

**UNITED STATES OF AMERICA  
BEFORE THE  
FEDERAL ENERGY REGULATORY COMMISSION**

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

**COMMENTS OF  
THE AMERICAN PUBLIC POWER ASSOCIATION AND  
THE LARGE PUBLIC POWER COUNCIL  
ON NOTICE OF PROPOSED RULEMAKING**

The American Public Power Association (“APPA”) and the Large Public Power Council (“LPPC”)<sup>1</sup> (hereinafter referred to as “APPA/LPPC”) hereby submit their comments on the Notice of Proposed Rulemaking (“NOPR”) on Mandatory Reliability Standards for Critical Infrastructure Protection, issued by the Federal Energy Regulatory Commission (“FERC” or the “Commission”) on July 20, 2007 and published in the Federal Register<sup>2</sup> on August 6, 2007.

**I. INTRODUCTION AND EXECUTIVE SUMMARY**

**A. Introduction**

APPA is the national service organization representing the interests of not-for-profit, publicly owned electric utilities throughout the United States. More than 2,000 public power systems provide over 15 percent of all kilowatt-hour (“kWh”) sales to ultimate customers, and do business in every state except Hawaii. Public power systems own almost 10 percent of the nation’s electric generating capacity, but purchase nearly 70 percent of the power used to serve their ultimate consumers. All APPA utility members are Load-Serving Entities (“LSEs”), with

---

<sup>1</sup> LPPC’s members are Austin Energy, Chelan County Public Utility District No. 1, Clark Public Utilities, Colorado Springs Utilities, CPS Energy (San Antonio), IID Energy (Imperial Irrigation District), JEA (Jacksonville, FL), Long Island Power Authority, Los Angeles Department of Water and Power, Lower Colorado River Authority, MEAG Power, Massachusetts Municipal Wholesale Electric Company, Nebraska Public Power District, New York Power Authority, Omaha Public Power District, Orlando Utilities Commission, Platte River Power Authority, Puerto Rico Electric Power Authority, Sacramento Municipal Utility District, Salt River Project, Santee Cooper, Seattle City Light, Snohomish County Public Utility District No. 1, and Tacoma Public Utilities.

<sup>2</sup> 72 Fed. Reg. 43,970 (August 6, 2007)

the primary goal of providing customers in the communities they serve with reliable electric power and energy at the lowest reasonable cost, consistent with good environmental stewardship. Approximately 325 APPA members are currently shown on NERC's compliance registry, and thus are responsible for compliance with applicable North American Electric Reliability Corporation ("NERC") NERC reliability standards.

LPPC is a trade association representing 24 of the nation's largest municipal electric systems. LPPC members are also members of APPA, representing the larger, asset owning segment of the APPA community. LPPC members provide reliable, low-cost electric service to most of the more than 40 million people served by public power. Together, LPPC members own and operate over 61,500 MW of generation and approximately 33,000 circuit miles of transmission line. LPPC members are governed by state and local laws that require reliable service be provided to their native load customers at least cost. As the owners and operators of electric systems around the country, APPA/LPPC members have an avid interest in maintaining and improving the reliability of the Bulk-Power System.

APPA/LPPC-member operations include planning of the Bulk-Power System, maintaining system facilities, and real-time system operation. APPA/LPPC members have long been involved in the development of NERC reliability standards and have played an active role in the Commission's process for approving mandatory reliability standards following passage of the Energy Policy Act of 2005. LPPC participated actively in the development of, and filed comments upon, the standards approved by the Commission in Docket No. RM06-16, and filed comments jointly with the APPA on the Staff Assessment issued in this docket on December 11, 2006.

## **B. Executive Summary**

The Commission proposes to direct NERC to develop standards that are in certain respects more prescriptive than those proposed by NERC and supported by APPA/LPPC. In most respects, APPA/LPPC support the Commission's approach, and appreciate the extent to which the Commission recognizes the importance of flexibility and discretion in crafting these Critical Infrastructure Protection ("CIP") Standards. APPA/LPPC emphasize that this is a new area for NERC, and that the operating circumstances between Responsible Entities with respect to cyber assets vary considerably.

However, there are subject matter areas in which APPC/LPPC recommend that the Commission rethink its proposed approach. Comments on specific standards offered below are summarized as follows:

- **Implementation Plan:** Although APPA/LPPC generally support NERC's proposed implementation plan, it must be modified to accommodate instances in which lists of critical assets prepared by Responsible Entities are revised under the Commission's proposal.
- **Business Judgment Rule:** APPA/LPPC agree with the Commission that NERC's proposed standards should have been revised to eliminate reference to the "business judgment rule," as that term is understood in the law relating to corporate governance. However, it is still appropriate for the revised standards to invest Responsible Entities with a degree of discretion.
- **Technical Feasibility:** APPA/LPPC support NERC's view that the Commission should permit the development of standards which would enable Responsible Entities to take advantage of the useful life of equipment that is not readily retrofitted to accommodate

all cyber-security measures. Where exceptions for “technical feasibility” are sought, enforcement should not commence until some reasonable time after disposition of the request.

- **Acceptance of Risk:** The Commission should permit the standards to incorporate limited license for Responsible Entities to refrain from implementing cyber security measures where they demonstrate that compliance would engender a greater threat to Bulk-Power System reliability.
- **Risk-Based Assessment Methodology:** The Commission must permit Responsible Entities to exercise a reasonable degree of discretion in establishing their methodologies for identifying critical assets.
- **Oversight of Critical Assets:** The Commission must provide for an appellate process enabling Responsible Entities to challenge decisions revising their designations of critical assets.
- **Security Management Controls:** The Commission should refrain from mandating that Responsible Entities take responsibility for the cyber-security public communications carriers they employ in providing service.
- **Electronic Security Perimeter** Alternatives to standard Electronic Security Perimeters should be permitted where approved by Regional Entities upon submission of a documented request for waiver.
- **Security Patch Management:** Responsible Entities must be invested with the discretion to determine whether Bulk-Power System reliability may be more threatened through implementation of a software security patch than operating with older versions of the software.

- **Regulatory Flexibility Act and Effects on Small Entities.** The Regulatory Flexibility Act of 1980 requires the Commission to include either an initial regulatory flexibility analysis in its NOPR or certify that the proposed rule will not have a “significant impact on a substantial number of small entities.” PP 340-341. APPA/LPPC agree with the Commission that NERC’s compliance registry goes a long way toward mitigating the economic impact of the proposed rules on small entities. P 343. Application of the NERC Statement of Compliance Registry Criteria has reduced the total number of public power utilities potentially subject to NERC’s Reliability Standards from nearly 2,000 to approximately 326 discrete public power utilities. While APPA/LPPC must disagree with the Commission’s categorical statement at P 344 that “the CIP Reliability Standards will not have a significant economic impact on a substantial number of small entities,” APPA/LPPC can support Commission approval of the proposed rule as it is now proposed, subject to the changes discussed in these comments.

## **II. Comments**

### **A. General Issues**

#### **1. Implementation Plan (PP 42-49)**

APPA/LPPC support the Commission’s proposal (P 47) to approve NERC’s Implementation Plan, including the proposed timeline for achieving compliance. APPA/LPPC particularly appreciate the Commission’s recognition that audits holding potential penalties should not take place prior to NERC’s proposed schedule for ascertaining when entities will be “auditably compliant,” and agree that NERC’s proposed self-certification process is a reasonable means of tracking the progress made by responsible entities toward full, auditable compliance.

Further, APPA/LPPC have no objection to the Commission’s proposal that such certification be rendered quarterly or semi-annually.

However, APPA/LPPC asks for clarification of the Implementation Plan as it bears on the Commission’s proposal (P 113) that regional oversight be exercised over the designation of critical assets by Responsible Entities. At PP 109 – 116, the Commission directs NERC to propose revised standards providing that either Regional Entities or some other region-wide institutions take responsibility for reviewing the list of Critical Assets prepared by Responsible Entities. That process contemplates that a Responsible Entity’s list of Critical Assets may be supplemented. Where that occurs, APPA/LPPC strongly suggests that an adjustment be made to the compliance timeline for being auditably compliant with respect to newly designated assets. APPA/LPPC ask the Commission to direct NERC to develop a reasonable schedule for determining when procedures regarding such assets should be auditably compliant.

## **2. Issues Presented by Terminology**

### **a. Business Judgment (PP 50-67)**

APPA/LPPC agree with the Commission that NERC’s proposed incorporation of the “reasonable business judgment rule” into CIP-002-1 and each of the specific CIP standards overstated the amount of discretion appropriately invested in Responsible Entities, to the extent that term was intended to incorporate a body of case law developed in the context of accountability for corporate governance. APPA/LPPC made their own position on this issue clear in the APPA/LPPC Comments on the Staff Assessment.<sup>3</sup>

However, APPA/LPPC also believe that the Commission should have directed NERC to substitute for the term “reasonable business judgment” another phrase intended to confer a level

---

<sup>3</sup> pp. 8 – 11.

of reasonable discretion in the implementation of the standards. The Commission agreed that the CIP standards should invest a substantial level of discretion in Responsible Entities, stating:

The Commission agrees that flexibility and discretion are essential in implementing the CIP Reliability Standards and that implementing those Reliability Standards must be done on the basis of the specific facts and circumstances applicable in the individual case at hand. Cyber security problems do not lend themselves to one-size-fits-all solutions. In addition, the Commission acknowledges that cost can be a valid consideration in implementing the CIP Reliability Standards.<sup>4</sup>

APPA/LPPC believe that the standards should expressly reflect this approach, and therefore renew the suggestion initially made in the APPA/LPPC comments on the Staff Assessment that the standards be revised expressly to provide that Responsible Entities may exercise a degree of discretion in their implementation. APPA/LPPC also renew the suggestion that the phrases “reasonable judgment,” or “judgment consistent with Good Utility Practice” may be employed for this purpose, since these terms do not carry the legal baggage to which the Commission reasonably objected in connection with the reasonable business judgment rule. In any event, the precise articulation of this concept may be left to the NERC standards development process.

This Commission has already defined the term “Good Utility Practice,” in section 1 of FERC’s Standard Large Generator Interconnection Procedures (“LGIP”). Section 1 of the Standard LGIP defines Good Utility Practice to mean:

Any of the practices, methods and acts engaged in or approved by a significant portion of the electric industry during the relevant time period, or any of the practices, methods and acts which, in the exercise of reasonable judgment in light of the facts known at the time the decision was made, could have been expected to accomplish the desired result at a reasonable cost consistent with good business practices, reliability, safety and expedition. Good Utility Practice is not intended to be limited to the optimum

---

<sup>4</sup> NOPR at P 59.

practice, method, or act to the exclusion of all others, but rather to be acceptable practices, methods, or acts generally accepted in the region.<sup>5</sup>

APPA/LPPC believe this definition is workable, but we are not wedded to it, and offer it as illustrative of an approach NERC may take on reconsideration in the standards development process. This already-accepted definitional concept seems particularly well-suited to the implementation of Cyber-Security standards, where the Commission has already agreed that a meaningful level of discretion is appropriate.

**b. Technical Feasibility and Acceptance of Risk (PP 68-86)**

**i. Technical Feasibility**

Although recognizing that certain of the CIP standards are appropriately subject to exception where compliance is not “technically feasible,” the Commission proposes at P 79 to require that the ERO develop standards ensuring that Responsible Entities relying on exceptions for lack of technical feasibility (1) develop and implement interim mitigation steps to address the vulnerabilities associated with each exception; (2) develop and implement a remediation plan to eliminate the exception, including interim milestones and a reasonable completion date; and (3) obtain written approval of these steps by the senior management assigned with overall responsibility for implementation and adherence to the CIP Reliability Standards. In addition, the Commission proposes to require a Responsible Entity to report and justify to the ERO or the Regional Entity for approval each exception and its expected duration.

---

<sup>5</sup> See Standardization of Generator Interconnection Agreement and Procedures, Order No. 2003, 68 Fed. Reg. 49,845, Appendix C at 4 (August 19, 2003), FERC Stats. and Regs., Regulations Preambles 2001-2005 ¶31,146 (2003), order on reh'g, Order No. 2003-A, 69 Fed. Reg. 15,932 (March 26, 2004), FERC Stats. and Regs., Regulations Preambles 2001-2005 ¶31,160 (2004), order on reh'g, Order No. 2003-B, 70 Fed. Reg. 265 (January 4, 2005), FERC Stats. and Regs., Regulations Preambles 2001-2005 ¶31,171 (2004), order on reh'g, Order No. 2003-C, 70 Fed. Reg. 37,661 (June 30, 2005), FERC Stats. and Regs., Regulations Preambles 2001-2005 ¶31,190 (2005); see also Notice Clarifying Compliance Procedures, 106 FERC ¶61,009 (2004).

In comments to be submitted contemporaneously, it is APPA/LPPC's understanding that NERC will point out that the technical feasibility exception in the proposed standards was initially included in recognition of the fact that older equipment in substations and generating plants can be incompatible with certain cyber security measures, including software updates and patches, although the underlying equipment is an important part of a reliable electrical network. NERC suggests that in the drafting process following issuance of the NOPR, NERC should have the flexibility to revise the standards in order to address this situation. For the reasons NERC suggests, APPA/LPPC believe that being able to take advantage of the useful life of existing equipment has value from a reliability standpoint that the standards should appropriately recognize.

APPA/LPPC add that whether a request for implementation of a technical feasibility exception is requested on an interim or permanent basis, the Commission should clarify that where a Regional Entity or the ERO ultimately rejects a request for approval of such an exception, the Responsible Entity may rely on the exception until it has been ruled upon, and a reasonable time within which to bring the organization into compliance has been provided. Without that clarification, utilities which in good faith believe that an exception is justified risk a finding that standards have been violated while waiting for an official determination. The inequities of such a framework seem self-evident.

## **ii. Acceptance of Risk**

At P 86, the Commission proposes to direct NERC to remove the "acceptance of risk" language from the CIP Reliability Standards, expressing concern that the phrase would permit Responsible Entities to ignore otherwise applicable standards, thereby jeopardizing the critical assets of others and creating a significant and unknown risk to Bulk-Power System reliability.

APPA/LPPC agree that it would be unwise to permit Responsible Entities to ignore reliability standards simply on the ground that they believe the risk of doing so is acceptable to them. However, in the limited instances in which the “acceptance of risk” language appears, APPA/LPPC believe that the inartfully articulated intent was to provide Responsible Entities a degree of discretion where compliance with the standard is perceived to pose a greater risk to Critical Asset availability (and thus ultimately to the Bulk-Power System) than non-compliance. The “acceptance of risk” language appears only in the context of CIP-007-1 (Cyber Security-System Management) in connection with (1): R2.3 Ports and Service; (2) R3.2, Security Patch and (3) R4.1, Malicious Software Prevention. In each instance, APPA/LPPC members can envision situations in which it is reasonable to conclude that compliance poses a significant risk. With respect particularly to R3.2 (security patch management), the input APPA/LPPC have received from individuals involved in software management is that inadequately tested patches pose a risk of system failure with some frequency. Thus, every entity must weigh the risk of using software with a known flaw against the risk that the vendor’s patch will introduce even Greater risk. In such limited cases it may be appropriate for an entity to accept the risk of not complying with the standard (i.e., the entity would reasonably conclude that compliance would pose a greater risk to Bulk-Power System reliability than non-compliance).

Acceptance of risk must be justified in terms of the risk of both courses of action to the reliable operations of the Bulk Power System (BPS), not just to the Responsible Entity. For example, a software patch may prevent external intrusion through a firewall, but also result in computer system failures due to interactions with other systems operated by the responsible entity. A reboot and restoration of corrupted data used in energy accounting software would be

disruptive to the entity and its customers, but would not pose a risk to BPS reliability.

Conversely, a loss of communications with reliability coordinators poses a severe risk.

Where such a judgment is made, APPA/LPPC believe that Responsible Entities must report the exercise of discretion to Regional Entities for approval, as the Commission proposes with respect to exceptions for lack of technical feasibility. Further, as recommended above for such exceptions, APPA/LPPC propose that Responsible Entities should be permitted to operate consistent with their self-certification, pending any contrary determination by the ERO or Regional Entity and a reasonable opportunity to comply with any ensuing directive.

## **B. Discussion of Each CIP Reliability Standard**

### **1. CIP-002-1-Critical Cyber Asset Identification**

#### **a. Risk-Based Assessment Methodology (PP 93-105)**

Although in initial comments, APPA/LPPC opposed Staff's recommendation for more prescriptive provisions applicable to the CIP-001-1, R1 (Critical Asset Identification Method),<sup>6</sup> APPA/LPPC do not here object to the Commission's proposal at P 103 to require NERC to "provide some basic guidance on the content or considerations to be applied in a risk assessment methodology." APPA/LPPC do pause to underscore the Commission's recognition, however (P 101), of "the need for flexibility in the risk assessment process to take into account the individual circumstances of a responsible entity." To provide substance to that approach, APPA/LPPC urge the Commission to permit NERC to include in its redraft of the proposed standard express reference to a utility's ability to exercise reasonable judgment in the specification of its risk-based assessment. Consistent with the comments above on the "Reasonable Business Judgment Rule," APPA/LPPC believe that a revised standard that requires responsible entities to exercise

---

<sup>6</sup> APPA/LPPC Joint Comments on Staff Assessment, pp. 18 – 202

and to demonstrate that they have exercised either “reasonable judgment” or “discretion consistent with good utility practice” would be appropriate.

**b. Internal Approval of Risk Assessment (PP 106-108)**

Consistent with their comments filed in response to the Staff Assessment, APPA/LPPC support the requirement at P 108 of the NOPR that a Responsible Entity’s senior managers annually review and approve the risk-based assessment methodology.

**c. Oversight of Critical Assets Identification (PP 109-115)**

APPA/LPPC agree with the Commission’s determination at P 111 of the NOPR that the primary responsibility for the identification of critical assets lies with the Responsible Entity. APPA/LPPC understand, however, the Commission’s interest in proposing to require oversight of the list of identified critical assets prepared by Responsible Entities. Having said that, APPA/LPPC do believe the Commission must take care to ensure that sufficient due process is provided enabling Responsible Entities to challenge decisions regarding their lists of critical assets. To provide appropriate due process, the Commission should specifically direct NERC to develop written procedures for Responsible Entities seeking to challenge decisions made by Regional Entities altering a Responsible Entity’s list of critical assets. Although APPA/LPPC take no position here on whether the entity reviewing the list of assets prepared by Responsible Entities is a Regional Entity, a Reliability Coordinator, a Transmission Operator, or a Balancing Authority, an appellate process is needed in all cases. Decisions by Regional Entities would logically be subject to an appellate process akin to what is described in Rule 410 of the NERC Rules of Procedure for appeals relating to a violation of a reliability standard or imposition of a penalty for violation of a reliability standard. Decisions by Reliability Coordinators, Transmission Operators, or Balancing Authorities may be appealed to the Commission. In any

case, if the Commission grants entities approval over Critical Assets lists, the Commission should commit to the development of such appellate procedures.

**d. Interdependency (PP 116-118)**

Consistent with their comments on the Staff Assessment, APPA/LPPC support the Commission's proposed determination at P 118 that the scope of reliability regulation is properly limited to assets critical to the Bulk-Power System, and does not extend to the management of assets that may be important to the operation of other (even if presumably critical) non-electric assets. The Commission simply lacks authority over non-electric assets, and has no particular role in their protection.

**2. CIP-003-1-Security Management Controls (PP 120-127)**

Reliability Standard CIP-003-1 seeks to ensure that each Responsible Entity has minimum security management controls in place to protect critical cyber assets identified pursuant to CIP-002-1. APPA/LPPC support FERC's determination that the nature and scope of each Responsible Entity's cyber security management policy should generally be committed to the Responsible Entity's discretion. APPA/LPPC also agree that security policies will address issues that are not currently reflected in the CIP Reliability Standards, but are important to the security of the control system.

In comments at P 126 expanding on its observation that security policies appropriately address issues not currently addressed in the CIP standards, the Commission notes that it "would expect a security policy for control systems to address the responsible entity's actions to protect communications networks." While APPA/LPPC understand the Commission's desire to ensure that communications networks are protected, the Commission should clarify that it does not contemplate that Responsible Entities will assume an obligation to ensure the security of commercial telecommunications systems routinely engaged by utilities in the conduct of their

business. It is reasonable to expect that Responsible Entities will shoulder responsibility for communications systems they own and operate, but this obligation cannot reasonably be extended to a commitment to oversee the operations of commercial communication carriers. The Commission should recognize that it has no direct authority to compel commercial communication carriers to comply with these proposed rules. Responsible entities cannot compel communications carriers to comply with NERC CIP standards as if they were jurisdictional entities. Promulgating a rule that would leave utilities with no recourse other than to construct and operate private communications networks may be prohibitively expensive. Moreover, the development of such business functions (even if not offered to third parties) by entities generally unfamiliar with these networks may very well increase the risk of cyber intrusions. Certainly, it is an open question whether smaller entities would be capable of performing these functions on a cost-effective basis. Accordingly, APPA/LPPC urge the Commission to clarify that pursuant to CIP-003-1 Responsible Entities are only responsible for the protection of communication networks owned by Responsible Entities.

### **3. CIP-004-1 Personnel and Training**

#### **a. Personnel Risk Assessment (PP 162-166)**

CIP-004-1, R3.1 provides in pertinent part that “[t]he Responsible Entity shall ensure that each assessment conducted include, at least,[a] seven-year criminal check” on employees with access to Critical Cyber Assets. While APPA/LPPC do not object to this requirement, NERC should be directed to clarify R3.1 to provide that Responsible Entities have discretion in reviewing the results of criminal background checks to determine whether any crime identified in the background check would disqualify an individual from obtaining access to Critical Cyber Assets. The Commission should clarify that after further investigation Responsible Entities have

the ability to make a determination on a case-by-case basis that a criminal record does not necessarily disqualify an employee from access to Critical Cyber Assets.

**b. Question of Joint Owned Facilities (PP 170-173)**

APPA/LPPC support the Commission’s proposal (P 173) to direct NERC to address the “joint use” concerns expressed by the APPA/LPPC when developing modifications to the Reliability Standards that the Commission may adopt in a final rule. As the Commission noted, APPA/LPPC are particularly concerned to clarify that utilities will not be called upon to block access to joint owners based on the belief that they are out of compliance with CIP-004-1R4. APPA/LPPC agree with the Commission’s preliminary view (*id.*) that “each entity...is responsible for only its compliance and may not attempt to block or limit another’s access on the basis of its perception that the other entity has not complied with CIP-004-1.”

**4. CIP-005-1 Electronic Security Perimeter(s)**

**a. Adequacy of Electronic Security Perimeter (PP 178-181)**

At P 181, the Commission proposes to direct the ERO to develop a requirement to implement a defensive security approach which would include two or more defensive measures to ensure a defense in depth posture. APPA/LPPC believe that CIP-005-1 is adequate as drafted by NERC, and provides the needed degree of flexibility to accommodate very diverse physical and electronic situations.

Moreover, it is not clear what the Commission intends by directing NERC to adopt a requirement for “two or more distinct security measures when constructing an electronic security perimeter.” If the Commission continues to require this, it should clarify whether or not the second security measure must be on par with the first security measure. As NERC points out in its comments, an inflexible rule calling for redundant electronic security in all cases poses some very practical problems in a variety of settings. APPA/LPPC believe that, given sufficient

flexibility by the Commission, these issues may be worked out in the standards development process. Alternatively, if the Commission remains wedded to a fixed requirement at this time, NERC's suggestion for a technical conference may help to vet the concerns that the requirement presents for Responsible Entities.

## **5. CIP-006-1 Physical Security of Critical Cyber Assets**

### **a. Physical Security Plan (PP 207-209)**

CIP-006-1, R1.1, provides that while Cyber Assets are generally to be protected by both an Electronic Security Perimeter and an identified Physical Security Perimeter, the Physical Security Perimeter requirement may be satisfied by "documented alternative measures" where a physical perimeter is infeasible. The Commission proposes to modify this provision (P 209) in order to provide that alternative measures are only interim, and must be subject to a mitigation plan, consistent with the manner in which exceptions for lack of technical feasibility are to be treated. APPA/LPPC believe that while it may be appropriate to consider certain alternatives to the general rule regarding physical security to be only interim, there may be good reason to allow use of alternative measures on a long-term basis. In fact, the configuration or layout of a specific cyber asset simply may not lend itself to a complete physical perimeter, and alternative means of protection (including electronic protections) may be entirely adequate, given the level of security risk posed by the asset and the nature of the alternative form of protection. So long as such means are documented and approved by Regional Entities, APPA/LPPC urge the Commission not to require "six wall" physical security perimeters in all instances.

### **b. Physical Access Controls and Monitoring Physical Access Controls (P 210-214)**

Compounding APPA/LPPC's concern over potentially needless and expensive redundancy, at P 214 the Commission proposes to direct the ERO to modify CIP-006-1, R2 and

R3, to require Responsible Entities to establish a minimum of two or more different security procedures when establishing a physical security perimeter around Critical Cyber Assets. Since R2 and R3 are already designed to be redundant (controlled access is backed up monitoring), the Commission's requirement for further redundancy would appear to require a total of four measures. If the Commission meant that Responsible Entities must implement four separate and distinct security measures to comply with R2 and R3 APPA/LPPC disagree with the Commission proposed change. APPA/LPPC recommend that the Commission adopt these requirements as proposed by NERC.

**6. CIP-007-1-System Security Management (Security Patch Management) (PP 235-239)**

The Commission's proposal to eliminate the "acceptance of risk" language from CIP-007-1 1, R3.2. is addressed at pps. 9-10 above. As this bears on security patch management, removal of the "acceptance of risk" language would appear to prevent Responsible Entities from exercising any discretion to determine not to implement a security patch on the ground that it posed more risk than justified. Restricting the use of the "acceptance of risk" language as suggested above (i.e., limiting its use to instances where adoption of a specific compliance measure is determined by the Responsible Entity to pose more risk than alternative compliance measures, subject to the concurrence of the Regional Entity), is appropriate, but eliminating all discretion in this area undermines necessary flexibility.

Alternatively, APPA/LPPC urge the Commission to require NERC to revise R3 of CIP-007-1 specifically to permit Responsible Entities to make the determination that specific security patches create more vulnerability to the Bulk Power System than they solve. The Commission itself suggests that this is appropriate (P 239), commenting that "using the most up-to-date

patches that deal specifically with security vulnerabilities is of the utmost importance, provided it does not degrade the system and the patch does not create more vulnerability than the problem it is intended to fix (emphasis added).” The Commission should require that this qualification be written into the standard if the “acceptance of risk” language is removed.

#### **7. CIP-009-1-Recovery Plans for Critical Cyber Assets Operational Exercises (PP 299-304)**

APPA/LPPC support the Commission’s proposal at P 303 calling for a full operational exercise every three years (unless an actual incident occurs), but permitting reliance on table-top exercises annually in other years. APPA/LPPC also agree with the Commission’s determination at P 304 that the term “full operational exercise” lacks clarity and that it is appropriate that NERC either define the term in its Glossary or provide more direction directly in the Reliability Standard as to the parameters of the term. APPA/LPPC strongly recommend against including within the ambit of a “full operational exercise” a live vulnerability test in which the susceptibility of the grid to malicious hacking would be tested. As the Commission itself notes at P 302, the benefits of operational exercises must be weighed against the technical feasibility and operational risks of such exercises. APPA/LPPC strongly believe that live vulnerability tests would pose operational risks that would outweigh any benefits such tests would produce.

#### **C. Violation Risk Factors**

While APPA and the LPPC members are certainly committed to complying with all of the CIP standards APPA/LPPC believe that the Commission’s proposal to elevate CIP-002-1 R2 from low to high and R3 from medium to high should be reexamined. At P 327 the Commission justifies its proposal to elevate R2 from low to high based on the fact that “overlooked” assets could result in Bulk-Power System failure. Yet, given the oversight process now contemplated by Regional Entities over asset designation, and the overwhelming incentive Responsible

Entities have to proceed cautiously, it is difficult to see a substantial potential for assets to be overlooked. In light of the oversight process proposed in the NOPR APPA/LPPC request that the Commission accept the risk factors that NERC had initially assigned to CIP-002-1 R2 and R3.

#### **D. Regulatory Flexibility Act and Effects on Small Entities**

The Regulatory Flexibility Act of 1980 (RFA) requires the Commission to include either an initial regulatory flexibility analysis in its NOPR or to certify that the proposed rule will not have a “significant impact on a substantial number of small entities.” PP 340-341. APPA/ LPPC certainly agree that NERC’s compliance registry goes a long way toward mitigating the economic impact of the proposed rules on small entities. P 343. Application of the NERC Statement of Compliance Registry Criteria has reduced the total number of public power utilities potentially subject to NERC’s Reliability Standards from nearly 2,000 to approximately 326 discrete public power utilities. Nonetheless, APPA/ LPPC must disagree with the Commission’s categorical statement at P 344 that “the CIP Reliability Standards will not have a significant economic impact on a substantial number of small entities.”

Approximately 293 of the 326 public power systems included on the NERC compliance registry meet the Small Business Administration definition of a small electric utility.<sup>7</sup> It thus seems beyond dispute that the proposed regulations will have an impact on a substantial number of small entities; the question at hand is how significant that impact will in fact be. APPA/LPPC believe that some of these small entities will incur significant economic costs to comply with the

---

<sup>7</sup> According to the Commission, the Small Business Administration defines a small electric utility as one that has a total electric output of less than four million MWh in the preceding year. P 340. The APPA/LPPC estimate is based on a comparison of public power systems listed on the NERC compliance registry as of September 2007 with Energy Information Administration Form 861 data for 2005 MWh sales to ultimate customers and sales for resale. The Commission estimates that “the CIP Reliability Standards will apply to approximately 632 small entities, consisting of 12 small investor-owned utilities and 620 small municipals and cooperatives.” P. 343

CIP Reliability Standards. For example, many small distribution utilities with fewer than 50 employees may nonetheless own and operate 20 MVA generators. Many of these generators were constructed prior to the industry's adoption of a modern information technology infrastructure. A rigid implementation of the "technical feasibility" exception discussed above may lead to directives to adopt remediation plans that bring these units up to current industry standards. However, the costs required to retrofit such facilities to meet new cyber-security requirements may well force the owners to retire many of these units instead.

Despite these reservations, APPA/ LPPC believe that the broad contour of the rule contemplated by the NOPR, *subject to the changes discussed above*, satisfies the requirements of the RFA. APPA/LPPC recognize that CIP Reliability Standards are necessary to ensure the reliable operation of the Bulk-Power System. While NERC's proposed standards will place the burden on many small entities to identify critical assets and critical cyber assets, this approach is far superior to a top-down approach to asset classification. Assuming small entities do have critical assets and critical cyber assets, they will have to take on significant burdens and incur significant costs to protect their critical cyber assets. However, NERC's proposed timeline for the Implementation Plan appears feasible. Moreover, as noted by the Commission at P 348, joint action agencies and other similar organizations may form Joint Registration Organizations that accept compliance responsibilities for their members or provide compliance services to their members.

APPA/LPPC strongly urge the Commission to remain mindful of the RFA as it considers modifications to the proposed rule. APPA/LPPC also request that the Commission direct NERC and its Regional Entities make a special effort to provide technical guidance and assistance to small entities aimed at ensuring they reach auditable compliance on a timely basis.

