled computer software personnel necessary to achieve substantive compliance are in much demand (but short supply), nationally, and accordingly command compensation levels considerably higher than the CIP NOPR assumptions. To remedy these shortcomings, MidAmerican requested that the Commission revisit this issue by sampling the 1,000 or so entities expected to be required to comply with the CIP Reliability Standards and revising the burden estimate accordingly.

Commission Response

MidAmerican seems to misunderstand the purpose of the information collection statement. The OMB regulations require agencies to submit a burden estimate for collections of information contained in proposed rules, not for the entire cost of compliance. As stated in the CIP NOPR, the Commission only included the cost of developing the required documentation for the required policies, plans, programs and procedures in its burden estimate, but did not

include in its burden estimate the cost of substantive compliance with the CIP Reliability Standards. MidAmerican raises concerns regarding the total cost of compliance with the Reliability Standards, rather than the burden associated with reporting requirements in the Reliability Standards. Therefore, the Commission does not believe it is necessary to revise the burden estimate based on MidAmerican's comments.

Approval of NERC's Proposed CIP Reliability Standards

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

Most commenters strongly supported the Commission's proposal to approve the CIP Reliability Standards as mandatory and enforceable.[20] For example, Edison Electric Institute (EEI) stated that the CIP Reliability Standards are technically sound and well designed to achieve the specified reliability goal, namely cyber security for electric industry critical assets. EEI added that the CIP Reliability Standards are designed to serve the interest of preserving grid reliability by seeking to prevent unauthorized access to control systems and other critical cyber assets, whether by physical or electronic means. EEI believes that the CIP Reliability Standards strike the appropriate balance in providing reasonable flexibility in an environment where systems vary greatly in architecture, technology, and risk profile.[21]

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

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

Western Interconnection Regional Advisory Board (WIRAB) supports NERC's CIP Reliability Standards and stated that they represent a significant advancement for cyber security and Bulk-Power System reliability. Yet, WIRAB recommended that the Commission remand

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

the CIP Reliability Standards to NERC with guidance as to the types of changes the Commission would like to see, but without direction to make any specific change. WIRAB expressed concern that the CIP NOPR proposed numerous detailed directives to modify the CIP Reliability Standards and goes beyond providing guidance to NERC. WIRAB stated that a remand would allow the Reliability Standards development process to work as anticipated and, in doing so, would avoid problems with different Reliability Standards or different levels of enforcement on different sides of the international border.

In response to the Commission's proposal to modify certain CIP Reliability Standards, some commenters maintained that the Commission's proposals were overly prescriptive.[22] Others stated that any prescriptive elements of the CIP NOPR should be replaced with directions that NERC use its Commission-approved Reliability Standards development process to address any necessary changes identified by the Commission.[23] Pacific Gas & Electric (PG&E) added that the measures agreed on in the NERC stakeholder process and included in the CIP Reliability Standards represent a reasonable balance between aggressive Reliability Standards and measures that are feasible and sustainable. EEI argued that the Commission needs to be careful when it provides guidance that it does not usurp NERC's authority as ERO by dictating a specific or exclusive outcome from this process.

Commenters also expressed concern that the Commission might intend to sidestep the NERC stakeholder process and have NERC simply revise the CIP Reliability Standards in accordance with the Commission's proposals without providing NERC stakeholders an opportunity to participate in this process.[24] In this regard, EEI urged that the Final Rule make clear that any improvements to the CIP Reliability Standards should be considered in the NERC Reliability Standards development process before being mandated.

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

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

---

22 E.g., CEA, EEI, FirstEnergy, PSEG Companies, SDG&E and Tampa Electric.

23 E.g., Georgia Operators, Idaho Power, Muscatine Power, NERC, Northern California, NRECA, TAPS and Xcel.

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

Commission Determination

The Commission is approving the eight CIP Reliability Standards pursuant to section 215(d) of the FPA. In approving the CIP Reliability Standards, the Commission concludes that they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. These CIP Reliability Standards, together, provide baseline requirements for the protection of critical cyber assets that support the nation's Bulk-Power System. Therefore, the CIP Reliability Standards serve an important reliability goal.[25] Further, the CIP Reliability Standards clearly identify the entities to which they apply, apply throughout the interconnected Bulk-Power System, and provide a reasonable timetable for implementation.[26]

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

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

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

---

25 See Order No. 672 at P 321.

26 Id. P 322-35.

27 16 USC 824o(d)(5) ("[t]he Commission . . . may order the Electric Reliability Organization to submit to the Commission a proposed Reliability Standard or modification to a Reliability Standard that addresses a specific matter if the Commission considers such a new or modified Reliability Standard appropriate to carry out this section.").

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

While the Commission provides specific details in some instances regarding the Commission's expectations, it intends by doing so to provide useful guidance to assist in the Reliability Standards development process, not to impede it. The Commission finds that this is consistent with statutory language that authorizes the Commission to order the ERO to submit a modification "that addresses a specific matter" if the Commission considers it appropriate to carry out section 215 of the FPA. In the Final Rule, the Commission has considered commenters' concerns and, where a directive for modification appears to be determinative of the outcome, the Commission provides flexibility by directing the ERO to address the underlying issue through the Reliability Standards development process without mandating a specific change to the CIP Reliability Standard. Further, the Commission clarifies that, where the Final Rule identifies a concern and offers a specific approach to address that concern; the Commission will consider an equivalent alternative approach provided that the ERO demonstrates that the alternative will adequately address the Commission's underlying concern or goal as efficiently and effectively as the Commission's proposal.

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

Applicability

The Applicability section of each proposed CIP Reliability Standard identifies the following 11 categories of responsible entities that must comply with the CIP Reliability Standard: reliability coordinators, balancing authorities, interchange authorities,[29] transmission service providers, transmission owners, transmission operators, generator owners, generator operators, load serving entities, NERC, and Regional Reliability Organizations.

28 See Order No. 693 at P 185-87.

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

The CIP NOPR explained that, with regard to the applicability of the CIP Reliability Standards to the Electric Reliability Organization (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.[30] Further, the delegation agreements between NERC and each of the eight Regional Entities expressly state that the Regional Entity is committed to comply with approved Reliability Standards. The Commission stated its belief that, while it is likely that NERC and the Regional Entities are not directly subject to mandatory Reliability Standards as users, owners or operators of the Bulk-Power System, their adherence to the CIP Reliability Standards pursuant to the NERC Rules of Procedure and the delegation agreements suffices.

The Commission also indicated in the CIP NOPR that it would rely on the NERC registration process to determine applicability with the CIP Reliability Standards.[31] While expressing concern about small entities becoming a gateway for cyber attacks, the Commission indicated that it was prepared to rely on the registration process based in part on the expectation that industry will use the "mutual distrust" posture.[32] The Commission also explained that it would rely on the NERC registration process to include all critical assets and associated critical cyber assets, and listed examples. Further, the Commission noted that because, as an initial compliance step, each entity that is responsible for compliance with the CIP Reliability Standards must first identify critical assets through the application of a risk-based assessment, CIP-002-1 acts as a filter, determining a subset of entities that must comply with the remaining CIP requirements (i.e., CIP-003-1 through CIP-009-1).

The Commission also raised concerns regarding operation of critical cyber assets by out-sourced entities.[33] The CIP NOPR noted that, on occasion, NERC negotiates contracts with third party vendors, and the products developed by the vendors are then used by responsible entities that, as owners of the critical cyber assets, are ultimately responsible for their cyber security protection under the CIP Reliability Standards. The Commission solicited comment on whether and how out-sourced entities should be contractually obligated to comply with the CIP Reliability Standards while satisfying their other contractual obligations.

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

---

30 See CIP NOPR at P 21-31; NERC Rules of Procedure, section 100.

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

32 Id. P 28. The term "mutual distrust" is used to denote how "outside world" systems are treated by those inside the control system. A mutual distrust posture requires each responsible entity that has identified critical cyber assets to protect itself and not trust any communication crossing an electronic security perimeter, regardless of where that communication originates. This concept is discussed further in the context of CIP-003-1.

33 CIP NOPR at P 31.

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

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

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

NRECA, MEAG Power and other commenters supported the Commission's reliance on the NERC registration process to identify appropriate entities and also share the concern that entities not registered could become a weakness in the security of the Bulk-Power System.[34] NRECA stated that the Commission's proposed approach is appropriate and consistent with the Commission's prior orders, the statute, and the ERO's Statement of Registry Criteria. EEI suggested that proper registration, combined with a strong ERO audit program, would assure that all critical assets are covered by the CIP Reliability Standards. EEI also asked the Commission to clarify that the NERC registration process would identify responsible entities, but not critical assets.

EEI and ISO/RTO Council agreed with the statement in the CIP NOPR that demand side aggregators might also need to be included in the NERC registration process if their load shedding capacity would affect the reliability or operability of the Bulk-Power System. EEI commented that demand side aggregators do not fit into any of the current registry categories and their inclusion would likely require the development of a definition of "demand response"

34 E.g., Duke, EEI, Energy Producers, Northeast Utilities and Reliant.

and "direct load control," as well as size thresholds, which are best addressed in the NERC Reliability Standards development process.

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

The majority of commenters contend that neither the ERO, nor the Commission, have authority to extend the applicability of the CIP Reliability Standards to third-party vendors.[35] NRECA, for example, argues that this conclusion is dictated by statute, as section 215 of the FPA only applies to users, owners and operators of the Bulk-Power System and does not confer jurisdiction over third-party vendors. Accordingly, commenters claim that the relationship between registered entities and their outsourced providers is necessarily one of contract, and the regulatory compliance obligation falls solely on the registered entity.

EEI agreed with the CIP NOPR statement that responsible entities, as owners of critical assets, are ultimately accountable for their cyber security protection under the Reliability Standards. EEI also commented that it is reasonable that responsible entities may wish to provide their vendors with incentives to comply with CIP Reliability Standards while satisfying their other contractual obligations.[36] According to Reliability First Corporation (ReliabilityFirst), out-sourced products developed for the exchange of data integral to reliability must be developed in compliance with the CIP Reliability Standards. It believes the responsible entity should contractually obligate vendors of such products to comply with appropriate requirements of the CIP Reliability Standards.

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

Other commenters contend that the CIP Reliability Standards must apply to vendors and contractors as well as responsible entities. For example, California Commission suggested that the CIP Reliability Standards should apply to every entity that has a cyber connection to the

---

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

36 Alliant, Mr. Brown, PG&E, SDG&E and Tampa Electric agreed with EEI's position.

Bulk-Power-System. However, in California Commission's view, some special rules must be developed on CIP Reliability Standards applicability for entities that are not responsible entities but that have entered contracts obligating them to comply with the CIP Reliability Standards. Consumers Energy Corporation (Consumers) claimed that vendors and contactors with access (remote and on-site) to the critical cyber assets should be required to comply with the CIP Reliability Standards' personnel risk assessment guidelines. Consumers also advocated that vendor companies should have a personnel risk assessment policy, i.e., background check, for all new personnel and all systems (software applications and hardware devices) should be tested for quality and reliability.

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

Commission Response

The Commission is adopting the CIP NOPR approach regarding NERC and Regional Entity compliance with the CIP Reliability Standards. The Commission maintains its belief that NERC's compliance is necessary in light of its interconnectivity with other entities that own and operate critical assets. Further, the Commission concludes that NERC's Rules of Procedure, which state that the ERO will comply with each Reliability Standard that identifies the ERO as an applicable entity, provides an adequate means to assure that NERC is obligated to comply with the CIP Reliability Standards. Likewise, the delegation agreements between NERC and each Regional Entity expressly state that the Regional Entity is committed to comply with approved Reliability Standards.[37] Based on these provisions, the Commission finds that the Commission has authority to oversee the compliance of NERC and the Regional Entities with the CIP Reliability Standards.

With regard to EEI's concerns about NERC's incentives to comply with the CIP Reliability Standards, the Commission believes that NERC's position as overseer of Bulk-Power System reliability provides a level of assurance that it will take compliance seriously. Moreover, section 215(e)(5) of the FPA provides that the Commission may take such action as is necessary or appropriate against the ERO or a regional entity to ensure compliance with a Reliability Standard or Commission order.[38]

The Commission is also adopting its CIP NOPR approach and concludes that reliance on the NERC registration process at this time is an appropriate means of identifying the entities that

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

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

must comply with the CIP Reliability Standards.[39] The Commission is concerned, like the California Commission that some small entities that are not identified in the NERC registry may become gateways for cyber attacks. However, the Commission is not prepared to adopt California Commission's suggested approach of requiring that any entity connected to the Bulk-Power System, regardless of size, must comply with the CIP Reliability Standards irrespective of the NERC registry. The Commission believes this approach is overly-expansive and may raise jurisdictional issues. Rather, the Commission relies on NERC and the Regional Entities to be vigilant in assuring that all appropriate entities are registered to ensure the security of the Bulk-Power System.

With regard to EEI's request for clarification, the NERC registry process is designed to identify and register entities for compliance with Reliability Standards, and not identify lists of assets. In the CIP NOPR, the Commission explained that it would expect NERC to register the owner or operator of an important asset, such as a blackstart unit, even though the facility may be relatively small or connected at low voltage.[40] While the facility would not be registered or listed through the registration process, NERC's or a Regional Entity's awareness of the critical asset may reasonably result in the registration of the owner or operator of the facility.

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

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

> . . . when an application is developed and maintained by an outsourced provider, that outsourced provider manages physical and cyber access to the environment on which the application runs and therefore must be contractually obligated to the Responsible Entity to comply with the Reliability Standards.
>
> While such providers are not registered entities subject to the Reliability

39 CIP NOPR at P 26-30.
40 Id. P 29.

> Standards, they must perform the services and operate the applications in a manner consistent with the Reliability Standards. . . the Responsible Entity should be charged with incorporating contractual terms and conditions into agreements with third-party service providers that obligate the providers to comply with the requirements of the Reliability Standards. In that regard, if a Responsible Entity determines that it is necessary to outsource a service that is essential to the reliable operation of a Critical Asset, Critical Cyber Asset, or the bulk electric system, it is clear that the Responsible Entity must be held responsible and accountable for compliance with the Reliability Standards.[41]

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

Self-Certification

In the CIP NOPR, the Commission expressed concern over whether responsible entities will be fully prepared for compliance upon reaching the implementation deadline and will take reasonable action to protect the Bulk-Power System during the interim period.[42] The Commission stated that NERC's plans to require self-certification during the interim period are helpful and proposed that, to allow adequate monitoring of progress, the ERO develop a self-certification process with certifications more frequent than once per year. The CIP NOPR suggested that self-certification be tied either to target dates in the schedule or perhaps quarterly or semi-annual certifications. The Commission indicated that, while an entity should not be subject to a monetary penalty if it is unable to certify that it is on schedule, such an entity should explain to the ERO the reason it is unable to self-certify. The ERO and the Regional Entities should then work with such an entity either informally or, if appropriate, by requiring a remedial plan, to assist such an entity in achieving full compliance in a timely manner. The Commission also stated that the ERO and the Regional Entities should provide informational guidance, upon request, to assist a responsible entity in assessing its progress in reaching "auditably compliant" status.

Many commenters oppose directing NERC to consider a self-certification process with more frequent self-certifications than on an annual basis.[43] In this regard, EEI argued that a more frequent self-certification requirement is likely to impose undue burdens without commensurate benefits. KCPL claims that there are sufficient processes already in place in order to evaluate and monitor CIP Reliability Standards compliance and additional requirements for self-certification provide no significant support or benefit to tracking a Responsible Entity's obligations to the CIP Reliability Standards and are unneeded.

---

41 ISO/RTO Council comments at 21-22.

42 CIP NOPR at P 48.

43 E.g., Alliant, Bonneville, Entergy, EEI, ISO-NE, KCPL, National Grid, Northeast Utilities, PG&E, Portland General, Progress, Puget Sound and Southern.

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

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

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

Commission Response

While the Commission is sensitive to concerns that more frequent self-certifications may be burdensome, it is important that the ERO and the Commission know whether industry, or segments of industry, are having difficulty implementing the CIP Reliability Standards. Therefore, the Commission is directing the ERO to require more frequent, semi-annual, self-certifications prior to the date by which full compliance is required. Such additional self-certifications may be a "stream-lined" version, but must be useful for the ERO and the Commission to assess industry's progress toward achieving compliance with the CIP Reliability Standards.

Further, the Commission adopts its CIP NOPR proposals that, while an entity should not be subject to a monetary penalty if it is unable to certify that it is on schedule, such an entity should explain to the ERO the reason it is unable to self-certify. The ERO and the Regional Entities should then work with such an entity either informally or, if appropriate, by requiring a remedial plan to assist such an entity in achieving full compliance in a timely manner. Further, the Commission expects the ERO and the Regional Entities to provide informational guidance,

upon request, to assist a responsible entity in assessing its progress in reaching "auditably compliant" status.

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

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

Reasonable Business Judgment

In the CIP NOPR the Commission stated,[44] 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.

In addition, each of the subsequent CIP Reliability Standards (i.e., CIP Reliability Standards CIP-003-1 through CIP-009-1) includes a statement that "Responsible Entities should interpret and apply the Reliability Standard using reasonable business judgment."

The Commission pointed out in the CIP NOPR that NERC's Glossary of Terms Used in Reliability Standards (NERC Glossary) does not define reasonable business judgment, and the CIP Reliability Standards do not otherwise suggest how the term is to be interpreted. NERC's Frequently Asked Questions (FAQ) document that accompanies the CIP Reliability Standards provides the only available guidance on the issue.[45] 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."

44 CIP NOPR at P 50.

45 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.

The FAQ document notes that there is a long history of judicial interpretation of the business judgment rule and states that "[c]ourts generally hold that the phrase indicates reviewing tribunals should not substitute their own judgment for that of the entity under review other than in extreme circumstances."

The Commission proposed, in the CIP NOPR, to direct the ERO to modify the CIP Reliability Standards to remove references to the "reasonable business judgment" language before compliance audits start in 2009.[46] In the CIP NOPR, the Commission discussed the history of the reasonable business judgment concept and the meaning attached to that concept by the courts in the corporate context.[47] The Commission pointed out that, if this term is applied to the CIP Reliability Standards, it could easily be understood to have the same meaning as in the corporate context.

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

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

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

The Commission stated that this test is fundamentally incompatible with Congress' decision to adopt a regime of mandatory Reliability Standards. The Commission explained that the issue under section 215 of the FPA is not whether the management of a business is acting in

46 CIP NORP at P 58.
47 Id. P 59, 61.

the interest of its own shareholders, but rather whether an entity is taking appropriate action to avert risks that could threaten the entire grid. Finally, the Commission noted that in the corporate governance context, the business judgment rule is invoked only in extreme circumstances, generally when an officer or director is found to have acted fraudulently, in bad faith, or with gross or culpable negligence. For all these reasons, the Commission proposed in the CIP NOPR that the ERO remove references to the "reasonable business judgment" language from the CIP Reliability Standards.

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

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

Numerous commenters argued that use of the term reasonable business judgment was never intended to import corporate law concepts into the CIP Reliability Standards but rather to ensure that Responsible Entities have sufficient flexibility when implementing them.[48] EEI stated that the term was intended to allow flexible but objective decision-making in determining an approach to compliance. It was not intended to provide flexibility on whether to comply, only on how to comply.

Mr. Laurence Brown (Mr. Brown) stated that neither the CIP Reliability Standards nor the FAQ document state that the use of reasonable business judgment would have the effects that the Commission suggested and that the Commission's description of the language and its

48 E.g., Alliant, Arizona Public Service, EEI, PSE&G, SoCal Edison and Xcel.

potential effect is an effort to set up a "straw man" rather than address the clear intent of the language. He maintained that the Commission's analysis of the language is "speculative and hyper-legalistic".

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

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

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

A number of commenters defended the use of reasonable business judgment in terms that focus more on the issue of liability than simple flexibility or economic considerations. AMP-Ohio stated that the plain language of the proposed CIP Reliability Standards could create a strict liability environment if there is no exception for "good faith" or "reasonable judgment." Mr. Brown stated that the proposal to remove the reasonable business judgment language appears to hold utilities, and perhaps individual managers, officers and directors, directly

responsible for any adverse impact of decisions based upon their inherently imperfect knowledge and information regardless of whether they acted in good faith and made reasonably well-informed decisions. Entergy stated that the industry must have reasonable assurance that the actions they are implementing meet the CIP Reliability Standards and Requirements if they acted in good faith, performed the proper evaluation, and took actions consistent with their evaluation.

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

EEI and other commenters argued that if the reasonable business judgment language is removed from the CIP Reliability Standards, it should be replaced with alternative language developed in the Reliability Standards development process.[49] They argued that such language is necessary to ensure necessary flexibility. National Grid stated that the Commission should allow the ERO to develop suitable replacement language to allow for the reasonable flexibility that the Commission acknowledges that the industry requires in addressing critical infrastructure protection issues.

APPA/LPPC suggested that phrases such as "reasonable judgment" or "judgment consistent with Good Utility Practice" as substitutes for reasonable business judgment. A number of commenters, including Northern Indiana and Georgia System Operations Corporation (Georgia Operators), pointed to the phrase "good utility practice" in the pro forma OATT as a model or starting point for alternative language.

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

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

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

Commission Response

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

While there may have been no intention to import corporate law concepts into the CIP Reliability Standards, it is difficult to draw any other conclusion on the basis of the documents provided. The Commission notes that the only guidance on reasonable business judgment that emerged from the Reliability Standards development process and that was supplied to the Commission is found in the FAQ document, and that document appears to invoke the traditional corporate law business judgment rule. The FAQ document specifically references existing court precedent on the rule, and it sets forth the elements of reasonable business judgment in what is essentially a restatement of classic formulations of the business judgment rule.[50] Moreover, the FAQ document specifically references one of the most objectionable aspects of the business judgment rule in the cyber security context, the requirement that the courts defer to the decisions of company officers and directors in all but the most extreme circumstances.

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

The most common argument raised in favor of reasonable business judgment is that it ensures flexibility. The Commission, however, acknowledged the importance of flexibility and discretion in the CIP NOPR.[51] The CIP Reliability Standards consist for the most part of quite general requirements that must be implemented in a wide variety of circumstances. As drafted, they do not provide one-size-fits-all solutions and, rather, require responsible entities to assess their individual situations and devise solutions appropriate to their circumstances. The Commission therefore disagrees with Ontario Power that outright removal of all references to reasonable business judgment would render the CIP Reliability Standards too rigid. It will still be necessary for responsible entities to choose between available alternatives to arrive at cyber

50 See, e.g., Cramer v. General Telephone and Electronics Corp., 582 F.2d 259 (3d Cir. 1978); Joy v. North, 692 F.2d 880 (2d Cir. 1982); In Re Bal Harbour Club, Inc., 316 F.3d 1192 (11th Cir. 2003); Froelich v. Senior Campus Living LLC, 355 F.3d 802 (4th Cir. 2004); Poth v. Rassey, 281 F. Supp. 2d (E.D. Va. 2003).
51 See CIP NOPR at P 17, 59.

security solutions that best fit their situation. In short, the CIP Reliability Standards do not simply allow flexibility, they require it.

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

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

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

Although the Commission disagrees with National Grid and others that alternative language is necessary to ensure necessary flexibility, the Commission agrees that the ERO and the participants in the Reliability Standards development process may choose to develop

alternative language to replace reasonable business judgment and propose it for Commission approval. Such language would need to be adapted to the issues involved in forming judgments on proper cyber security measures and embody an objective standard focused on conduct that promotes the interests of Bulk-Power System security and reliability. Such language would also need to take into consideration our finding discussed below that a responsible entity cannot excuse itself from compliance with a requirement of the CIP Reliability Standards.

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

Finally, the Commission rejects arguments that it is being overly prescriptive in directing the ERO to remove all references to reasonable business judgment from the CIP Reliability Standards. It is, important to note that such objections are inapposite in this instance for an additional reason that involves the specific nature of the issue raised. The concept of reasonable business judgment speaks to a general legal standard of conduct proposed to apply under a statute that Congress has directed the Commission to administer. It does not involve matters specific to reliability but rather is bound up with the problem of legal enforceability. The Commission has a particular duty to see that the laws it administers can be enforced effectively. The Commission is not being overly prescriptive when acting to ensure that this will be the case. Based on this discussion, as well as the Commission's lengthy analysis in the CIP NOPR, the ERO is directed in the Final Rule to modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin.

Technical Feasibility

As the Commission explained in the CIP NOPR, two proposed CIP Reliability Standards provide exceptions from compliance with Requirements based on "technical feasibility."[52] The NERC Glossary does not define the term "technically feasible," nor do the CIP Reliability Standards themselves specify how an entity is to determine whether an action is technically feasible. NERC's FAQ document provides the following guidance on the meaning of the phrase "where technically feasible:"

> Technical feasibility refers only to engineering possibility and is expected to be a "can/cannot" determination in every circumstance. It is also intended to be determined in light of the equipment and facilities already owned by the responsible entity. The responsible entity is not required to replace any equipment in order to achieve compliance with the Cyber Security Standards. When existing equipment is replaced, however, the responsible entity is expected to use

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

> 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.[53]

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

Thus, the Commission proposed in the CIP NOPR to direct that the ERO establish a structure to require accountability from those who rely on "technical feasibility" as the basis for an exception. The CIP NOPR described such a structure as requiring a responsible entity to: (1) develop and implement interim mitigation steps to address the vulnerabilities associated with each exception; (2) develop and implement a remediation plan to eliminate the exception, including interim milestones and a reasonable completion date; and (3) obtain written 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.[54]

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

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

The Commission sought comment on additional categories of information that should be included in the content of this report that would be useful for the Commission, as well as the

53 FAQ document at 1.
54 CIP NOPR at P 79.

ERO and Regional Entities, in evaluating the invocation of technical feasibility and similar provisions, and the impact on protection of critical assets.

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

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

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

NERC stated that the Commission properly recognized the appropriateness of an exception based on technical feasibility and suggests that it be designated an "exemption for reliability."[55] NERC supports clarification of the Reliability Standards to ensure that an exemption is documented and justified in terms of its impact on Bulk-Power System reliability. ReliabilityFirst made similar proposals.

NERC and others believe that the appropriate way to address the Commission's specific proposed directives is through the Commission-approved Reliability Standards development process.[56] Northern California Power Agency (Northern California) supported the Commission's recommendation that the ERO re-examine and clarify the meaning of technical feasibility and provide guidance on the appropriate procedures for claiming an exemption based on it. Ontario Power Generation Inc. (Ontario IESO) commented that, if the term reasonable business judgment is removed from the CIP Reliability Standards, industry and the ERO may find other areas where the concept of technical feasibility is applicable when revising the CIP Reliability Standards. NRECA stated that technical feasibility is a matter on which the Commission should defer to the ERO's technical expertise and not adhere to a one-size-fits-all approach.

NERC explained that the CIP Reliability Standards include references to technical feasibility to recognize that, in many cases, equipment in place in substation and generating plant environments was implemented with operational functions paramount to all other considerations, including security. This equipment is not at the end of its useful life and historically has not been designed with ready access to software updates and patches. Such software upgrades that could increase functionality without directly contributing to reliability

55 NERC comments at 20-22.
56 E.g., Alliant, Manitoba Hydro, Northern California and NRECA.

generally have not been made. NERC stated that modern replacement equipment is more readily compatible with an environment where updates and patches are more commonplace and security functionality is an understood necessity. Securable equipment will be used when equipment is replaced due to natural end-of-life or failure, but this modern equipment represents a very small percentage of the installed base of all cyber equipment in substations and generating plants.

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

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

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

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

Manitoba Hydro stated that industry attempted to strike a balance for security at the various types of facilities while recognizing the large base of legacy systems at remote locations.

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

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

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

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

Commission Response

The Commission is adopting the CIP NOPR proposal and directing the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards. The Commission will modify some of its proposed criteria for that framework of accountability further below. The Commission is persuaded by commenters that the proposed conditions for

invoking the technical feasibility exception should allow for operational considerations. In response to Northern Indiana and other commenters, the Commission notes that the Commission did not propose to eliminate references to technical feasibility from the CIP Reliability Standards, only that the term be interpreted narrowly and without reference to considerations of business judgment.

In response to those commenters who argued that the Commission's concerns and directives should be addressed through the Reliability Standards development process, the Commission agrees that to the degree revisions to the Reliability Standards are necessary to address its concerns; they would be made through that process. The Commission disagrees, however, with the arguments that claim it is rewriting the CIP Reliability Standards or adhering to a one-size-fits-all approach. With respect to the latter point, the Commission notes that technical feasibility issues are by their nature something that must be dealt with on a case-by-case basis, as they only arise in specific circumstances. The Commission's concern here is primarily with the framework within which decisions on technical feasibility are made and ensuring that this framework promotes sound decisions that lead to effective results.

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

The Commission, however, disagrees with Northern Indiana that technical feasibility should be interpreted to apply to future assets also. The justification presented for technical feasibility exceptions is rooted in the problem of long-life legacy equipment and the economic considerations involved in the replacement of such equipment before the end of its useful life. The Commission recognizes that these considerations can be valid in some cases, but Northern Indiana has not explained why technical feasibility exceptions should apply to replacement equipment. The Commission neither assumes that technical infeasibility issues will be present only during the transition period, nor does it assume that on a going forward basis there will be only one single means to comply with the CIP Reliability Standards. It does assume, however, that all responsible entities eventually will be able to achieve full compliance with the CIP Reliability Standards when the legacy equipment that creates the need for the exception is supplemented, upgraded or replaced.

The Commission agrees with various commenters that the implementation of the CIP Reliability Standards should not be permitted to have an adverse effect on reliability and that proper implementation requires that care be taken to avoid unintended consequences. The Commission believes it is important to clarify that the meaning of "technical feasibility" should

not be limited simply to whether something is technically possible but also whether it is technically safe and operationally reasonable.

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

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

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

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

9. EXPLAIN ANY PAYMENT OR GIFTS TO RESPONDENTS

No payments or gifts have been made to respondents.

10. DESCRIBE ANY ASSURANCE OF CONFIDENTIALITY PROVIDED TO RESPONDENTS

The Commission generally does not consider the data filed to be confidential. However, certain standards may have confidentiality provisions in the standard.

The Commission has in place procedures to prevent the disclosure of sensitive information, such as the use of protective orders and rules establishing critical energy infrastructure information (CEII). However, the Commission believes that the specific, limited area of Cyber security Incidents requires additional protections because it is possible that system security and reliability would be further jeopardized by the public dissemination of information involving incidents that compromised the cyber security system of a specific user, owner or operator of the Bulk-Power System. In addition, additional information provided with a filing may be submitted with a specific request for confidential treatment to the extent permitted by law and considered pursuant to 18 C.F.R. 388.112 of FERC's regulations.

11. PROVIDE ADDITIONAL JUSTIFICATION FOR ANY QUESTIONS OF A SENSITIVE NATURE THAT ARE CONSIDERED PRIVATE.

There are no questions of a sensitive nature that are considered private.

12. ESTIMATED BURDEN OF COLLECTION OF INFORMATION

The Commission's estimate is based on all 1,000 entities documenting an assessment methodology to identify critical assets and critical cyber assets pursuant to CIP-002-1. As explained above, only those entities that identify critical cyber assets pursuant to CIP-002-1 are responsible to comply with the requirements of CIP-003-1 through CIP-009-1. Accordingly, the cost burden estimate differs for those entities that identify critical cyber assets and those that do not.

Further, the reporting burden would vary with the number of critical cyber assets identified pursuant to CIP-002-1. An entity that identifies numerous critical cyber assets, including assets located at remote locations, will likely require more resources to develop its policies, plans, programs and procedures compared to an entity that identifies one or two critical cyber assets, housed at a single location. Based on this distinction, the Commission has developed separate estimates for large investor-owned utilities and other responsible entities such as municipals, generators and cooperatives.

Prior to the development of CIP-002-1 through CIP-009-1, NERC approved through its urgent action process a cyber security Reliability Standard known as "UA-1200," which applied to entities "such as control areas, transmission owners and operators, and generation owners and operators." UA-1200 addressed a number of the same reporting burdens as the CIP Reliability Standards at issue in this proceeding. For example, UA-1200 required the creation and maintenance of a cyber security policy, the identification of "critical cyber assets," and the development of a cyber security training program. Thus, entities that voluntarily complied with UA-1200 will continue these practices when the mandatory CIP Reliability Standards are in

effect.

In addition, 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.

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 municipals & cooperatives	795	1	1,000	795,000
Entities that have not identified critical cyber assets	50	1	160	8,000
Totals				1,125,400

13. ESTIMATE OF THE TOTAL ANNUAL COST BURDEN TO RESPONDENTS

Information Collection Costs: The Commission sought 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.[57]

While Mid American challenged the Commission estimates for both burden and cost (see

57 See http://www.bls.gov/oes/current/naics2_22.htm.

item #8 "Information Collection Statement"), they did not provide specific data. In addition, no other commenter provided specific comments concerning the Commission's estimates in the NOPR. Therefore the Commission adopts its proposal in the CIP NOPR and will use the same estimates here in the Final Rule.

NERC submitted an implementation schedule submitted with the CIP Reliability Standards and calls for responsible entities to be "auditably compliant" with most requirements by mid-2010 or later. Therefore, the Commission developed an annual burden estimate by dividing total costs by 4 years.

14. ESTIMATED ANNUALIZED COST TO FEDERAL GOVERNMENT

The estimate of the cost to the Federal Government is based on salaries for professional and clerical support, as well as direct and indirect overhead costs. Direct costs include all costs directly attributable to providing this information, such as administrative costs and the cost for information technology. Indirect or overhead costs are costs incurred by an organization in support of its mission. These costs apply to activities which benefit the whole organization rather than anyone particular function or activity. It is difficult to provide an assessment at this stage of what the costs will be to the Commission in its review and of Reliability Standards submitted to it. These requirements are at the preliminary stages and the Regional Entities and Regional Advisory bodies are being created. Both organizations will play a role in standards development prior to their submission to the Commission.

Initial Estimates anticipate that 3.5 FTE's will review the Reliability standards at the Commission or a total cost of 3.5 x $126,384 = $442,344.[58]

15. REASONS FOR CHANGES IN BURDEN INCLUDING THE NEED FOR ANY INCREASE

This is a new information collection requirement that implements the provisions of the Electricity Modernization Act of 2005. The Act created section 215 of the Federal Power Act which provides for a system of mandatory reliability rules developed by the ERO, established by the Commission, and enforced by the Commission, subject to Commission review. As noted above, the information collections proposed in this Final Rule are needed to protect the electric industry's Bulk-Power System against malicious cyber attacks that could threaten the reliability of the Bulk-Power System

16. TIME SCHEDULE FOR THE PUBLICATION OF DATA

The filed proposed Reliability Standards are available on the Commission's eLibrary document retrieval system in Docket No. RM06-22-000 and the Commission will require that

58 An FTE = Full Time Employee. The $126,384 "cost" consists of approximately $102,028 in salaries and benefits and $24,355 in overhead. The Cost estimate is based on the estimated annual allocated cost per Commission employee for Fiscal Year 2008.

all Commission-approved Reliability Standards be available on the ERO's website, with an effective date (http://www.nerc.com/~filez/nerc_filings_ferc.html).

Copies of the filings are made available to the public within two days of submission to FERC via the Commission's web site. There are no other publications or tabulations of the information.

The CIP Reliability Standards were approved as voluntary reliability standards by the NERC board in May 2006, with a designated effective date of June 1, 2006.[59] The proposed implementation schedule as noted above, submitted with the CIP Reliability Standards plans for responsible entities to be "auditably compliant" with most requirements by mid-2010 or later. Mid-2010 is four years after NERC's voluntary reliability standards went into effect.

17. DISPLAY OF THE EXPIRATION DATE

59 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.

It is not appropriate to display the expiration date for OMB approval of the information collected. The information will not be collected on a standard, preprinted form which would avail itself to that display. Rather the Electric Reliability Organization must prepare and submit filings that reflect unique or specific circumstances related to the Reliability Standard. In addition, the information contains a mixture of narrative descriptions and empirical support that varies depending on the nature of the transaction.

18. **EXCEPTIONS TO THE CERTIFICATION STATEMENT**

Item No. 19(g) (vi) see Instruction No. 17 above for further elaboration. In addition, the data collected for this reporting requirement is not used for statistical purposes. Therefore, the Commission does not use as stated in item no. 19(i) "effective and efficient statistical survey methodology." The information collected is case specific to each Reliability Standard.

B. COLLECTION OF INFORMATION EMPLOYING STATISTICAL METHODS.

This is not a collection of information employing statistical methods.

Attachment A. Glossary of Terms Used in Reliability Standards

 Term Acronym Definition

Available Transfer Capability	ATC	A measure of the transfer capability remaining in the physical transmission network for further commercial activity over and above already committed uses. It is defined as Total Transfer Capability less existing transmission commitments (including retail customer service), less a Capacity Benefit Margin, less a Transmission Reliability Margin.
Balancing Authority	BA	The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.
Balancing Authority Area		The collection of generation, transmission, and loads within the metered boundaries of the Balancing Authority. The Balancing Authority maintains load-resource balance within this area.
Base Load		The minimum amount of electric power delivered or required over a given period at a constant rate.
Blackstart Capability Plan		A documented procedure for a generating unit or station to go from a shutdown condition to an operating condition delivering electric power without assistance from the electric system. This procedure is only a portion of an overall system restoration plan.
Bulk Electric System		As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition.
Burden		Operation of the Bulk Electric System that violates or is expected to violate a System Operating Limit or Interconnection Reliability Operating Limit in the Interconnection, or that violates any other NERC, Regional Reliability Organization, or local operating reliability standards or criteria.
Capacity Benefit Margin	CBM	The amount of firm transmission transfer capability preserved by the transmission provider for Load-Serving Entities (LSEs), whose loads are located on that Transmission Service Provider’s system, to enable access by the LSEs to generation from interconnected systems to meet generation reliability requirements. Preservation of CBM for an LSE allows that entity to reduce its installed generating capacity below that which may otherwise have been necessary without interconnections to meet its generation reliability requirements. The transmission transfer capability preserved as CBM is

		intended to be used by the LSE only in times of emergency generation deficiencies.
Capacity Emergency		A capacity emergency exists when a Balancing Authority Area's operating capacity, plus firm purchases from other systems, to the extent available or limited by transfer capability, is inadequate to meet its demand plus its regulating requirements.
Cascading		The uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.
Cascading Outages		The uncontrolled successive loss of Bulk Electric System Facilities triggered by an incident (or condition) at any location resulting in the interruption of electric service that cannot be restrained from spreading beyond a pre-determined area.
Clock Hour		The 60-minute period ending at :00. All surveys, measurements, and reports are based on Clock Hour periods unless specifically noted.
Cogeneration		Production of electricity from steam, heat, or other forms of energy produced as a by-product of another process.
Compliance Monitor		The entity that monitors, reviews, and ensures compliance of responsible entities with reliability standards.
Confirmed Interchange		The state where the Interchange Authority has verified the Arranged Interchange.
Congestion Management Report		A report that the Interchange Distribution Calculator issues when a Reliability Coordinator initiates the Transmission Loading Relief procedure. This report identifies the transactions and native and network load curtailments that must be initiated to achieve the loading relief requested by the initiating Reliability Coordinator.
Constrained Facility		A transmission facility (line, transformer, breaker, etc.) that is approaching, is at, or is beyond its System Operating Limit or Interconnection Reliability Operating Limit.
Contingency		The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch or other electrical element.
Contingency Reserve		The provision of capacity deployed by the Balancing Authority to meet the Disturbance Control Standard (DCS) and other NERC and Regional Reliability Organization contingency requirements.
Contract Path		An agreed upon electrical path for the continuous flow of electrical power between the parties of an Interchange Transaction.
Control	CPS	The reliability standard that sets the limits of a

Performance Standard		Balancing Authority's Area Control Error over a specified time period.
Corrective Action Plan		A list of actions and an associated timetable for implementation to remedy a specific problem.
Cranking Path		A portion of the electric system that can be isolated and then energized to deliver electric power from a generation source to enable the startup of one or more other generating units.
Critical Assets		Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.
Critical Cyber Assets		Cyber Assets essential to the reliable operation of Critical Assets.
Curtailment		A reduction in the scheduled capacity or energy delivery of an Interchange Transaction.
Curtailment Threshold		The minimum Transfer Distribution Factor which, if exceeded, will subject an Interchange Transaction to curtailment to relieve a transmission facility constraint.
Cyber Assets		Programmable electronic devices and communication networks including hardware, software, and data.
Cyber Security Incident		Any malicious act or suspicious event that: 1 • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, 2 • Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.
Delayed Fault Clearing		Fault clearing consistent with correct operation of a breaker failure protection system and its associated breakers, or of a backup protection system with an intentional time delay.
Demand		1. The rate at which electric energy is delivered to or by a system or part of a system, generally expressed in kilowatts or megawatts, at a given instant or averaged over any designated interval of time. 2. The rate at which energy is being used by the customer.
Demand-Side Management	DSM	The term for all activities or programs undertaken by Load-Serving Entity or its customers to influence the amount or timing of electricity they use.
Direct Control Load	DCLM	Demand-Side Management that is under the direct control of the system operator. DCLM may control the electric supply to individual appliances or

Management		equipment on customer premises. DCLM as defined here does not include Interruptible Demand.
Dispersed Load by Substations		Substation load information configured to represent a system for power flow or system dynamics modeling purposes, or both.
Distribution Factor	DF	The portion of an Interchange Transaction, typically expressed in per unit that flows across a transmission facility (Flowgate).
Distribution Provider		Provides and operates the “wires” between the transmission system and the end-use customer. For those end-use customers who are served at transmission voltages, the Transmission Owner also serves as the Distribution Provider. Thus, the Distribution Provider is not defined by a specific voltage, but rather as performing the Distribution function at any voltage.
Disturbance		1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system. 3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.
Disturbance Control Standard	DCS	The reliability standard that sets the time limit following a Disturbance within which a Balancing Authority must return its Area Control Error to within a specified range.
Disturbance Monitoring Equipment	DME	Devices capable of monitoring and recording system data pertaining to a Disturbance. Such devices include the following categories of recorders[1]: 1 • Sequence of event recorders which record equipment response to the event • Fault recorders, which record actual waveform data replicating the system primary voltages and currents. This may include protective relays. 1 • Dynamic Disturbance Recorders (DDRs), which record incidents that portray power system behavior during dynamic events such as low-frequency (0.1 Hz – 3 Hz) oscillations and abnormal frequency or voltage excursions

[1] Phasor Measurement Units and any other equipment that meets the functional requirements of DMEs may qualify as DMEs.

Dynamic Interchange Schedule or Dynamic Schedule	A telemetered reading or value that is updated in real time and used as a schedule in the AGC/ACE equation and the integrated value of which is treated as a schedule for interchange accounting purposes. Commonly used for scheduling jointly owned generation to or from another Balancing Authority Area.

Dynamic Transfer	The provision of the real-time monitoring, telemetering, computer software, hardware, communications, engineering, energy accounting (including inadvertent interchange), and administration required to electronically move all or a portion of the real energy services associated with a generator or load out of one Balancing Authority Area into another.
Economic Dispatch	The allocation of demand to individual generating units on line to effect the most economical production of electricity.
Electrical Energy	The generation or use of electric power by a device over a period of time, expressed in kilowatthours (kWh), megawatthours (MWh), or gigawatthours (GWh).
Electronic Security Perimeter	The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.
Element	Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be comprised of one or more components.
Emergency or BES Emergency	Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System.
Emergency Rating	The rating as defined by the equipment owner that specifies the level of electrical loading or output, usually expressed in megawatts (MW) or Mvar or other appropriate units, that a system, facility, or element can support, produce, or withstand for a finite period. The rating assumes acceptable loss of equipment life or other physical or safety limitations for the equipment involved.
Energy Emergency	A condition when a Load-Serving Entity has exhausted all other options and can no longer provide its customers' expected energy requirements.
Equipment Rating	The maximum and minimum voltage, current, frequency, real and reactive power flows on individual equipment under steady state, short-circuit and transient conditions, as permitted or assigned by the equipment owner.
Facility	A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)
Facility Rating	The maximum or minimum voltage, current, frequency, or real or reactive power flow through a facility that does not violate the applicable equipment rating of any equipment comprising the facility.
Fault	An event occurring on an electric system such as a short circuit, a broken wire, or an intermittent connection.
Fire Risk	The likelihood that a fire will ignite or spread in a particular

	geographic area.
Firm Demand	That portion of the Demand that a power supplier is obligated to provide except when system reliability is threatened or during emergency conditions.
Firm Transmission Service	The highest quality (priority) service offered to customers under a filed rate schedule that anticipates no planned interruption.
Flashover	An electrical discharge through air around or over the surface of insulation, between objects of different potential, caused by placing a voltage across the air space that results in the ionization of the air space.
Flowgate	A designated point on the transmission system through which the Interchange Distribution Calculator calculates the power flow from Interchange Transactions.
Forced Outage	1. The removal from service availability of a generating unit, transmission line, or other facility for emergency reasons. 2. The condition in which the equipment is unavailable due to unanticipated failure.
Frequency Bias	A value, usually expressed in megawatts per 0.1 Hertz (MW/0.1 Hz), associated with a Balancing Authority Area that approximates the Balancing Authority Area's response to Interconnection frequency error.
Frequency Bias Setting	A value, usually expressed in MW/0.1 Hz, set into a Balancing Authority ACE algorithm that allows the Balancing Authority to contribute its frequency response to the Interconnection.
Frequency Deviation	A change in Interconnection frequency.
Frequency Error	The difference between the actual and scheduled frequency. ($F_A - F_S$)
Frequency Regulation	The ability of a Balancing Authority to help the Interconnection maintain Scheduled Frequency. This assistance can include both turbine governor response and Automatic Generation Control.
Frequency Response	(Equipment) The ability of a system or elements of the system to react or respond to a change in system frequency. (System) The sum of the change in demand, plus the change in generation, divided by the change in frequency, expressed in megawatts per 0.1 Hertz (MW/0.1 Hz).
Generator Operator	The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.

Generator Owner		Entity that owns and maintains generating units.
Generator Shift Factor	GSF	A factor to be applied to a generator's expected change in output to determine the amount of flow contribution that change in output will impose on an identified transmission facility or Flowgate.
Generator-to-Load Distribution Factor	GLDF	The algebraic sum of a Generator Shift Factor and a Load Shift Factor to determine the total impact of an Interchange Transaction on an identified transmission facility or Flowgate.
Host Balancing Authority		1. A Balancing Authority that confirms and implements Interchange Transactions for a Purchasing Selling Entity that operates generation or serves customers directly within the Balancing Authority's metered boundaries. 2. The Balancing Authority within whose metered boundaries a jointly owned unit is physically located.
Hourly Value		Data measured on a Clock Hour basis.
Implemented Interchange		The state where the Balancing Authority enters the Confirmed Interchange into its Area Control Error equation.
Inadvertent Interchange		The difference between the Balancing Authority's Net Actual Interchange and Net Scheduled Interchange. (I_A – I_S)
Independent Power Producer	IPP	Any entity that owns or operates an electricity generating facility that is not included in an electric utility's rate base. This term includes, but is not limited to, cogenerators and small power producers and all other nonutility electricity producers, such as exempt wholesale generators, who sell electricity.
Institute of Electrical and Electronics Engineers, Inc.		IEEE
Interchange Distribution Calculator	IDC	The mechanism used by Reliability Coordinators in the Eastern Interconnection to calculate the distribution of Interchange Transactions over specific Flowgates. It includes a database of all Interchange Transactions and a matrix of the Distribution Factors for the Eastern Interconnection.
Interchange		Energy transfers that cross Balancing Authority boundaries.
Interchange Authority		The responsible entity that authorizes implementation of valid and balanced Interchange Schedules between Balancing Authority Areas, and ensures communication of Interchange information for reliability assessment purposes.

Interchange Schedule		An agreed-upon Interchange Transaction size (megawatts), start and end time, beginning and ending ramp times and rate, and type required for delivery and receipt of power and energy between the Source and Sink Balancing Authorities involved in the transaction.
Interchange Transaction		An agreement to transfer energy from a seller to a buyer that crosses one or more Balancing Authority Area boundaries.
Interchange Transaction Tag or Tag		The details of an Interchange Transaction required for its physical implementation.
Interconnected Operations Service		A service (exclusive of basic energy and transmission services) that is required to support the reliable operation of interconnected Bulk Electric Systems.
Interconnection		When capitalized, any one of the three major electric system networks in North America: Eastern, Western, and ERCOT.
Interconnection Reliability Operating Limit	IROL	A System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading Outages that adversely impact the reliability of the Bulk Electric System.
Interconnection Reliability Operating Limit T_v	IROL T_v	The maximum time that an Interconnection Reliability Operating Limit can be violated before the risk to the interconnection or other Reliability Coordinator Area(s) becomes greater than acceptable. Each Interconnection Reliability Operating Limit's T_v shall be less than or equal to 30 minutes.
Intermediate Balancing Authority		A Balancing Authority Area that has connecting facilities in the Scheduling Path between the Sending Balancing Authority Area and Receiving Balancing Authority Area and operating agreements that establish the conditions for the use of such facilities
Interruptible Load or Interruptible Demand		Demand that the end-use customer makes available to its Load-Serving Entity via contract or agreement for curtailment.
Joint Control		Automatic Generation Control of jointly owned units by two or more Balancing Authorities.
Limiting Element		The element that is 1.)Either operating at its appropriate rating, or 2,) Would be following the limiting contingency. Thus, the Limiting Element establishes a system limit.

Load		An end-use device or customer that receives power from the electric system.
Load Shift Factor	LSF	A factor to be applied to a load’s expected change in demand to determine the amount of flow contribution that change in demand will impose on an identified transmission facility or monitored Flowgate.
Load-Serving Entity		Secures energy and transmission service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.
Misoperation		1 Any failure of a Protection System element to operate within the specified time when a fault or abnormal condition occurs within a zone of protection. 2 Any operation for a fault not within a zone of protection (other than operation as backup protection for a fault in an adjacent zone that is not cleared within a specified time for the protection for that zone). 3 Any unintentional Protection System operation when no fault or other abnormal condition has occurred unrelated to on-site maintenance and testing activity.
Native Load		The end-use customers that the Load-Serving Entity is obligated to serve.
Net Actual Interchange		The algebraic sum of all metered interchange over all interconnections between two physically Adjacent Balancing Authority Areas.
Net Energy for Load		Net Balancing Authority Area generation, plus energy received from other Balancing Authority Areas, less energy delivered to Balancing Authority Areas through interchange. It includes Balancing Authority Area losses but excludes energy required for storage at energy storage facilities.
Net Interchange Schedule		The algebraic sum of all Interchange Schedules with each Adjacent Balancing Authority.
Net Scheduled Interchange		The algebraic sum of all Interchange Schedules across a given path or between Balancing Authorities for a given period or instant in time.
Network Integration Transmission Service		Service that allows an electric transmission customer to integrate, plan, economically dispatch and regulate its network reserves in a manner comparable to that in which the Transmission Owner serves Native Load customers.
Non-Firm Transmission Service		Transmission service that is reserved on an as-available basis and is subject to curtailment or interruption.

Non-Spinning Reserve	1. That generating reserve not connected to the system but capable of serving demand within a specified time. 2. Interruptible load that can be removed from the system in a specified time.	
Normal Clearing	A protection system operates as designed and the fault is cleared in the time normally expected with proper functioning of the installed protection systems.	
Normal Rating	The rating as defined by the equipment owner that specifies the level of electrical loading, usually expressed in megawatts (MW) or other appropriate units that a system, facility, or element can support or withstand through the daily demand cycles without loss of equipment life.	
Nuclear Plant Generator Operator	Any Generator Operator or Generator Owner that is a Nuclear Plant Licensee responsible for operation of a nuclear facility licensed to produce commercial power.	
Nuclear Plant Off-site Power Supply (Off-site Power)	The electric power supply provided from the electric system to the nuclear power plant distribution system as required per the nuclear power plant license.	
Nuclear Plant Licensing Requirements (NPLRs)	Requirements included in the design basis of the nuclear plant and statutorily mandated for the operation of the plant, including nuclear power plant licensing requirements for: 1 1) Off-site power supply to enable safe shutdown of the plant during an electric system or plant event; and 2 2) Avoiding preventable challenges to nuclear safety as a result of an electric system disturbance, transient, or condition.	
Nuclear Plant Interface Requirements (NPIRs)	The requirements based on NPLRs and Bulk Electric System requirements that have been mutually agreed to by the Nuclear Plant Generator Operator and the applicable Transmission Entities.	
Off-Peak	Those hours or other periods defined by NAESB business practices, contract, agreements, or guides as periods of lower electrical demand.	
On-Peak	Those hours or other periods defined by NAESB business practices, contract, agreements, or guides as periods of higher electrical demand.	
Open Access Same Time Information Service	OASIS	An electronic posting system that the Transmission Service Provider maintains for transmission access data and that allows all transmission customers to view the data simultaneously.

Open Access Transmission Tariff	OATT	Electronic transmission tariff accepted by the U.S. Federal Energy Regulatory Commission requiring the Transmission Service Provider to furnish to all shippers with non-discriminating service comparable to that provided by Transmission Owners to themselves.
Operating Plan	A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan.	
Operating Procedure	A document that identifies specific steps or tasks that should be taken by one or more specific operating positions to achieve specific operating goal(s). The steps in an Operating Procedure should be followed in the order in which they are presented, and should be performed by the position(s) identified. A document that lists the specific steps for a system operator to take in removing a specific transmission line from service is an example of an Operating Procedure.	
Operating Process	A document that identifies general steps for achieving a generic operating goal. An Operating Process includes steps with options that may be selected depending upon Real-time conditions. A guideline for controlling high voltage is an example of an Operating Process.	
Operating Reserve	That capability above firm system demand required to provide for regulation, load forecasting error, equipment forced and scheduled outages and local area protection. It consists of spinning and non-spinning reserve.	
Operating Reserve – Spinning	The portion of Operating Reserve consisting of: 1 • Generation synchronized to the system and fully available to serve load within the Disturbance Recovery Period following the contingency event; or 2 • Load fully removable from the system within the Disturbance Recovery Period following the contingency event.	
Operating Reserve – Supplemental	The portion of Operating Reserve consisting of: 1 • Generation (synchronized or capable of being synchronized to the system) that is fully available to serve load within the Disturbance Recovery Period following the contingency event; or 2 • Load fully removable from the system within the Disturbance Recovery Period following the contingency event.	

Operating Voltage		The voltage level by which an electrical system is designated and to which certain operating characteristics of the system are related; also, the effective (root-mean-square) potential difference between any two conductors or between a conductor and the ground. The actual voltage of the circuit may vary somewhat above or below this value.
Overlap Regulation Service		A method of providing regulation service in which the Balancing Authority providing the regulation service incorporates another Balancing Authority's actual interchange, frequency response, and schedules into providing Balancing Authority's AGC/ACE equation.
Peak Demand		1. The highest hourly integrated Net Energy For Load within a Balancing Authority Area occurring within a given period (e.g., day, month, season, or year). 2. The highest instantaneous demand within the Balancing Authority Area.
Performance-Reset Period		The time period that the entity being assessed must operate without any violations to reset the level of non compliance to zero.
Physical Security Perimeter		The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.
Planning Authority		The responsible entity that coordinates and integrates transmission facility and service plans, resource plans, and protection systems.
Point of Delivery	POD	A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction leaves or a Load-Serving Entity receives its energy.
Point of Receipt	POR	A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction enters or a Generator delivers its output.
Point to Point Transmission Service	PTP	The reservation and transmission of capacity and energy on either a firm or non-firm basis from the Point(s) of Receipt to the Point(s) of Delivery.
Pro Forma Tariff		Usually refers to the standard OATT and/or associated transmission rights mandated by the U.S. Federal Energy Regulatory Commission Order No. 888.
Protection System		Protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry.

Pseudo-Tie	A telemetered reading or value that is updated in real time and used as a “virtual” tie line flow in the AGC/ACE equation but for which no physical tie or energy metering actually exists. The integrated value is used as a metered MWh value for interchange accounting purposes.
Purchasing-Selling Entity	The entity that purchases or sells, and takes title to, energy, capacity, and Interconnected Operations Services. Purchasing-Selling Entities may be affiliated or unaffiliated merchants and may or may not own generating facilities.
Ramp Rate or Ramp	(Schedule) The rate, expressed in megawatts per minute, at which the interchange schedule is attained during the ramp period. (Generator) The rate, expressed in megawatts per minute, that a generator changes its output.
Rated Electrical Operating Conditions	The specified or reasonably anticipated conditions under which the electrical system or an individual electrical circuit is intend/designed to operate
Rating	The operational limits of a transmission system element under a set of specified conditions.
Reactive Power	The portion of electricity that establishes and sustains the electric and magnetic fields of alternating-current equipment. Reactive power must be supplied to most types of magnetic equipment, such as motors and transformers. It also must supply the reactive losses on transmission facilities. Reactive power is provided by generators, synchronous condensers, or electrostatic equipment such as capacitors and directly influences electric system voltage. It is usually expressed in kilovars (kvar) or megavars (Mvar).
Real Power	The portion of electricity that supplies energy to the load.
Reallocation	The total or partial curtailment of Transactions during TLR Level 3a or 5a to allow Transactions using higher priority to be implemented.
Real-time	Present time as opposed to future time. (From Interconnection Reliability Operating Limits standard.)
Receiving Balancing Authority	The Balancing Authority importing the Interchange.
Regional Reliability Organization	1. An entity that ensures that a defined area of the Bulk Electric System is reliable, adequate and secure. 2. A member of the North American Electric Reliability Council. The Regional Reliability Organization can serve as the Compliance Monitor.
Regional Reliability Plan	The plan that specifies the Reliability Coordinators and Balancing Authorities within the Regional Reliability Organization, and explains how reliability coordination

	will be accomplished.	
Regulating Reserve	An amount of reserve responsive to Automatic Generation Control, which is sufficient to provide normal regulating margin.	
Regulation Service	The process whereby one Balancing Authority contracts to provide corrective response to all or a portion of the ACE of another Balancing Authority. The Balancing Authority providing the response assumes the obligation of meeting all applicable control criteria as specified by NERC for itself and the Balancing Authority for which it is providing the Regulation Service.	
Reliability Coordinator	The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator’s vision.	
Reliability Coordinator Area	The collection of generation, transmission, and loads within the boundaries of the Reliability Coordinator. Its boundary coincides with one or more Balancing Authority Areas.	
Reliability Coordinator Information System	RCIS	The system that Reliability Coordinators use to post messages and share operating information in real time.
Remedial Action Scheme	RAS	See “Special Protection System”
Reportable Disturbance	Any event that causes an ACE change greater than or equal to 80% of a Balancing Authority’s or reserve sharing group’s most severe contingency. The definition of a reportable disturbance is specified by each Regional Reliability Organization. This definition may not be retroactively adjusted in response to observed performance.	

Reserve Sharing Group		A group whose members consist of two or more Balancing Authorities that collectively maintain, allocate, and supply operating reserves required for each Balancing Authority's use in recovering from contingencies within the group. Scheduling energy from an Adjacent Balancing Authority to aid recovery need not constitute reserve sharing provided the transaction is ramped in over a period the supplying party could reasonably be expected to load generation in (e.g., ten minutes). If the transaction is ramped in quicker (e.g., between zero and ten minutes) then, for the purposes of Disturbance Control Performance, the Areas become a Reserve Sharing Group.
Resource Planner		The entity that develops a long-term (generally one year and beyond) plan for the resource adequacy of specific loads (customer demand and energy requirements) within a Planning Authority Area.
Response Rate		The Ramp Rate that a generating unit can achieve under normal operating conditions expressed in megawatts per minute (MW/Min).
Request for Interchange	RFI	A collection of data as defined in the NAESB RFI Datasheet, to be submitted to the Interchange Authority for the purpose of implementing bilateral Interchange between a Source and Sink Balancing Authority.
Right-of-Way (ROW)		A corridor of land on which electric lines may be located. The Transmission Owner may own the land in fee, own an easement, or have certain franchise, prescription, or license rights to construct and maintain lines.
Scenario		Possible event.
Schedule		(Verb) To set up a plan or arrangement for an Interchange Transaction. (Noun) An Interchange Schedule.
Scheduled Frequency		60.0 Hertz, except during a time correction.
Scheduling Entity		An entity responsible for approving and implementing Interchange Schedules.
Scheduling Path		The Transmission Service arrangements reserved by the Purchasing-Selling Entity for a Transaction.
Sending Balancing Authority		The Balancing Authority exporting the Interchange.
Sink Balancing Authority		The Balancing Authority in which the load (sink) is located for an Interchange Transaction. (This will also be a Receiving Balancing Authority for the resulting Interchange Schedule.)
Source Balancing		The Balancing Authority in which the generation (source) is located for an Interchange Transaction. (This will also be a Sending Balancing Authority for the resulting Interchange

Authority	Schedule.)
System Operating Limit	The value (such as MW, MVar, Amperes, Frequency or Volts) that satisfies the most limiting of the prescribed operating criteria for a specified system configuration to ensure operation within acceptable reliability criteria. System Operating Limits are based upon certain operating criteria. These include, but are not limited to: 1 • Facility Ratings (Applicable pre- and post-Contingency equipment or facility ratings) 2 • Transient Stability Ratings (Applicable pre- and post-Contingency Stability Limits) 3 • Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability) 4 • System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits)
System Operator	An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.
Telemetering	The process by which measurable electrical quantities from substations and generating stations are instantaneously transmitted to the control center, and by which operating commands from the control center are transmitted to the substations and generating stations.
Thermal Rating	The maximum amount of electrical current that a transmission line or electrical facility can conduct over a specified time period before it sustains permanent damage by overheating or before it sags to the point that it violates public safety requirements.
Tie Line	A circuit connecting two Balancing Authority Areas.
Tie Line Bias	A mode of Automatic Generation Control that allows the Balancing Authority to 1.) maintain its Interchange Schedule and 2.) respond to Interconnection frequency error.
Time Error	The difference between the Interconnection time measured at the Balancing Authority(ies) and the time specified by the National Institute of Standards and Technology. Time error is caused by the accumulation of Frequency Error over a given period.
Time Error Correction	An offset to the Interconnection’s scheduled frequency to return the Interconnection’s Time Error to a predetermined value.

TLR Log		Report required to be filed after every TLR Level 2 or higher in a specified format. The NERC IDC prepares the report for review by the issuing Reliability Coordinator. After approval by the issuing Reliability Coordinator, the report is electronically filed in a public area of the NERC Web site.
Total Transfer Capability	TTC	The amount of electric power that can be moved or transferred reliably from one area to another area of the interconnected transmission systems by way of all transmission lines (or paths) between those areas under specified system conditions.
Transaction		See Interchange Transaction.
Transfer Capability		The measure of the ability of interconnected electric systems to move or transfer power *in a reliable manner* from one area to another over all transmission lines (or paths) between those areas under specified system conditions. The units of transfer capability are in terms of electric power, generally expressed in megawatts (MW). The transfer capability from "Area A" to "Area B" is *not g*enerally equal to the transfer capability from "Area B" to "Area A."
Transfer Distribution Factor		See Distribution Factor.
Transmission		An interconnected group of lines and associated equipment for the movement or transfer of electric energy between points of supply and points at which it is transformed for delivery to customers or is delivered to other electric systems.
Transmission Constraint		A limitation on one or more transmission elements that may be reached during normal or contingency system operations.
Transmission Customer		1. Any eligible customer (or its designated agent) that can or does execute a transmission service agreement or can or does receive transmission service. 2. Any of the following responsible entities: Generator Owner, Load-Serving Entity, or Purchasing-Selling Entity.
Transmission Line		A system of structures, wires, insulators and associated hardware that carry electric energy from one point to another in an electric power system. Lines are operated at relatively high voltages varying from 69 kV up to 765 kV, and are capable of transmitting large quantities of electricity over long distances.
Transmission Operator		The entity responsible for the reliability of its "local" transmission system, and that operates or directs the operations of the transmission facilities.
Transmission Owner		The entity that owns and maintains transmission facilities.

Transmission Planner		The entity that develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within its portion of the Planning Authority Area.
Transmission Reliability Margin	TRM	The amount of transmission transfer capability necessary to provide reasonable assurance that the interconnected transmission network will be secure. TRM accounts for the inherent uncertainty in system conditions and the need for operating flexibility to ensure reliable system operation as system conditions change.
Transmission Service		Services provided to the Transmission Customer by the Transmission Service Provider to move energy from a Point of Receipt to a Point of Delivery.
Transmission Service Provider		The entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.
Vegetation		All plant material, growing or not, living or dead.
Vegetation Inspection		The systematic examination of a transmission corridor to document vegetation conditions.
Wide Area		The entire Reliability Coordinator Area as well as the critical flow and status information from adjacent Reliability Coordinator Areas as determined by detailed system studies to allow the calculation of Interconnected Reliability Operating Limits.