Supporting Statement for

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

As Proposed in Docket No. RM06-22-000
(A Notice of Proposed Rulemaking Issued July 20, 2007)

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-xxxx) is a new Commission data collection, (filing requirements), as contained in 18 Code of Federal Regulations, Part 40.

FERC-725B is a new information collection implementing standards that were previously part of a voluntary program. The Commission requests that OMB approve the projected estimates reported in this submission. 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. These Reliability Standards are approved by the Commission pursuant to its authority under section 215 of the Federal Power Act (FPA), which authorizes the Commission to approve a Reliability Standard proposed by the Electric Reliability Organization (ERO) if the Commission determines that it is just and reasonable, not unduly discriminatory or preferential and in the public interest. The Reliability Standards approved in this NOPR 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

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).

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 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.

In accordance with section 215(d)(2) of the FPA and § 39.5(c) of the Commission's regulations, the Commission is required to give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard or to a Regional Entity organized on an Interconnection-wide basis with respect to a proposed Reliability Standard or a proposed modification to a Reliability Standard to be applicable within that Interconnection.[5]

RM06-22-000 NOPR

The Commission proposes to approve eight Critical Infrastructure Protection (CIP) Reliability Standards submitted to the Commission for approval by the North American Electric Reliability Corporation (NERC). The CIP Reliability Standards require certain users, owners, and operators of the Bulk-Power System to comply with specific requirements to safeguard critical cyber assets. In addition, in accordance with section 215(d)(5) of the FPA, the Commission proposes to direct NERC to develop modifications to the CIP Reliability Standards to address specific concerns identified by the Commission. Approval of these standards will help protect the nation's Bulk-Power System against potential disruptions from cyber attacks.

---

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

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.[6] 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), transmission owners and operators, and generation owners and operators that perform defined functions. Specifically, it established a self-certification process relating to the security of system control centers of the applicable entities. The Urgent Action 1200 standard remained in effect on a voluntary basis until June 1, 2006, at which time the eight CIP Reliability Standards that are the subject of the current rulemaking replaced the Urgent Action 1200 standard.

On August 28, 2006, NERC submitted to the Commission for approval the following eight proposed CIP Reliability Standards:[7]

- **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.

---

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

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

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

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

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

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

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.[8] 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 the 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.[9] In response to the outages, the Secretary of Energy convened a task force to advise 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.[10] 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.[11]

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.

---

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

9 The Electric Power Outages in the Western United States, July 2-3, 1996, at 76 (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).

10 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.

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

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

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

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

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

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

sound basis for action.[14] Likewise, in this NOPR, the Commission recognizes the merits of specific Blackout Report recommendations as a basis for proposing certain modifications to the eight CIP Reliability Standards that the Commission proposes to approve.

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 will evaluate the proposed CIP Reliability Standards in the context of the above over-arching considerations.

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. One task of this office has been to participate in North American Reliability Council's (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 also directed transmission owners to report by June 2004, on the vegetation management practices they use for transmission and rights of way.[15] FERC's Reliability Division 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. Reasonable supply relative to demand is essential for competitive markets to work. Without sufficient delivery infrastructure, some suppliers will not be able to enter the market, customer

14 See Order No. 693 at P 234.

15 1902-0207, FERC-723 "Vegetation Report" in Docket No. EL04-52-000. El04-52-000. This was a one-time information collection that expired 10/31/04. FERC submitted a report to Congress in September 2004 that set forth the Commission's findings and recommendations, including the need for mandatory, enforceable reliability rules.

choices will be limited, and prices will be needlessly volatile. 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.**

The Commission has developed the capability for electronic filing of all major submissions to the Commission. In Order No. 619, the Commission established an electronic filing initiative that permits over 40 qualified types of documents to be filed over the Internet to its website. This includes the ability to submit standard forms using software that is readily available and easy to use. Electronic filing, combined with electronic posting and service over the web site, permits staff and the public to obtain filings in a faster and more efficient manner. The Commission is working to expand the qualified types of documents that can be filed over the Internet.

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. (See item no. 8 for further discussion.)

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 proposed 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 and 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.

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

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

A number of commenters stated that the focus should be on those entities that own or operate critical assets, rather than being addressed in terms of "large" or "small" size of entities.[16] These commenters warn that a blanket waiver that uniformly exempts small entities from compliance with certain provisions of the proposed CIP Reliability Standards therefore would not be appropriate. NERC and other commenters maintain that applicability should not be determined based on cyber connections but, rather by identifying those users, owners and

16 E.g., Allegheny, California PUC, EEI, Georgia System, ISO-NE, MidAmerican, NERC, ReliabilityFirst, Northeast Utilities, NRECA, Ontario IESO, Tampa Electric, and Xcel.

operators of the Bulk-Power System that own or operate critical assets and associated critical cyber assets. Another group of commenters urged that the Commission not impose the same compliance obligations on smaller entities as on larger entities when a violation by the smaller entity would not have a critical impact on the Bulk-Power System. They maintain that adverse impacts on the grid from small entities would be an uncommon occurrence and urged a case-by-case approach to granting waivers from compliance with the CIP Reliability Standards.[17]

Commission Proposal

The Commission's determinations in Order No. 693 are relevant to deciding the applicability of the CIP Reliability Standards to small entities. In Order No. 693, the Commission approved NERC's compliance registry process as a reasonable means "to ensure that the proper entities are registered and that each knows which Commission-approved Reliability Standard(s) are applicable to it."[18] Further, the Commission approved NERC registry criteria that identify specific categories of users, owners and operators of the Bulk-Power System and criteria for registering entities within each of the categories.[19]

The Commission will also rely on the NERC registration process to determine applicability with the CIP Reliability Standards. In other words, an entity would be responsible to comply with the CIP Reliability Standards if the entity is (1) registered by NERC under one or more functional categories and (2) within a functional category for which the entity is registered as identified in the Applicability section of the CIP Reliability Standards. However, even though it is the Commission's present intention to rely on the NERC registration process to identify appropriate entities, the Commission remains concerned about the possibility of entities not identified by the registration process becoming a weakness in the security of the Bulk-Power System. In this regard, the Commission notes that, in Order No. 693, the Commission explained that, "if there is an entity that is not registered and NERC later discovers that the entity should have been subject to the Reliability Standards, NERC has the ability to add the entity, and possibly other entities of a similar class, to the registration list . . . ."[20] In addition, in Order No. 693, the Commission indicated that it would further examine applicability issues under section 215 of the FPA in a future proceeding, and intends in this NOPR to make the same examination.

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

17 E.g., APPA/LPPC and Santa Clara.
18 Order No. 693 at P 92, quoting ERO Certification Order, 116 FERC ¶ 61,062 at P 689.
19 Order No. 693 at P 93-95. NERC's Statement of Compliance Registry Criteria (Revision 3), approved by the Commission in Order No. 693, is available on NERC's website at: ftp://www.nerc.com/pub/sys/all_updl/ero/Statement_of_Compliance_Registry_Criteria_Rev3.pdf.
20 Order No. 693 at P 97.

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

Similarly, the Commission is relying on the NERC registration process to include all critical assets and associated critical cyber assets. For example, if assets are important to the reliability of the Bulk-Power System, such as black start units, the Commission would expect that the NERC registration process would identify the owners or operators of those units as critical, and require them to register, even though the facilities may be "smaller" or at low voltages. Demand side aggregators might also need to be included in the NERC registration process if their load shedding capacity would affect the reliability or operability of the Bulk-Power System.

As discussed in the NOPR, as an initial compliance step, each entity that is responsible for compliance with the CIP Reliability Standards must identify critical assets through the application of a risk-based assessment as required by CIP-002-1. Whether that entity must comply with the remainder of the requirements in the CIP Reliability Standards would depend on the outcome of that assessment and the subsequent identification of critical cyber assets, also required by CIP-002-1. Thus, CIP002-1 acts as a filter, determining which entities must comply with the remaining CIP requirements (i.e., CIP-003-1 through CIP-009-1). (See further discussion on CIP-002-1 under item no. 8 of this submission.

Notes:

The compliance registry identifies specific categories of users, owners and operators that correlate to the types of entities responsible for performing specific functions described in the NERC Functional Model.[21] These same functional types are also used by the ERO to identify the entities responsible for compliance with a particular Reliability Standard in the Applicability section of a given standard. Thus, each registered entity will be registered under one or more appropriate functional categories, and that registration by function will determine with which Reliability Standards – and Requirements of those Reliability Standards – the entity must comply. In other words, a user, owner or operator of the Bulk-Power System would be required to comply with each Reliability Standard that is applicable to any one of the functional types for which it is registered.

21 The Statement of Compliance Registry Criteria, as well as the Functional Model, identify, inter alia, the following functions: balancing authority, distribution provider, generator operator, generator owner, load serving entity, planning authority, purchasing-selling entity, transmission owner, transmission operator and transmission service provider. An entity may be registered under one or more of these functions.

According to the Small Business Act (SBA), a small electric utility is defined as one that has a total electric output of less than four million MWh in the preceding year. Thus, the set of small entities that must comply with mandatory Reliability Standards would be those that exceed the ERO registry criteria but still meet the SBA definition.

The Commission's analysis shows that the DOE's Energy Information Administration (EIA) reports that there were 3,284 electric utility companies in the United States in 2005,[22] and 3,029 of these electric utilities qualify as small entities under the SBA definition. Of these 3,284 electric utility companies, the EIA subdivides them as follows: (1) 883 cooperatives of which 852 are small entity cooperatives; (2) 1,862 municipal utilities, of which 1842 are small entity municipal utilities; (3) 127 political subdivisions, of which 114 are small entity political subdivisions; (4) 159 power marketers, of which 97 individually could be considered small entity power marketers;[23] (5) 219 privately owned utilities, of which 104 could be considered small entity private utilities; (6) 25 state organizations, of which 16 are small entity state organizations and (7) nine federal organizations of which four are small entity federal organizations.

Alternatives

In Order No. 693, which approved 83 Reliability Standard for the Bulk-Power System, the Commission discussed several alternatives that are also applicable to the CIP Reliability Standards.[24] Several of these have already been implemented such as the approval of the NERC definition of bulk electric system, which reduces significantly the number of small entities responsible for compliance with mandatory Reliability Standards.[25] Further, the Commission adopted the NERC compliance registry process to identify the entities responsible for compliance with mandatory Reliability Standards.

Another significant alternative is the ability for a small entity to join a joint action agency or similar organization. Such an organization may accept responsibility for compliance with mandatory Reliability Standards on behalf of its members and also may divide the responsibility for compliance with its members. The Commission generally approved the concept of joint action agencies in Order No. 693 and directed NERC to submit implementing procedures.[26] NERC submitted revisions to its Rules of Procedure to allow for joint action agencies and similar organizations and, in an order issuing concurrently with this NOPR, the Commission approves NERC's joint action agency rules. These rules, supported by APPA, NRECA and others, will provide significant flexibility for small entities on how they will achieve compliance with the CIP Reliability Standards or to assign compliance responsibility to a central

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

23 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.

24 See Order No. 693 at P 1945.

25 Id. at P 75, 1945.

26 Id. at P 107.

organization.

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 are due by October 5, 2007.

Background

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

The CIP Assessment raised two issues regarding applicability of the CIP Reliability Standards. First, it stated that, although it is likely that NERC and the Regional Entities[27] are not directly subject to mandatory Reliability Standards, their compliance with the CIP Reliability Standards is important to the extent that they have cyber communications with users, owners or operators of the Bulk-Power System.[28] The CIP Assessment suggested that NERC and Regional Entity compliance could be required pursuant to NERC's Rules of Procedure. Some commenters pointed out that NERC out-sources critical application systems that are relied upon by many responsible entities, such as the Interchange Distribution Calculator, and

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

28 See CIP Assessment at 12-14.

suggested that the out-source provider should be contractually compelled to comply with the CIP Reliability Standards, with NERC ultimately responsible for non-compliance.[29]

Second and as noted above, the CIP Assessment raised concerns about the appropriateness of a size threshold, below which small entities would be exempt from compliance. (The Commission provides a full discussion of these concerns and its response in item no. 5 above.)

The Commission agrees with the commenters that access to information essential to the operation of critical cyber assets by out-sourced entities that are not otherwise subject to the CIP Reliability Standards presents a potential vulnerability to the Bulk-Power System. The Commission understands that, on occasion, NERC negotiates contracts with such third party vendors, and the products developed by the vendors are then used by responsible entities that, as owners of the critical cyber assets, are ultimately responsible for their cyber security protection under the CIP Reliability Standards. The Commission is inviting comments in the NOPR on whether and how such out-sourced entities should be contractually obligated to comply with the CIP Reliability Standards while satisfying their other contractual obligations.

Compliance Measured by Outcome

Performance-Based Standards

The CIP Assessment expressed concern that the lack of specificity within the proposed CIP Reliability Standards could result in inadequate implementation efforts and inconsistent results.[30] NERC, along with a number of other commenters, stated that the CIP Reliability Standards are not prescriptive, positing that the level of specificity they embody is appropriate. NERC explained that the use of a performance-based structure frames the CIP Reliability Standards in terms of required results or outcomes with criteria for verifying compliance, but without prescribing the methods for achieving the required results. In other words, the specific means to achieve that outcome are left to the discretion of the responsible entity. Such an approach contrasts with a prescribed or design-based standard. NERC concluded that, when taken together, the proposed Reliability Standards constitute a comprehensive set of cyber security activities, stating that it is more important that a pre-defined, desirable outcome is achieved than prescribing the means to that end.

Commission Proposal

The Commission generally agrees that use of performance-based standards is a part of the design of cyber security safeguards for the Bulk-Power System's critical assets. However, as the Commission indicated in Order No. 672, performance-based standards may not always be appropriate, for example, in situations where "the 'how' may be inextricably linked to the Reliability Standard and may need to be specified to ensure the enforceability of the standard."[31]

29 E.g., ISO-NE, ISO/RTO Council, and SPP.

30 CIP Assessment at 3.

.

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

Accordingly, where necessary, the Commission proposes to direct NERC to modify the CIP Reliability Standards to address the "how." Moreover, the Commission is concerned that, while NERC explains that the CIP Reliability Standards are performance-based, the CIP Reliability Standards do not provide a mechanism to measure performance or otherwise determine whether a responsible entity has met the goals of a particular requirement set forth in the standards.

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

Adequacy of Outcomes

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

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

NERC and others do not share the CIP Assessment concern regarding the focus on documentation.[32] NERC and ReliabilityFirst acknowledged the extensive use of documentation throughout the CIP Reliability Standards, but note that the majority of this documentation is used to demonstrate that the Requirements have been met. NERC indicated that, while the "mere possession of documentation" does not guarantee compliance, appropriate documentation is essential to demonstrate that steps to comply with the Requirements have been taken and will streamline after-the-fact compliance audits. Similarly, EEI believes that the quality of the documentation is an important factor for assessing compliance and should be the subject of an audit. FirstEnergy and Santa Clara stated that it would be helpful for NERC to provide guidance on what constitutes reasonable documentation.

32 E.g., ReliabilityFirst, APPA/LPPC, and SPP.

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

Commission Proposal

The Commission agrees with NERC that, while documentation is necessary, the documentation by itself does not satisfy the Requirements of a Reliability Standard. Rather, implementation of the substance of the Requirements is most important in determining compliance. As the Commission explained in Order No. 693, "while Measures and Levels of Non-Compliance provide useful guidance to the industry, compliance will in all cases be measured by determining whether a party met or failed to meet the Requirement given the specific facts and circumstances of its use, ownership or operation of the Bulk-Power System."[33] Moreover, the Commission recognized that:

> The most critical element of a Reliability Standard is the Requirements. As NERC explains, "the Requirements within a standard define what an entity must do to be compliant . . . [and] binds an entity to certain obligations of performance under section 215 of the FPA." If properly drafted, a Reliability Standard may be enforced in the absence of specified Measures or Levels of Non-Compliance.[34]

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

Related, certain Requirements of the CIP Reliability Standards obligate a responsible entity to develop and maintain a plan, policy or procedure. However, such Requirements do not always explicitly require implementation of the plan, policy or procedure.[35] The Commission interprets such provisions to include an implicit requirement to implement the plan, policy or

33 Order No. 693 at P 253.

34 Id., quoting NOPR at P 105 (footnote omitted).

35 See, e.g., CIP-006-1, Requirement R1 (requiring a responsible entity to "create and maintain a 'physical security plan'"); cf. CIP-003-1, Requirement R1 (requiring a responsible entity to "document and implement a cyber security policy").

procedure; and to make a responsible entity subject to a non-compliance action for failing to implement the policy. Such an interpretation is reasonable to prevent the scenario in which the ERO, Regional Entity or the Commission could assess a penalty against a responsible entity for failure to develop a plan, policy or procedure that satisfies the Requirements of the Reliability Standard, but unable to assess a penalty against a responsible entity that has developed an adequate plan but fails to implement it. Further, the Commission proposes that the ERO, in developing modifications to the CIP Reliability Standards, include explicitly in such Requirements that a responsible entity must implement a plan, policy or procedure that it is required to develop.

Implementation Plan

Unlike the Reliability Standards approved in Order No. 693, which NERC formulated based on existing voluntary standards, the CIP Reliability Standards are new and require applicable entities in many cases to develop new cyber security systems and procedures, which will take time to develop and implement. To address this task, NERC developed an implementation plan that includes a proposed four-stage schedule for implementing the proposed CIP Reliability Standards over a three-year period.[36]

The Implementation Plan sets out a proposed schedule for accomplishing the various tasks associated with compliance with the CIP Reliability Standards. The schedule gives a timeline by calendar quarters for completing various tasks and prescribes milestones for when a responsible entity must: (1) "begin work;" (2) "be substantially compliant" with a requirement; (3) "be compliant" with a requirement; and (4) "be auditably compliant" with a requirement.

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

CIP Assessment

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

36 NERC August 28, 2006 Filing, Exhibit B "Implementation Plan for Cyber Security Standards" (Implementation Plan).

Comments

A number of commenters agreed that some type of assessment, although not necessarily in the form of an audit, is both possible and potentially beneficial prior to the time an entity achieves "auditably compliant" status.[37] NERC agreed that there is a benefit to ensuring that responsible entities are moving timely toward "auditably compliant" status. While NERC believes that audits at an interim stage are not possible, it stated that it plans to monitor progress through self-certification without assessing penalties. Other commenters opposed interim audits, stating that they could interfere with implementation plans and lead to penalties for non-compliance.[38]

Commission Proposal

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

However, the Commission is concerned whether the industry will be fully prepared for compliance upon reaching the implementation deadline and will take reasonable action to protect the Bulk-Power System during this interim period. The Commission believes that NERC's plans to require self-certification during the interim period are helpful. NERC, however, does not indicate the interval for self-certification. The Commission believes that an annual certification would not allow adequate monitoring of progress and propose to direct that the ERO develop a self-certification process with more frequent certifications, either tied to target dates in the schedule or perhaps quarterly or semi-annual certifications. While the Commission agrees with NERC that an entity should not be subject to a monetary penalty if it is unable to certify that it is on schedule, such an entity should explain to the ERO the reason it is unable to self-certify. The ERO and the Regional Entities should then work with such an entity either informally or, if appropriate, by requiring a remedial plan to assist such an entity in achieving full compliance in a timely manner. Further, the ERO and the Regional Entities should provide informational guidance, upon request, to assist a responsible entity in assessing its progress in reaching "auditably compliant" status.

To further address the Commission's concerns about the period prior to when responsible entities achieve full compliance with the CIP Reliability Standards, the Commission also proposes to direct the ERO to add a cyber security assessment to NERC's existing readiness

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

38 E.g., ATC, EEI, National Grid, Tampa Electric, and FirstEnergy.

reviews. In this readiness assessment process, the ERO should assist in the identification of best practices and deficiencies of the reviewed entities, both to help them prepare for implementation of the CIP Reliability Standards and to assess the status of their compliance efforts. The readiness reviews will also help the Commission to evaluate the potential effectiveness of the cyber security Reliability Standards before they are implemented by disclosing the progress made by reviewed entities in their CIP Reliability Standards implementation efforts.

Specific Standards:

CIP-002-1 – Critical Cyber Asset Identification

Reliability Standard CIP-002-1 deals with the identification of critical cyber assets. The NERC glossary defines "cyber assets" as "programmable electronic devices and communication networks including hardware, software, and data." It defines "critical cyber assets" as "cyber assets essential to the reliable operation of critical assets." NERC defines "critical assets" as "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."[39]

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

The CIP Assessment emphasized that, while CIP-002-1 through CIP-009-1 function as an integrated whole, CIP-002-1 is a key to the success of the cyber security framework that these Reliability Standards seek to create.[40] The CIP Assessment also stressed that, because CIP-002-1 addresses the assessment methodology and process for identifying critical assets and critical cyber assets, it represents the critical first step that can fundamentally affect the chances for successful implementation of the remaining CIP Reliability Standards. The methodology and process used by a responsible entity must be stringent and rigorous. Otherwise, a responsible entity may fail to identify some facilities that are critical to effective cyber protection and, as a consequence, leave them vulnerable to an attack that could threaten the reliability of the Bulk-Power System.

39 "The term 'reliable operation' means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements." EPAct 2005, section 215 (a)(4).

40 CIP Assessment at 16-17.

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

Risk-Based Assessment Methodology

CIP Assessment

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

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

Comments

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

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

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

NERC and others oppose including additional specificity, claiming that CIP-002-1 is specifically written to allow each responsible entity the flexibility to implement it as it applies to the specific circumstances within each organization, and at each location containing critical cyber assets.[41] These commenters are concerned that a Commission directive to include additional guidance would restrict the needed flexibility. For example, APPA argued that the proposed provisions provide an adequate basis for evaluating the methodology, stating that prescribing a national-level "one size fits all" risk-based assessment methodology would require a costly effort to comply, but would not result in measurable cyber security improvements. APPA added that every entity's risk-based assessment will be subject to challenge by an audit team from time-to-time, which will include review by peer technical experts who share the goal of preventing any successful attack on critical assets. AMP-Ohio suggested that it would be inappropriate to divide the Bulk Electric System into a large number of small, discrete and in some cases rather isolated pieces and then to assign responsibility to each of these small pieces to determine what is or is not critical to the reliable operation of the Bulk Electric System.

Commission Proposal

Most commenters on the CIP Assessment acknowledged the importance of CIP-002-1 in ensuring that an appropriate set of critical assets is identified. However, many commenters oppose any modification to CIP-002-1 to provide additional specificity regarding the risk

41 E.g., ReliabilityFirst, EEI, EPSA, and APPA.

assessment methodology for identifying critical assets, based on concerns that such specificity will impede the needed flexibility that is currently provided by the Reliability Standard.

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

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

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

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

to such entities that would assist them in determining whether their assets are critical to the Bulk-Power System.

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

Internal Approval of Risk Assessment

Requirement R4 of CIP-002-1 requires that a senior manager "or delegate(s)" must approve annually the list of critical assets and critical cyber assets. The CIP Assessment suggested that this senior management involvement should be extended to approving the risk-based assessment methodology developed pursuant to Requirement R1.[42] Several commenters disagreed,[43] stating that this approval is implied by the requirement for senior management approval of the critical asset list and the critical cyber asset list. Other commenters generally believe that senior management approval of the risk-based assessment methodology would be a benefit.[44]

Commission Proposal

The Commission believes that senior management approval of the risk-based assessment methodology has clear benefits that exceed any additional burden placed on the responsible entities, and the rigor that the senior management approval would encourage is worth the effort. As explained in the CIP Assessment, since a poor methodology will likely result in an inadequate identification of critical assets and critical cyber assets, senior management awareness and approval of the chosen risk-based assessment methodology is of critical importance.[45] It is not clear to the Commission that, as some commenters suggested, senior management approval of the risk-based assessment methodology is implicit in the requirement that senior management approve the critical asset list and critical cyber asset list. Commenters did not object to the concept, but only believed that it might be redundant. The Commission believes this additional layer of oversight is important and should be made explicit. The Commission also notes that requiring this senior management approval helps to implement the Blackout Report's Recommendation 43, which calls for establishing "clear authority and ownership for physical and cyber security."[46]

Therefore, in accordance with section 215(d)(5) of the FPA and § 39.5(f) of its regulations, the Commission proposes to direct that the ERO develop a modification to CIP-

42 CIP Assessment at 17-18.
43 NERC, ReliabilityFirst, and Santa Clara.
44 E.g., APPA/LPPC, FirstEnergy, National Grid, Progress Energy, and Xcel.
45 CIP Assessment at 18.
46 See Blackout Report at 169, Recommendation 43.

002-1 through its Reliability Standards development process to include a requirement that a senior manager annually review and approve the risk-based assessment methodology.

Oversight of Critical Assets Identification

The CIP Assessment emphasized the underlying importance that each responsible entity develops accurate lists of critical assets and critical cyber assets. Several commenters noted that responsible entities currently lack a wide-area view that would enable them to better assess the risks associated with certain assets.[47] They suggested that guidance or oversight from an external organization could help ensure that responsible entities have properly identified critical assets from a regional perspective. Cleveland Public Power suggested that the Regional Entities should assume this role. Similarly, AMP-Ohio recommends that the Regional Entities should be responsible for identifying critical assets, with input from reliability coordinators and transmission planners. EPSA indicates that independent system operators (ISOs) and regional transmission organizations (RTOs) could provide guidance to individual companies in assessing critical assets and their vulnerability, in coordination with NERC and the Commission.

NERC, however, opposes regional oversight, stating that "[i]t is not the function of the standards to implement an oversight or hierarchical organization for determining risks or vulnerabilities."[48] NERC suggested that regional perspective is gained through information sharing forums such as the Electricity Sector Information Sharing and Analysis Center (ESISAC)[49] and NERC's Critical Infrastructure Protection Committee.

Commission Proposal

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

On the other hand, the Commission believes that a formal or systematic approach to external oversight of the identification of critical assets would assure a wide-area view. Such an approach, on a regional basis, would better ensure that responsible entities are identifying

47 E.g., AMP-Ohio, EPSA, and Cleveland Public Power.

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

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

similar assets. Even taking into account the individual circumstances of a responsible entity, the Commission would expect certain trends in critical asset identification within a class of responsible entities, such as generator owners or transmission owners. If the vast majority of transmission owners, for example, identified a certain asset as critical, and a few did not, this result could be due to the unique circumstances of those transmission owners or from a flawed risk-based assessment methodology. However, without external oversight using a wide-area view, such trends or deviations would never be identified prior to an incident or audit, perhaps precluding a necessary adjustment to a particular critical asset list. In addition, a wide-area view would help to ensure that assets that have regional importance, such as for reactive power supply, are included as critical assets.

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

Moreover, the Commission notes that the definition of "critical cyber assets" encompasses data.[50] Thus, marketing or other data essential to the proper operation of a critical asset, and possibly the computer systems that produces or processes that data, would be considered critical cyber assets subject to the CIP Reliability Standards. Therefore, the Commission proposes to direct the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to include computer systems that produce the data.

The Commission is concerned that all critical assets are identified, and interprets the phrase, "[t]he risk-based assessment shall consider the following assets:" in Requirement R1.2 to mean that a responsible entity must be able to show, based on the risk-based assessment methodology used, why specific assets were or were not chosen as critical assets. The Commission is also concerned that sufficient rigor is applied in examining whether control systems are determined to be critical assets. While it seems obvious that an evaluation of a control system for critical asset status would consider the potential loss of operability of the control center due to power or communications failure, the Commission also believes that such an evaluation should include an examination of any misuse of the control system, the impact this misuse could have on any electric facilities that the responsible entity controls, and the

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

combined impact of such facilities. Therefore, the Commission proposes to direct the ERO to modify Requirement R1.2 to clarify the requirement to show why specific assets were/were not chosen as critical assets, and to require the consideration of misuse of control systems.

Interdependency

The CIP Assessment noted that CIP-002-1 does not address the issue of interdependency with other infrastructures and explained that there may be occasions where an electric sector asset, while not critical to Bulk-Power System reliability, may be crucial to the operation of another critical infrastructure.[51] The CIP Assessment asked (1) whether this issue is appropriate for inclusion in CIP-002-1 and (2) whether this topic is an area for future coordination and collaboration with other industries and government agencies.

Commenters generally agreed that this issue is worthy of consideration and coordination and cooperation could be advantageous. However, most commenters consider the topic outside the scope of CIP-002-1.[52] By contrast, one commenter posited that there is a clear need to articulate that this type of interdependency analysis should be part of the responsible entity's determination of critical assets.[53]

Commission Proposal

Reliability Standard CIP-002-1 pertains to the identification of assets critical to Bulk-Power System reliability. While broader interdependency issues cannot be ignored, the Commission intends to revisit this matter through future proceedings and with other agencies. This work will help to inform the electric sector and this Commission about the need for future Reliability Standards, especially when the interdependent infrastructures affect generating capabilities, such as through fuel transportation.

Commission Proposal Summary

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

51 CIP Assessment at 17.

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

53 ISA Group.

CIP-008-1 – Incident Reporting and Response Planning

Proposed Reliability Standard CIP-008-1 requires a responsible entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets. Specifically, Requirement R1 of CIP-008-1 requires responsible entities to develop and maintain an Incident Response Plan that addresses responses to a cyber security incident. The plan should characterize and classify pertinent events as reportable cyber security incidents and provide corresponding response actions. The response actions should include: (1) the roles and responsibilities of the incident response teams, (2) procedures for handling incidents, and (3) associated communication plans. In addition, cyber security incidents must be reported to the ESISAC either directly or through an intermediary. The Incident Response Plan should be reviewed and tested at least annually. Changes to the Incident Response Plan are to be documented within 90 days. Responsible entities must retain documentation related to reportable cyber security incidents for a period of three years.

The Commission proposes to approve Reliability Standard CIP-008-1 as mandatory and enforceable. In addition, the Commission proposes to direct the ERO to develop modifications to this Reliability Standard. In its discussion below, the Commission addresses its concerns in the following topic areas regarding CIP-008-1: (1) definition of a reportable incident; (2) reporting; and (3) full operational exercises and lessons learned.

Definition of a Reportable Incident

The CIP Assessment noted that Requirement R1 of CIP-008-1 makes reference to reportable cyber security incidents, but it does not provide a definition of a "reportable incident." Consequently, cyber security incidents may go unreported depending upon a responsible entity's interpretation of a "reportable incident."[54]

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

A number of commenters stated that FERC should require NERC to clarify what types of cyber security incidents are "reportable incidents." National Grid points out that the Commission should seek to ensure that any further interpretation of what is considered a reportable incident be consistent with the reporting obligations of utilities under the DOE Form 417. Allegheny suggests that, in order to maintain consistency, the DOE Form 417 reporting

54 CIP Assessment at 36. The CIP Assessment recognized that NERC's FAQ document answers the question of "what is a reportable incident?" by referencing definitions in the ESISAC Indications, Analysis, and Warnings Program guidelines document entitled "Indications, Analysis and Warnings Program Standard Operating Procedure" and the Department of Energy Form OE 417 Report entitled "Electric Emergency Incident and Disturbance Report." However, since these materials are not incorporated into the proposed CIP Reliability Standards, CIP-008-1 remains ambiguous in this regard. North American Electric Reliability Council, Frequently Asked Questions (FAQs) Cyber Security Standards CIP-002-1 through CIP-009-1, March 6, 2006, page 27, question 1.

requirements should be referenced as part of the Reliability Standard. Progress Energy, on the other hand, states that such increased specificity is not possible and would be subject to constant revision in response to ever-changing incidents or threats to cyber systems.

Commission Proposal

The Commission believes that guidance regarding what should be included in the term "reportable incident" can be provided. The Blackout Report pointed out the need for "uniform standards for the reporting and sharing of physical and cyber security incident information" in Recommendation 42.[55] As NERC and ReliabilityFirst state, the definition of a "reportable incident" is currently undergoing extensive industry debate. This debate can be a catalyst for developing an appropriate level of guidance. As noted in the NERC Glossary, a "cyber security incident" is defined as a compromise, or an attempt to compromise, the electronic security perimeter or physical security perimeter of a critical asset. The Commission proposes to direct the ERO to: (1) develop and include in CIP-008-1 language that takes into account a breach that may occur through cyber or physical means;[56] (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced.

Reporting

CIP-008-1, Requirement R1.3, requires that each responsible entity establish a process for reporting cyber security incidents to the ESISAC. The responsible entity must ensure that all reportable cyber security incidents are reported to the ESISAC either directly or through an intermediary.

ESISAC procedures require the reporting of a cyber incident within one hour of a suspected malicious incident. However, compliance with ESISAC's Indications, Analysis and Warnings Program (IAW) Standard Operating Procedure (SOP) is voluntary. The CIP Assessment noted the importance of other responsible entities receiving timely information regarding a reportable cyber security incident, so they can take precautions against being the target of a similar incident. The CIP Assessment stated that, depending upon the nature of the incident, timelines of incident reporting may be critical. It expressed concern with regard to the voluntary nature of the one-hour reporting requirement associated with ESISAC's IAW SOP. Therefore, the CIP Assessment requested comment on whether CIP-008-1 should incorporate ESISAC's one-hour reporting limit or another reporting interval that would provide adequate time for another responsible entity to take meaningful precautions.

55 See also Blackout Report at 168, Recommendation 42.

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

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

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

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

Commission Proposal

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

Second, while the Commission agrees that, in the aftermath of a cyber attack, restoring the system is the utmost priority, the Commission does not believe that sending this short report would be a time consuming distraction, and the Commission judges that its probative value would justify the minimal time spent in making this report.

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

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

Therefore, the Commission proposes to direct the ERO to modify CIP-008-1 to require a responsible entity to contact appropriate government authorities and industry participants in the event of a Cyber Security Incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report. While the Commission leaves development of the details to NERC, the Commission agrees with APPA/LPPC that the reporting timeframe should run from the discovery of the incident by the responsible entity, and not the occurrence of the incident.

Full Operational Exercises and Lessons Learned

The CIP Assessment stated that the annual testing of the Incident Response Plan should require full operational exercises due to the potential for such exercises to uncover unforeseen complications.[57] In addition, it indicated that CIP-008-1 does not require documentation or reassessment of a plan's adequacy as a result of lessons learned from testing or in response to specific issues.

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

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

Several commenters noted that there may be a significant benefit in executing an operational exercise over a paper drill, but note that an operational exercise also can require expensive back-up systems and may unnecessarily risk damaging system functionality in case of an error or unforeseen system effect. Georgia System believes each responsible entity has to determine whether the incremental benefit from a yearly exercise is worth the costs and reliability risks associated with the exercise. MidAmerican stated it could support full operational exercises for a limited number of critical assets, with paper exercises for the remaining facilities. National Grid suggested that operational drills are more appropriate for

57 CIP Assessment at 37.

actual recovery plans under CIP-009-1, and paper drills are more than adequate to assess whether the response plans under CIP-008-1 identify and alert the right responders. Xcel Energy is concerned that operational drills (like vulnerability tests) could cause an inadvertent disruption to EMS and SCADA systems.

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

Commission Proposal

The Commission understands from commenters that annual testing may be costly and disruptive. Nonetheless, periodic operational drills are important because they may reveal weaknesses, vulnerabilities, and opportunity for improvement that a paper drill would not identify. The Commission agrees with the commenters that suggest that a full operational exercise should be performed at least once every three years, and that tabletop exercises are sufficient for the other two years. The Commission believes this strikes an appropriate balance between the benefits of executing an operational exercise and the associated costs and potential risks of misoperations. Therefore, the Commission proposes to direct the ERO to revise the Reliability Standard to require responsible entities to perform a "full operational exercise" at least once every three years, or to fully document its reason for not conducting an exercise in full operational mode pursuant to the technical feasibility parameters discussed earlier in section II.A.5.b. Further, the Commission proposes to direct the ERO to provide guidance on the meaning of the term "full operational exercise."

The Commission believes that industry will benefit from a requirement to document and implement lessons learned from testing or responses to actual cyber security incidents. Although NERC and ReliabilityFirst suggest that this is included in the "update" language of Requirement R1.4, we believe that the Reliability Standard would be improved by making a "lessons learned" requirement explicit. Therefore, the Commission proposes to direct that the ERO refine CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned. The Commission also proposes to direct the ERO to include language to require revisions to the Incident Response Plan to address these lessons learned.

Commission Proposal Summary

In summary, the Commission proposes to approve Reliability Standard CIP-008-1 as mandatory and enforceable. In addition, the Commission proposes to direct the ERO, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of the Commission's regulations to develop modifications to CIP-008-1 through its Reliability Standards development process that: (1) develop and include language regarding the term "reportable incident" that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form 417; (3) recognize that the term "reportable incident" should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced; (5) require a responsible entity to contact appropriate government authorities and industry participants in the event of a Cyber Security Incident as soon as possible, but at least within one hour of the event, even if it is a preliminary report; (6) require responsible entities to perform a "full operational exercise" at least once every three years, or to fully document its reason for not conducting an exercise in full operational mode pursuant to the technical feasibility parameters discussed earlier herein and provide guidance on the meaning of the term "full operational exercise;" (7) refine Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned; and (8) require revisions to the Incident Response Plan to address the lessons learned.

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 developed its estimate of burden based upon the CIP Reliability Standards as proposed by NERC. The CIP Reliability Standards include only one actual reporting requirement. Specifically, CIP-008-1 requires responsible entities to report cyber security incidents to ESISAC. In addition, the eight CIP Reliability Standards require responsible entities to develop various policies, plans, programs and procedures. For example, each responsible entity must develop and document a risk-based assessment methodology to identify critical assets, which is then used to develop a list of critical cyber assets (CIP-002-1). A responsible entity that identifies any critical cyber assets must also document: a cyber security policy (CIP-003-1); a security awareness program (CIP-004-1, Requirement R1); a personnel risk assessment program (CIP-004-1, Requirement R3); an electronic security perimeter and processes for control of electronic access to all electronic access points to the perimeter (CIP-005-1, Requirements R1 and R2); a physical security plan (CIP-006-1); procedures for securing certain cyber assets (CIP-007-1); and recovery plans for critical cyber assets (CIP-008-1). The above is not an exhaustive list and, in addition, the CIP Reliability Standards require responsible entities to maintain various lists and access logs.

The CIP Reliability Standards do not require a responsible entity to report to the Commission, ERO or Regional Entities the various policies, plans, programs and procedures. However, the documentation of the policies, plans, programs and procedures must be available to demonstrate compliance with the CIP Reliability Standards. The Commission has included the cost of developing the required documentation for the required policies, plans, programs and procedures in its burden estimate. The Commission, however, did not include in its burden estimate the cost of substantive compliance with the CIP Reliability Standards, separate from the requirements to develop specific documentation.

In formulating its estimate of the reporting burden, the Commission has been guided by several factors.

Number of Entities: As of April 2007, NERC identified 1,266 registered entities in the United States. The Applicability section of each CIP Reliability Standard specifies nine categories of users, owners and operators of the Bulk-Power System (as well as NERC and the Regional Entities) that must comply with the CIP Reliability Standards. The nine categories of users, owners and operators are based on the categories of functions identified in the NERC Functional Model. Based on a review of NERC's registration list, the Commission estimates that approximately 1,000 entities will be required to comply with the CIP Reliability Standards.
Variations in Compliance Burden: The Commission's estimate is based on all 1,000 entities

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

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

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

Further, many entities, including those that did not comply with UA-1200, typically have followed certain practices specified in the CIP Reliability Standards. The Commission believes that practices such as conducting cyber security training, having procedures for whom to contact in case of a cyber security incident, and developing a plan for how to restore a computerized control system should it fail are usual and customary practices in the electric industry and others. The Commission has taken such customary practices into account when estimating the reporting burden.

Time Period: The CIP Reliability Standards were approved by the NERC board in May 2006, with a designated effective date of June 1, 2006.[58] The proposed implementation schedule submitted with the CIP Reliability Standards plans for responsible entities to be "auditably compliant" with most requirements by mid-2010 or later. Mid-2010 is four years after CIP Reliability Standards went into effect. Therefore, the Commission developed an annual burden estimate by dividing total costs by 4 years.

Data Collection	Number of Respondents	Number of Responses	Hours Per Response	Total Annual Hours

58 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.

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 seeks comments on the costs to comply with these requirements. It has projected the costs to be:

Large investor-owned utility = 322,400 hours@$88 = $ 28,371,200
Others, including munis and coops = 795,000 hours@$88 = $69,960,000
Entities that have not identified critical cyber assets = 8,000 hours@$88 = $704,000
Because auditably compliant status is not required for many requirements until mid-2010, the Commission has projected the costs over a four-year period. On an annual basis the costs will be ($28,371,200 + $69,960,000 + $704,000)/ 4 years = $24,758,800 per year.
The hourly rate of $88 is a composite figure of the average cost of legal services ($200 per hour), technical employees ($39.99 per hour) and administrative support ($25 per hour), based on hourly rates from the Bureau of Labor Statistics (BLS). Using the May 2006 OES Industry-Specific Occupational Employment and Wage Estimates, the median hourly rate wage estimate for a computer software engineer is $39.99.[59]

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

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

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 3.0 FTE's will review the Reliability standards at the Commission or a total cost of 3.0 x $122,137 = $427,480.[60]

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 NOPR are needed to protect the electric industry's Bulk-Power System against malicious cyber attacks that could threaten the reliability of the Bulk-Power System

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 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.

17. DISPLAY OF THE EXPIRATION DATE

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

60 An FTE = Full Time Employee. The $122,137 "cost" consists of approximately $98,876 in salaries and benefits and $23,261 in overhead. The Cost estimate is based on the estimated annual allocated cost per Commission employee for Fiscal Year 2007.

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.