

UNITED STATES OF AMERICA  
BEFORE THE  
FEDERAL ENERGY REGULATORY COMMISSION

Mandatory Reliability Standards for Critical ) Docket No. RM06-22-000  
Infrastructure Protection )

NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION  
COMMENTS ON THE COMMISSION STAFF PRELIMINARY ASSESSMENT

Pursuant to the Notice of Comment Period (“Notice”) that the Federal Energy Regulatory Commission (“Commission” or “FERC”) issued in the above-captioned proceeding on December 11, 2006, the National Rural Electric Cooperative Association (“NRECA”) submits these comments on the Commission Staff Preliminary Assessment (“Preliminary Assessment”), also issued on December 11, 2006, of eight Reliability Standards (“Proposed Standards”) proposed by the North American Electric Reliability Council (“NERC”) concerning Critical Infrastructure Protection (“CIP”).

The Notice states that the Commission intends to issue a subsequent Notice of Proposed Rulemaking (“NOPR”) on each Proposed Standard. Since this is a Preliminary Assessment and there will be a further opportunity for comment guided by a NOPR, NRECA is using these comments to address general matters raised by the Preliminary Assessment, rather than to provide a detailed treatment of the individual Proposed Standards.

I. NRECA’S INTEREST IN RELIABILITY MATTERS

NRECA is the not-for-profit national service organization representing approximately 930 not-for-profit, member-owned rural electric cooperatives. NRECA’s members encompass both (a) distribution cooperatives that operate primarily at retail over lower-voltage distribution systems and provide retail electric service to over 40 million consumer-owners in 47 states, and (b) 65 generation and transmission (“G&T”) cooperatives that supply wholesale power to their

distribution cooperative owner-members and/or operate higher-voltage transmission systems. Many G&T cooperatives are already subject to NERC's current (pre-ERO) reliability standards (the "Current Standards") and are active participants in NERC. The distribution cooperatives generally are not. This distinction is fact-based and fully consistent with Congress's directive in 16 U.S.C. § 215(a)(1) of the Federal Power Act that the "bulk-power system ... does not include facilities used in the local distribution of electricity," such as the facilities owned and operated by most distribution cooperatives.

All cooperatives depend on the reliable operation of the bulk-power system and stand to experience substantial harm should that system fail. NRECA and its members thus have a vital interest in the reliable operation of the bulk-power system and the adoption and implementation of sound rules and procedures for ensuring its continued reliable operation. At the same time, NRECA and its members recognize that reliability comes at a cost and that reliability must be balanced with other important objectives.

NRECA submits that: (A) the CIP Proposed Standards should focus not on "large" and "small" entities, but instead on the entities that own and/or operate critical assets, and those are the entities to which the standards should apply; (B) the NERC Glossary properly defines critical assets and critical cyber assets, and while greater transparency and consistency across regions in the identification of such assets is desirable, legitimate regional difference do exist and should be permitted; (C) business judgment should apply to how an entity implements a standard, but not to whether the entity is subject to the standard; (D) the implementation timetable is appropriate given the extensive protection systems required by the standards, although NERC should consider annual progress audits; and (E) the scope of the standards should not be expanded to

apply to additional functions under NERC's Functional Model without first being considered and determined to be necessary in the NERC standards development process.

## II. COMMENTS ON THE PRELIMINARY ASSESSMENT

NRECA believes that the Preliminary Assessment is in general a useful document. In particular, NRECA agrees with the statement at page 6 of the Preliminary Assessment that the Proposed Standards "represent the most thorough attempt to-date to address cyber security issues for the Bulk-Power System." NRECA believes that the Proposed Standards will make a major contribution to enhanced reliability, and NRECA supports the approval of the standards.

Since the Notice indicates that the Commission intends to issue a NOPR for the Proposed Standards, and since under the applicable statute, 16 U.S.C. § 215, reliability standards are to be developed at the ERO and not the Commission, NRECA is limiting its comments to five general matters at this time: (A) the interaction of large and small entities from a cyber security perspective and inclusion of small entities for cyber security purposes; (B) the identification of critical assets and critical cyber assets; (C) the "business judgment" language in the Proposed Standards; (D) the implementation timetable; and (E) the expansion of the scope of the standards to apply to new functions under NERC's Functional Model. Each of these matters is discussed in turn below.

### A. Interaction of Large and Small Entities from a Cyber Security Perspective and Inclusion of Small Entities for Cyber Security Purposes

NRECA does not believe that it is particularly useful to address this issue in terms of "large" versus "small" entities. NRECA believes that the issue should instead be framed by identifying those entities that own and/or operate critical assets and the associated critical cyber assets as defined in the NERC glossary. The cyber security standards and requirements should

then apply to the entities that are identified as owning and operating those assets. The most logical, effective, and efficient place to “dig the cyber moat” is around those critical cyber assets. Requiring further levels of cyber security measures by the myriad other entities that interact on a read or report-only level with these cyber assets will not add appreciably to the level of security, but will impose substantial costs on those other entities, many of which are subject to protection under the Regulatory Flexibility Act.

It should be the responsibility of the entity that owns and operates the critical cyber assets to protect those assets against outside intrusion. To give one example, banks do not require customers who employ electronic banking to install firewalls or security measures on their personal computers due to the associated cost and customer resistance. Rather, the banks themselves take on the responsibility to protect their systems. The same is true of other networks such as airlines, railroads, and even the internet itself. Such asset owners/operators, however, should be allowed to impose reasonable limitations on users of their systems to support their security measures.

NERC and the Commission should not impose requirements on entities that neither own nor operate the critical cyber assets. (For the same reason, it is inappropriate to expand CIP-0020-1 to apply to assets that are beyond the control of the Responsible Entities.) Placing responsibility on the entities that control the assets will promote accountability and simplify compliance. Much of the actual work in this area will, of necessity, be performed by software and hardware developers, and their efforts will be facilitated if they are directly responsible to a smaller number of entities that are best equipped to develop the specifications for these matters and monitor their implementation.

## B. Identification of Critical Assets and Critical Cyber Assets

NRECA agrees with the definitions of critical assets and critical cyber assets set out in the NERC Glossary. NRECA also recognizes that the Regional Entities have a substantial role to play in designating critical assets. While NRECA supports greater transparency and consistency across regions in the identification of critical assets, legitimate regional differences do affect the designation of critical assets and should thus be permitted.

## C. "Business Judgment" Language in the Standards

NRECA believes that business judgment is an entirely legitimate consideration in determining how to best and most efficiently meet a cyber security standard requirement. In particular, not all assets pose the same risks, the risks associated with a particular asset may vary from one entity to another, the benefits and costs of particular approaches to protection will vary by entity and situation, and thus a "one size fits all approach" is likely to increase costs without maximizing protection. Moreover, allowing entities to develop and implement different approaches will enable "best practices" to emerge and evolve. Business judgment, however, should not be employed to decide whether or not to comply with a standard in a first instance.

Accordingly, the CIP Proposed Standards, including those that reference business judgment, should be approved, so that cyber security standards will be in place in a timely fashion.

## D. Implementation Timetable

NRECA appreciates that the implementation timetable may seem somewhat lengthy and that the Commission might have concerns in this regard. At the same time, the Commission should appreciate that NRECA's affected members, and no doubt many others, will be under

substantial pressure to implement the extensive protection systems that the standards require within the stated time frames.

NRECA does believe that it would be appropriate for the Regional Entities to require the entities that are subject to the standards to show they are making adequate progress towards implementation. One possibility to be considered (in the first instance by NERC and the Regional Entities, as opposed to the Commission) is to have the Regional Entities conduct annual interim compliance audits to verify that affected entities are on the path to compliance as described in the NERC cyber security standards implementation plan.

#### E. Expansion of Standards to Additional Functions under NERC's Functional Model

NRECA opposes the suggestion in the Preliminary Assessment that the Commission expand the scope of the cyber security standards to apply to additional classes of functions under the NERC Functional Model. As explained above, any such expansion would impose costs without commensurate or even appreciable benefits, as well as pose complications in terms of compliance with the Regulatory Flexibility Act. Furthermore, any such proposal should first be fully considered through NERC's standards development process and not mandated by the Commission.

## V. CONCLUSION

For the reasons explained in the foregoing comments, NRECA supports the Proposed Standards and urges the Commission to approve them.

NRECA expects to have further comments in response to the NOPR that the Commission states that it intends to issue in the future.

Respectfully submitted,

NATIONAL RURAL ELECTRIC COOPERATIVE  
ASSOCIATION

**/s/ Wallace F. Tillman**

Wallace F. Tillman  
Vice President, Energy Policy and General Counsel  
Richard Meyer  
Senior Regulatory Counsel  
David L. Mohre  
Executive Director - Energy and Power Division  
Barry R. Lawson  
Manager, Power Delivery  
National Rural Electric Cooperative Association  
4301 Wilson Blvd.  
Arlington, VA 22203  
(703) 907-5811  
Fax: (703) 907-5517  
E-mail: [richard.meyer@nreca.coop](mailto:richard.meyer@nreca.coop)

**/s/ Robert D. Rosenberg**

Robert D. Rosenberg  
Slover & Loftus  
1224 Seventeenth Street, N.W.  
Washington, D.C. 20036  
(202) 347-7170  
(202) 347-3619 (fax)  
E-mail: [rdr@sloverandloftus.com](mailto:rdr@sloverandloftus.com)

Counsel for National Rural Electric Cooperative  
Association

Dated: February 12, 2007

Submission Contents

NRECA Comments on Staff Preliminary Assessment  
rdr2538.pdf..... 1-7