

**System Security
SMD NOPR
Comment Excerpts**

ABB

**I. Security Standards for Electric Market Participants
(Appendix G)**

We commend the Commission for setting out basic security requirements for the electricity grid's physical components and the operation of the system and the market. Based on our experience with the design and implementation of software systems for retail, wholesale and central markets, we offer the following comments.

Access Control. In addition to the most basic access control measures, the enterprise must also maintain a catalogue of sensitive data and a database of the users that have access to what data and the level of such access. To increase the security of bid/offer price information, we would recommend that this data be encrypted where feasible without restricting the system operators' role.

System Management. In addition to the nine minimum requirements listed in the NOPR, the system management should also require the use of Public Key Infrastructure (PKI) security for any system that uses Internet protocols such as HTTP (S) for users that are internal or external to the enterprise. This system should include digital certification and smart cards. We also recommend that data submissions by market participants should be preserved using PKI Digital Signatures. Such non-repudiation technology will provide irrefutable proof that the data were submitted by the participant.

Business Continuity. We urge the Commission to add requirements for disaster recovery sites, such as not being co-located or next door to the actual operation site. Requirements should also include minimum staffing levels and competence needed, as well as the timeframe for the recovery in order to minimize impact to the consumer. We also recommend that the Commission require a listing of what data is critical to maintain and what data are non-critical in the event of a disaster.

Allegheny Energy Supply Company, LLC and Allegheny Power

I. Security Standards for Electric Market Participants

1. System Security — Self-Certification

The Allegheny Companies concur with the BET Security Committee's position that transmission providers will have undue burdens placed on them to track security standards compliance by entities not under FERC jurisdiction. The Allegheny Companies believe that by not having to comply with the security standards, these entities would not only have a competitive advantage, but any such exemption could also impact the transmission system's security. The Allegheny Companies recommend that the Commission, not the transmission provider, perform compliance verification for 4 market participants.

2. Appendix G — Security Standards for Electric Market Participants

a. Overview

The Allegheny Companies agree with the Commission that due to the highly interdependent operation of the transmission system, minimum cyber security standards should be established for all wholesale electric system and market participants. If the intent of the SMD Security Standards is to focus on cyber security, however, the Security Standards contained in Appendix G of the SML) NOPR are too broad and ill defined, creating potentially significant time and financial commitments to companies regulated by the Commission that are required to comply with the Security Standards.

In addition to internal evaluation, the Allegheny Companies are working with and monitoring the BET Security Committee and NERC to determine how they are reacting to the Security Standards. Based on preliminary discussions 'with the EE Security Committee and NERC, many of their concerns with Section M and the Security Standards mirror the Allegheny Companies' concerns. The Allegheny Companies understand that the Commission is allowing NERC to resubmit a refined draft Security Standard. The Allegheny Companies concur with this approach and will work through the BET Security Committee to provide input on the refined Security Standards.

Finally, cost recovery for additional security measures (physical, cyber, background investigations, training) and the mechanism to recover such costs is not included in Section M or the Security Standards. The Allegheny Companies recommend that security costs directly related to implementation of the Security Standards be

recoverable as part of the overall SMD implementation costs through a limited Section 205 rate change filing.

b. Purpose

The Allegheny Companies generally agree with the purpose of the security standards, but must reiterate that the purpose is too broadly defined. The purpose should be limited to critical cyber systems and assets that directly affect the transmission system. Thus, all references to security programs, security perimeters, etc. should, at minimum, be restricted to cyber security programs, cyber security perimeters, etc. The Allegheny Companies concur with BET that the referenced list of other industry standards in the document should be excluded as they may conflict with the intent of the SMD Security Standards. The Allegheny Companies recommend maintaining the reference to the NERC Security Guidelines in the standards.

c. Compliance

The Allegheny Companies recommend that the Commission delete the following two sentences from the standards: “Failure to comply with these security standards will result in loss of direct access privileges to the electric market” and “Malicious acts directed against the electric market, shall be prosecuted by FERC and law enforcement agencies to the full extent of the law, including the recovery of damages.” These sentences add no significant value to the standards. 11, however, the SMD does not provide sanctions for non-compliance with any of the SMD’s requirements, the Allegheny Companies recommend that the Commission impose significant financial penalties for non-compliance with the security standards.

d. Security Scope

It appears the Commission intends to limit the Security Scope to “cyber security,” but as written, it is not so limited and would cost utilities significant time and money to comply. The Commission needs to provide a clearer statement of the intent and scope of the Security Scope. The Commission should clearly define cyber and physical security in relation to the transmission system’s critical cyber assets. The Allegheny Companies agree with the definitions proposed by the EE Security Committee.

e. Asset Classification and Control

This section is also ill-defined and could be read to include much more than the critical cyber assets that control the transmission grid. The Allegheny Companies

recommend that the section be rewritten to include only the assets targeted by the standards.

f. Personnel

The Personnel section requires security awareness training programs to be developed and implemented for new employees “who are authorized access within the security perimeter, or are authorized access to administer, operate or maintain assets within the security perimeter.” The program would require annual security awareness updates.

The Allegheny Companies recommend that the training requirement should apply only to personnel seeking access (either physical or cyber) to the classified/defined critical cyber systems. For authorized, unescorted personnel (Company and Contingent Worker) background investigations will need to be completed initially and at least every five years thereafter. Background investigations should be limited to those seeking access to the classified critical cyber facilities. Without limiting background investigations to the critical cyber facilities, the resources required to conduct background investigations or escort personnel into the loosely defined “security perimeter” will be tremendous. State and local law may preclude utilities from completing Background Investigations on those employees already employed. The Allegheny Companies, therefore, concur with the EE Security Committee that the Commission note in the standards that “each company follow their own internal adjudication procedures when derogatory information is developed on an individual who has access to cyber facilities.”

Alliant Energy Corporation

CYBER SECURITY STANDARDS

Governance:

Market Participant senior management shall designate a management official to be responsible for establishing and managing a basic Cyber Security Program for electric wholesale market operations and for submitting self-certifications to the FERC.

Information supporting annual self-certification of compliance with these cyber-security standards shall be retained by the Market Participant for a period sufficient to permit reasonable review and verification by FERC.

Scope:

Market Participants shall define their security perimeters and identify the boundaries and defenses for physical and cyber security that delineate and protect the critical resources under their control. The security perimeters shall identify all entry and exit points and the requirements for access controls.

A Cyber Security Program and policy based on these Cyber Security Standards shall be developed to protect Market Operations. Additionally, related procedures shall be created that guide implementation and enforcement of the Cyber Security Program and policy. The Cyber Security Program, policy, and procedures shall be reviewed for appropriateness (due to changes in personnel, technology, equipment configuration, vulnerabilities and threats) as necessary, and at least annually.

Asset Identification:

Each Market Participant shall identify those cyber assets that are critical to the operation of the wholesale market. Those assets shall be afforded a level of security commensurate with their overall criticality.

Access Control:

Procedures shall be in place to identify individual users of critical cyber assets within the security perimeters and their time of access. Personnel, including visitors and service vendors, shall only have access to critical cyber assets within the security perimeters for which they are authorized. Personnel allowed temporary access within the security perimeter shall be escorted at all times.

Procedures for critical electric resources within the cyber security perimeter shall be established to monitor and control physical access in accordance with relevant NERC Security Guidelines.

Critical electric facilities shall restrict the distribution of maps, floor plans and equipment layouts pertaining to those facilities, and restrict the use of signage indicating critical facility locations.

Personnel:

Any person authorized to have access within a secure perimeter shall be trained on the Cyber Security Program and security standards relevant to their respective positions. This training shall start upon employment, be reviewed annually and at career points where significant responsibilities change.

Ongoing programs to ensure trustworthiness and reliability of individuals with authorized access to critical cyber systems are required. These programs shall be conducted consistent with applicable laws, human resource practices, and NERC Security Guidelines for Background Investigations.

Systems Management:

Procedures for protecting critical cyber assets within the security perimeter shall address:

- The use of effective password routines that periodically require changing of passwords, including the replacement of default passwords on newly installed equipment;
- Authorization and periodic review of computer accounts and physical access rights;
- Disabling of unauthorized (invalidated, expired) or unused computer accounts and physical access rights;
- Disabling of unused network services and ports;
- Secure dial-up modem connections;
- Firewall software;
- Intrusion detection;
- Security patch management;
- Installation and update of anti-virus software checkers;
- Assurance that communication channels are adequate so as not to impact Market Operations.

For critical electric systems, operator logs and intrusion detection logs shall be maintained for the purpose of checking system anomalies and for evidence of suspected unauthorized activity.

Planning:

Security requirements for Critical Cyber Assets within the Electronic Security Perimeters shall be identified, documented and agreed upon prior to development, procurement, enhancement to, installation of and acceptance testing for cyber assets or related physical features. For Critical Cyber Assets, this means developing cyber security procedures to augment existing test and/or acceptance procedures.

Development and testing of Critical Cyber Assets shall be conducted in a manner so as to not adversely impact electric and wholesale market operations.

Incident Response:

Market Participants shall have incident response procedures, which define roles, responsibilities and actions to rapidly detect and protect critical cyber assets in the event of harmful or unusual incidents, whether accidental or malicious.

Market Participants shall report incidents in accordance with the NERC-NIPC Indications, Analysis and Warning (IAW) Program.

Business Continuity:

Market Participants shall have contingency plans that define roles, responsibilities and actions for protecting the rest of the electric grid and wholesale market from the failure of their own critical resources. Those plans should further define the roles, responsibilities and actions needed to quickly recover or reestablish electric grid and wholesale market functions, processes and systems, in the event that a critical physical or cyber resource fails or suffers harm or attack. Such plans shall be tested or exercised regularly.

Ameren Corporation

E. Security (SMD NOPR PP 575-79)

Ameren asserts that minimum cyber security standards must apply to all market participants, in light of the reality that the areas of the entire wholesale electric grid and market are highly interdependent. See SMD NOPR at P 575. Further, the Commission should refrain from permitting exceptions to the minimum standards, as exceptions compromise the intent in establishing standards. See SMD NOPR at P 577.

The Commission should continue to look to NIERC to develop security standards. The Commission already proposes administering, through self certification, the set of recommended minimum requirements developed by NERC's Critical Infrastructure Protection Advisory Group ("CIPAC") to ensure that a given entity has a basic security program protecting the electric grid and market. See SMD NOPR at P 576; Appendix G. However, this set of minimum requirements has not been fully scrutinized through the NERC consensus standards process. NERC is in the process of developing and refining the minimum requirements, and the Commission should accept the revisions to the minimum requirements that result from that process. SMD NOPR at P 579.

In addition to the overall position that the Commission should follow NIERC with respect to the appropriate security standards, the Commission should also make several specific security-related revisions to the SMD Final Rule. The Commission should revise the title of Appendix G to read "Cyber Security Standard for the Electric Wholesale

Market Operations Participants.” This title would better convey the Commission’s intent to focus on cyber security issues. The Commission should also remove the list of industry standards references in the “PURPOSE” section of Appendix G because those standards do not directly address the Commission’s concerns and could potentially conflict with the Commission’s future intentions regarding security. Additionally, the Commission should adopt the definitions developed by the EEI Security Committee and the NERC CIPAG for the following terms: critical cyber assets, electronic security perimeter, physical security perimeter, and authorized person. Further, certain sections of the standard stated in Appendix G relate to policy and the Commission therefore should address those sections in the preamble to the SMD Final Rule, where it would be more appropriate. These sections include the “APPLICATION” section, the “COMPLIANCE” section, and the “REFERENCES” section.

Ameren also suggests that the Commission acknowledge certain obstacles to the background checks and self certification processes. While ongoing programs related to background checks are important to ensure the trustworthiness and reliability of individuals with access to critical cyber systems, the Commission should recognize that utilities may be limited by state and local laws restricting the ability of companies to perform background investigations on existing employees. Ameren also urges the Commission to remove the following provision regarding the provision of self-certification forms as it would impose an undue burden on public utilities to track the compliance of non-public utilities:

The customer can satisfy this requirement by supplying the public utility with a copy of the executed self-certification form. In the case of entities seeking transmission service that are not public utilities subject to the Commission’s regulations, the entity would still be required to demonstrate that it has a basic security program in place to receive transmission services. This could be done by supplying the transmission provider with an executed self-certification using the Commission’s form.

SMD NOPR at P 577.

Requiring public utilities to track the compliance of non-public utilities would be time-consuming prohibitively and expensive. The ITP would be better suited to keep track of security compliance.

American Public Power Association

comments on System Security (Section IV.M, ¶¶ 575-579, and Appendix G)

Security is a reliability issue and should be handled by NERC and NAESB, and requirements should be crafted to minimize burdens on small LSEs.

In Section M, and Appendix G of the SMD NOPR, the Commission proposes to impose physical and cyber-security compliance obligations on all entities with access to information on RTO/ITP markets, including transmission and energy market customers. See in particular ¶ 577. APPA shares the Commission's concerns with this national security issue, but suggests that physical and cyber-security is not inherently part of a standard wholesale electricity market design and properly encompasses other industry activities, such as the reliability of electric grid operations, retail electric service and the nation's natural gas supply and delivery system. Submission by each customer of an annual certification of compliance also fails to establish the means by which small entities can assure compliance in fact, not just on paper. The Commission should task NERC and NAESB with this issue.

APPA and its members are active within and supportive of the North American Electric Reliability Council (NERC) standing committees and working groups that address these issues. In fact, APPA has been a member of the NERC Critical Infrastructure Protection Advisory Group (CIPAG) since its inception in 1998, and recommends that this NERC body continue to develop and issue the necessary standards and guidelines in accordance with the NERC standards development process, to ensure the reliability and security of the interstate transmission grid. The Electric Sector Guidelines developed by NERC's CIPAG are currently in place and cover many of the same requirements discussed in the original Section M and Appendix G of the NOPR. These Physical and Cyber-focused requirements will ultimately become standards through this NERC process. APPA recommends that FERC specifically reference the NERC process rather than develop redundant standards for the industry through the final rulemaking.

APPA does have concerns that the NERC CIPAG membership does not represent a balance of all stakeholder interests within the electric power industry. As one would properly expect, the work products of this group reflect the engineering and security orientation of the participants. Thus the proper concerns of commercial interests in establishing standards that do not present undue, inadvertent barriers to buying and selling energy or scheduling transmission may not have received the attention they deserve. NERC and NAESB, working under a newly developed Memorandum of Understanding (MOU) that is awaiting approval by their respective Boards, are currently

developing an open process for development of standards that have implications for both grid reliability and business practices/communication protocols. APPA recommends that this joint NERC-NAESB process be employed. The Commission should request that NAESB review the standards under development by the NERC CIPAG and that NERC and NAESB consider whether joint standards development is appropriate.

Further, the cost of compliance with these rules is a critical issue for APPA members and for smaller electric utilities of all types. APPA reminds the Commission that there are over 3000 electric utilities in this country, 2000 of which are state, municipal and other locally owned systems. There are over 1000 public power systems that own no electric generation capacity, have total annual revenues of less than \$5 million per year, or serve less than 2000 customer meters.

The inception of another certification process, especially one that is self-certification, adds an additional reporting burden, especially for smaller entities that already face other extensive and burdensome regulatory reporting requirements. Security Guidelines and Standards, both physical and cyber (which go far beyond the proper scope of a standard electric market design rule promulgated under the Federal Power Act), should be left to those entities that have been tasked with overall the reliability and security of the electric grid – NERC, DOE, and the anticipated US Department of Homeland Security. APPA is working with all of these agencies to ensure that the security standards development process is FOBI – Fair, Open, Balanced and Inclusive. This method ensures that the final standards are clearly defined, broadly accepted, and cognizant of the budgetary implications that are involved with instituting additional security standards.

If, however, such physical and cyber security standards are included in a final SMD rule, LSEs that do not own or operate facilities or systems that affect the reliable operation of the interstate transmission grid should not be required to implement these standards, nor submit any certification form. Instead, these entities, which will not affect the operation of the electric grid, should work with their ITP, RTO, or other transmission provider(s) to ensure appropriate security protections are in place.

To the extent that the Commission's concerns relate to use of electronic interfaces with electric markets developed in response to the proposed rule, tiered access to ITP systems is appropriate and more cost-effective than attempting to ensure that each electronic interface with ITP systems has protections equivalent to the physical and cyber-security requirements adopted for electric utility control center and dispatching operations. For example, transmission customers may want or need access to only a limited number of ITP markets (e.g., self-scheduling of generation resources or bilateral schedules) and read-only access to many data bases (e.g., current nodal prices and the

status of certain transmission lines that are critical to reliable service to their load buses). A small LSE obviously might prefer limited electronic access to the ITP's systems with built-in limitations on its trading activities to prevent the commercial terrorism with which the Commission may be concerned, in lieu of installing rigorous physical security barriers for the office of a municipal electric with ten or twenty employees.

Arizona Corporation Commission

F. System Security

(¶ 575.)The ACC agrees that reliable operation of the transmission grid must not be compromised by software and system information infrastructure needed to monitor, dispatch and manage the wholesale market. Establishing minimum standards for such infrastructure is appropriate.

(¶ 576.)The ACC supports NERC's Critical Infrastructure Protection Advisory Group recommendation of minimum standards for securing information assets that support grid reliability. Administering these requirements via an annual self-certification process seems reasonable.

(¶ 579.)Applying information standards strictly for commercial expediency of the wholesale market may be unduly costly. The true test for implementing such information standards should be based on maintaining grid reliability rather than for commercial convenience. Relying on NERC for such standards rather than NAESB will assure FERC that the reliability goal is the fundamental purpose of such standards.

Canadian Electricity Association

(3) Critical Infrastructure Protection

CEA actively participates on NERC's Critical Infrastructure Protection Advisory Group and endorses the need to establish minimum security standards as drafted in Appendix G of the NOPR. CEA has identified a number of concerns and suggestions regarding these proposed standards, including:

- clarify that the scope of the security standards is centred on critical "cyber" assets, and not the physical security of electricity infrastructure or facilities
- emphasize that the implementation of protective measures by individual Market Participants is intended to be proportional, and driven by their individual risk to the electricity market

- clearly define key terms such as critical cyber assets, electronic security perimeter and physical security perimeter
- ensure that the applicability of the security standards to various Market Participants is consistent with the Standard Market Design itself
- harmonize the self-certification process with other compliance processes developed by NERC as part of its developing standards process
- clarify the self-certification process, including how exceptions and areas of noncompliance are identified

CEA is working with NERC to provide comments and develop a revised Appendix G. As such, CEA strongly suggests that FERC accept NERC's comments and recommendations. Further, CEA expects that these standards will need to evolve over time and should endure through the developing NERC standards process.

Cinergy Services, Inc

Section IV, M: System Security and Appendix G

This section refers to NERC's Critical Infrastructure Protection Advisory Group and the set of recommended minimum requirements it has developed. These would be administered through a self-certification process and would impact Cinergy both as a transmission owner and a transmission customer.

Comment: Cinergy generally supports the Comments filed on November 15, 2002 in this docket by Edison Electric Institute on § M and Appendix G.

CMS Energy Corporation

14. The System Security standards discussed at the end of the SMD NOPR require careful Commission attention regardless of the disposition of the balance of the SMD NOPR.

The System Security standards dealt with in Section IV. M. at the end of the SMD NOPR and in Appendix G are important matters for the electric industry in their own right, separate from the industry restructuring that is the subject of the rest of the SMD NOPR. It is important that System Security receive careful attention on its own and not merely be swept along on the wave of industry restructuring.

Thus, it is important that the Commission allow the North American Electric Reliability Council (“NERC”), in consultation with market participants, to submit a more refined set of draft standards in place of the version that was hurriedly prepared for inclusion in the SMD NOPR and carefully and critically review the individual components of the standards. Since the standards are important in their own right and are essentially separate from the main thrust of the SMD NOPR, it would seem appropriate for the Commission to develop these standards in a process separate from the SMD process where the standards would be more likely to receive the attention that their significance merits.

CMS has the following specific comments to offer. They all address Appendix G, as supplemented by the Commission’s August 1, 2002, Errata in this docket.

a. Clarify the focus on “cyber” security.

At the bottom of page 1 of Appendix G is the statement that the “[s]ecurity standards will primarily focus on . . . cyber [matters].” The balance of Appendix G does not explicitly limit itself to cyber security. The final version of the standards should make it clear that the standards apply only to cyber facilities and cyber security.

b. Proper scope of cyber security.

The Appendix G standards and Self-Certification form both make reference to maintaining security perimeters, but fail to provide specific guidance on how to establish perimeters or what to include. The initial inclination is to draw perimeter lines broadly to make sure they do not miss any potential threat. But drawing perimeters too broadly can be counterproductive. Effective cyber security is not achieved easily or cheaply. Drawing too broad of a perimeter would be unnecessarily expensive for the entities required to comply. Even worse, requiring security too broadly for low risk facilities waters down the overall security effort and distracts attention and resources away from the truly critical cyber assets that require vigilant attention.

Appendix G recognizes this balance in its definition of “cyber” at the bottom of the Appendix’s first page. That definition refers to control systems “as they impact the grid or market.” At page 4, the standards discuss classifying assets by their criticality. Consistent with those notions, the final version of the standards should make it clear that security perimeters are intended to include only those cyber assets that have an enhanced capability of having a material impact on the electric grid or electric markets.

An illustration of this concept is provided by generating plants in CECo's service territory. Cyber devices at CECo's generating plants can receive data from the network-operating system and send data about the generating plant's status back to the network-operating computer. There is, however, no software at those generating plants that could control the electric network. Therefore, even if an individual gained access to a generating plant's cyber devices, he could not control the electric network. The electric network is controlled remotely using SCADA equipment that is located outside the physical boundary of the generating plants. Any cyber attack to the network would have to take place at the physical location of the SCADA equipment or via an Internet telephone access. While Internet access from a generating plant computer, there is no technical advantage to someone trying to access the SCADA system from a plant computer. In fact, there would be a greater risk of detection of SCADA access from a generation plant computer than from a remote computer.

Given the lack of any real threat to the electric network from a generating plant's limited cyber assets it is not reasonable to impose the costs of creating a physical security perimeter around cyber assets at a generating plant. The plant itself already has security features designed to control access to the plant. Adding a second physical security perimeter within the plant adds costs and inconvenience without adding any real benefit to the security of the electrical network. It would only unnecessarily drain off and dilute cyber security resources that are needed more elsewhere.

CMS agrees that cyber protection measures, such as firewalls and password protection should apply to generating plant cyber devices. But where there is no enhanced ability to use those devices to materially impact the electric grid or electric markets, there should be no requirement for special physical security requirements for generating plant cyber assets.

c. Security standards for third-party personnel and equipment; wireless connectivity.

The standards do not explicitly address the required extent of security measures for consultant or contract personnel or security certification for purchased software, etc. This is an important part of overall security and explicit guidance should be given on requirements and on who is responsible for which portions of those requirements. CMS believes that it would be most efficient for contractors to pre-screen and pre-train their personnel. The Commission should consider providing a mechanism for certification of such third party programs.

d. Treatment of incident report data.

At page 8 and in the Self-Certification form, Appendix G deals with the reporting of incidents to ES-ISAC. But no mention is made of what becomes of reported data. CMS suggests that the data (once it has been reviewed and “scrubbed”) be made available to other entities for use in their own security efforts. Such shared information would be helpful in preventing the occurrence of similar incidents elsewhere.

e. **Personnel training and screening.**

(1) **Training.**

Page 4 of Appendix G calls for security training for “[a]ny personnel who are authorized access within the security perimeter . . .” and calls for “[s]ecurity awareness training . . . [f]or all staff.” “All” and “any” are quite broad and take in many personnel for whom such training would not be necessary and whom the drafters of the standard may not have intended to include.

“Any personnel who are authorized access within the security perimeter” includes on its face people with access within the perimeter but who do not work with the critical assets and who have no passwords, etc. to allow them cyber access. It can include various levels of support personnel such as mailroom and janitorial staff. For such personnel a lower level of training, possibly security awareness training, would be more appropriate.

For larger, multi-purpose entities “all staff” can include personnel who never come within 100 miles of critical assets and personnel who have no contact at all with electric matters, much less electric operations. Taken literally, it includes gas staff at a combination utility like CECO. Presumably these standards would not apply to non-jurisdictional operations, but Appendix G fails to explicitly limit the scope of “any” and “all.” Appendix G needs to be more detailed in this area and needs to reflect that the standards will cover entities that have a broad range of activities, many of them unrelated to electricity.

(2) **Screening.**

The standards call for screening personnel initially and every five years “to the extent permitted by law.” Thus, the standards totally ignore the subject of what is and is not permitted by law. Especially in certain states, such periodic background screening may not be permitted by law at all. The federal Fair Credit Reporting Act significantly limits the extent to which selective background checks can be performed. The Appendix G standards give no guidance as to what is to be done if such personnel screening proves

to be illegal. If such a standard is to be imposed, FERC and or NERC need to take a close look at legal restrictions and devise a standard that is compatible with those legal limitations rather than just “punting” and calling for something that may not be possible.

An alternative would be for some specific entity, such as the Office of Homeland Security, to perform background checks and screens. That outside entity would be responsible for weighing the balance between what is desired and what is legally possible.

f. Need for flexibility.

In its standards of conduct for Transmission Providers, the Commission explicitly provides for deviations from the standards in emergency circumstances. (*See* 18 C.F.R. § 37.4(a)(2).) Similar flexibility needs to be provided in the cyber-security standards. In unusual situations, such as large-scale service restorations after major storms, additional staff will need to be present within the security perimeter. The standards need to provide the flexibility needed to deal with such situations.

As noted above, System Cyber-Security is a matter of growing importance. The Commission needs to devote its attention to the subject on its own, rather than as a last minute addition carried along by the SMD wave. If that means re-noticing a revised NERC set of standards in a separate docket, so be it. But, at a minimum, the Commission should address the draft standards’ shortcomings discussed above.

Crescent Moon Transmission Owners

F. THE COMMISSION SHOULD ADOPT NRECA’S POSITION REGARDING THE SMD SECURITY REQUIREMENTS.

NRECA (at 103-104) of its November 5, 2002 comments addressed Appendix G of the NOPR containing the security standards proposed by the NOPR. The implementation of those standards could be very expensive and could be prohibitively so on a per customer basis to rural utilities. Accordingly, the Crescent Moon members support in full the NRECA’s position as to the Appendix G security provisions.

Duke Energy Corporation

X. System Security (NOPR ¶¶ 575-579)

In brief,

- Although Duke Energy agrees that public utilities should have basic security programs in place, the SMD rulemaking is not the appropriate forum in which to address the issue. Therefore, the Commission should eliminate the proposal from the Final Rule.

Although Duke Energy agrees that public utilities should have basic security programs in place, it does not believe that the SMD rulemaking is not the appropriate forum in which to address the issue. As a result, Duke Energy strongly recommends that the Commission eliminate the system security proposal from the Final Rule altogether and complete it on a separate track. Duke Energy participates in and supports NERC's process to develop the standards. The Commission's proposal, however, suffers from various problems. First, the NERC process is a work in progress. Second, the Commission's proposal does not explain what the public utility is supposed to do with customer self-certifications, *i.e.*, is the ITP supposed to determine whether they are in compliance? The SMD Tariff says that the ITP is to "receive" the self-certifications, but there is no indication whether the ITP has any power to determine whether it is sufficient. Without such power, there does not appear to be any value from customers providing self-certifications to the ITP. If the Commission determines to leave the system security provisions in the NOPR, then Duke Energy suggests that deliberations on such matters be held in abeyance pending final NERC action on its proposed standards. Moreover, if system security standards are adopted, the Commission should recognize the cost of implementation and balance the value of such measures against the cost associated with them.

Edison Electric Institute

XI. EEI SUPPORTS CONTINUED NERC DEVELOPMENT OF SYSTEM CYBER SECURITY STANDARDS.

As the Commission has recognized, the operations of the wholesale electric grid and market are highly interdependent and failures in one area of the grid or market can have serious repercussions elsewhere. Therefore, EEI agrees that minimum cyber security standards are needed to safeguard the wholesale electric system and market. This minimum set of standards should be applicable to all Commission-determined responsible entities participating in the wholesale market ("responsible entities"). The Commission

has suggested that the most effective method for establishing minimum-security standards for the electric market would be for the Commission to reference the existing North American Electric Reliability Council (“NERC”) Security Guidelines.

EI supports the Commission’s approach to allow NERC to continue to develop these minimum cyber security standards. EI and its members have already worked with NERC and its members to develop and refine the draft standards which NERC intends to resubmit to the Commission. While preparation of these standards have been approved by the NERC Board, they have not been fully vetted by the industry. Before these standards are adopted they should be proposed for consideration through the NERC standards process. In addition, the Commission should request that this development be closely coordinated with NAESB to ensure that the cyber security standards are compatible with business and data practices being developed by that group. For example, NAESB electronic delivery standards for the natural gas industry already reflect security-related elements and have been reviewed favorably by Sandia National Laboratories. Wherever possible, the cyber security standards development should avoid “reinventing the wheel.” EI will continue to work with both NERC and NAESB processes.

NERC had a limited amount of time to provide the Commission with the initial draft of Cyber Security Standards. The standards, set forth in Appendix G of the SMD NOPR, are very likely to change during the NERC process. Recognizing that Appendix G represents a document that will change, EI offers in Appendix D to these comments some suggestions for modifications to the draft cyber security explanatory language as reflected in Section M of the NOPR. Several of these comments suggest that certain issues be removed from the Standards and instead be discussed by the Commission within the final rule itself. The basis for these comments is that the identified issues are more appropriately the subject of policy determinations by the Commission, rather than being decided in the context of the NERC standards development process.

Electric Power Research Institute

Electric power systems constitute the fundamental infrastructure of modern society. A successful terrorist attempt to disrupt electricity supplies could have devastating effects on national security, the economy, and the lives of every citizen. Yet power systems have widely dispersed assets that can never be absolutely defended against a determined attack. Following the September 11, 2001, terrorist attacks; EPRI undertook a preliminary assessment of major threats to the U.S. electricity system, together with potential countermeasures. This assessment was not intended to be a comprehensive guide to plant or grid security. Rather, it was assumed that individual utilities would quickly enhance the physical security of their own systems and that the EPRI assessment should concentrate instead on broader threats, where state-of-the-art technology could

make a substantial contribution to improving security. Building on these recommendations, an Infrastructure Security Initiative (ISI) has been created as a two-year effort to address key areas of security R&D. For ISI and other efforts to be successful, FERC should immediately ensure that adequate incentives are provided to the institutional entities that require them, for development and widespread implementation of security-related technology.

Electronic Scheduling Collaborative

Appendix G – We note in Appendix G that some discussion is given to the securing of information technology resources. The Electronic Scheduling Collaborative would like to ask the Commission to be aware of the need for a single, industry-wide security standard for protecting information assets. It is our belief that the current diversity of security standards from region to region and even application to application is extremely inefficient, requiring the uses of multiple passwords, security tokens, and other devices. While we do not dismiss the criticality of a secure system, we would ask that the Commission, either in its Final SMD Order or in subsequent Orders regarding OASIS, mandate the use of a single industry-wide security standard. Considering technology available today, we envision implementing this with digital certificate and public-key infrastructure technologies. While this may be premature for this Order, we ask the Commission to recognize the costly nature of such endeavors and, if the Commission believes a single standard to be appropriate, formally communicate to the industry that such a standard will be enacted. This will send a clear message to entities regarding their implementation budgets as they move forward.

Exelon Corporation and Sithe Energies, Inc

M. SYSTEM SECURITY

The NOPR notes that NERC's Critical Infrastructure Protection Advisory Group has developed standards for securing information assets that support grid reliability and market operations and for the physical environment in which those assets operate. The Commission proposes to require that public utilities with tariffs on file self-certify compliance with the standards annually beginning in 2004 (¶¶ 576-77). Exelon has been working with NERC on these issues and fully support NERC's position. Exelon understands that NERC is submitting its comments on these issues separately from its other comments on the SMD NOPR.

Georgia Transmission Corporation

System Security (NOPR PP 575-579)

GTC agrees that system security is critical to the reliable operation of the interstate transmission grid. In the NOPR, the Commission proposes a compliance schedule regarding the cyber-focused security standards listed in Appendix G of the NOPR.¹ NERC has previously submitted security standards to the Commission and the Commission should allow these standards to be developed rather than add an additional layer of oversight. Additionally, the Commission would require that non-jurisdictional entities, as a condition of taking transmission service, demonstrate or ensure that there is a basic security program implemented. GTC does not believe that it is appropriate to impose a “one size fits all” approach to these security standards. If, however, such standards are included in a final SMD rule, the Commission should take into account regional variations and allow the various regions flexibility in meeting these requirements, including how any non-jurisdictional entities are able to meet the requirement.

GreenBuilt Consulting

I just read the NERC CIPAG documents titled, “Final CIPAG comments on Security Sections of FERC SMD NOPR”, dated November 13, 2002. (These three documents are available at the following address:
<http://www.nerc.com/~filez/cipfiles.html>.)

When I consider the NERC CIPAG recommendations and compare them to other documents in the FERC Standard Market Design and Structure NOPR Docket RM01-12-000, I have the following concerns:

NERC CIPAG has proposed a much more limited definition of “market participants”, indicating that they are primarily entities that file an SMD tariff. This new definition overlooks other market participants that do in fact have impact on the integrity of the network through operations of process control systems.

The newly-proposed “self-certification form” is less defined than that which was included in Appendix G of the FERC SMD NOPR, wherein 17 specific proposed security standards are clearly stated. I consider this to be “back-pedaling” on the requirements, with the result that compliance would be much more subjective and security less stringent throughout the industry. Now is the time to ensure that this critical infrastructure industry

¹ NOPR at P 577.

takes security seriously; we are vulnerable and we need to implement clear measures to mitigate this vulnerability.

I am concerned about the NERC CIPAG statement that "...most participants believed that there should be some process to bring noncompliant entities into compliance before their access to the wholesale market (is) terminated." I agree with this suggestion in principle, but that said, my concurrence naturally depends upon the business processes that will be implemented to determine the level of non-compliance, the potential impacts of that failure to comply, and the level of commitment required to correct this failure. None of these business processes have been proposed. The goal must be compliance, not development of remedial programs that will eventually achieve compliance. Market participants will have a year to comply if the FERC ruling on security standards is made by year-end: that leaves plenty of time for participants to comply.

I am saddened that NERC CIPAG is not supporting required compliance for the January 2004 date that the standards will become effective, ostensibly because "...budgets for 2003..." have been finalized and "...it is not appropriate to expect more than substantial compliance by January 1, 2004." I understand that preparation to mitigate potential terrorist attacks does not fit into the industry's collective planning budget timeline, but this is certainly not a reason to allow for non-compliance so far in advance! Market participants should pursue compliance now with commitment and dedication; we certainly do not want a catastrophic breach of security to provide the impetus for willing compliance with proposed security standards.

In summary, I am concerned about the recent NERC CIPAG cyber security recommendations that suggest that:

There should be fewer companies identified as "market participants"
Proposed cyber security standards should be more general
Participants that aren't in compliance shouldn't be restricted from grid access without options to make amends
It should be OK to be "mostly" compliant in the first year because 2003 budgets are already set

Interruptible Industrial Intervenors

J. System Security (PP 575-79)

The NOPR recognizes that, "[s]ystem security is critical to the reliable operation of the interstate transmission grid" (NOPR at P 575), and the Commission proposes minimum security standards. *Id.* at P 576. The standards are designed to ensure that

market participants have basic security programs in place in order to “protect the electric grid and market from the impact of acts, either accidental or malicious, that could cause wide-ranging harmful impacts on grid operations.” *Id.*

The NOPR calls upon public utilities to file for self-certification of their security measures by January 31, 2004, and every January 31 thereafter. *Id.* at P 577. The Commission also proposes to extend the requirement to cover “any customer seeking to buy or sell through the markets operated by the Independent Transmission Provider or take transmission service.” *Id.* at P 578.

Interruptible Industrial Intervenors agree that security measures are important, but they are concerned about the Commission’s proposal to extend the requirements to cover any customer seeking to buy or sell through the markets. Historically, public utilities implemented their own security measures in order to safeguard their systems from the types of accidents or malicious acts the NOPR discusses, and they have been able to spread the costs of implementing those measures over many end users in the regulated markets. A similar requirement on single-site industrial end-users participating in the markets will prove overly burdensome; because these end-users, unlike utilities, would have to absorb 100% of the costs of implementing these security measures themselves.

The security requirements that the NOPR specifically discusses include:

- Designating a management official to be the Security Program manager;
- Defining security perimeters and boundaries for physical and cyber security;
- Classifying electric market assets;
- Assigning custodians for critical assets;
- Training employees;
- Maintaining logs of users of critical systems;
- Establishing procedures for protecting critical market resources including:
 - ▶ Appropriate security barriers and entry controls;
 - ▶ Mechanical and electronic key and badge programs;
 - ▶ Access locking of unattended assets; and,
 - ▶ Protection from environmental threats and hazards (e.g., loss of cooling).
- Implementing planning measures for security requirements;
- Implementing incident response measures; and
- Establishing contingency plans.

For an industrial customer acting as its own LSE, some or all of these measures may be unnecessary as its load does not critically impact the grid, and the cost of compliance may be very high. The Commission should ensure that, if system security

requirements apply to end-users at all, such requirements not be any more burdensome than absolutely necessary. Otherwise, non-essential requirements could be so onerous that they keep end-users from participating in the markets.

ISO New England Inc

“M. System Security” (¶¶ 575-579)

¶ 575-579 System Security

The Commission has set forth a security program including self-certification. ISO-NE supports this program and recommends that compliance be measured against the Commission’s Security Standards; a signed Self-Certification should always be required. Reasonable due process should be provided before the final decision is made to prohibit a non-compliant entity from engaging in market activity. Also, it is unclear whether the ITP would be required to make the decision and directly take the action to prohibit noncompliant entities from participating in the market. The Commission should clarify the hearing process envisioned, the identity of the final decision-maker, and the process for allowing re-entry into the market. Depending on the scope of the final rule, additional funding and site inspection teams may also be required.

“Data and Confidentiality Provisions” (Appendix B, Part I, A, 12)

The Commission has included a new section in the proposed SMD Tariff concerning data and confidentiality provisions. As part of the final rule, ISO-NE recommends that the Commission consider provisions allowing for ITP market monitoring units to share confidential market information. This would help ITPs more effectively to identify and prevent inappropriate gaming strategies.

Kansas City Power & Light Company

APPENDIX G – FORM FOR ANNUAL SELF-CERTIFICATION OF COMPLIANCE WITH COMMISSION SECURITY STANDARDS

KCP&L has participated in EEI (Edison Electric Institute) conferences concerning the subject matter of Appendix G. KCP&L encourages the Commission to consider the EEI recommendations on this matter.

Los Angeles Department of Water and Power

V. SYSTEM SECURITY

The NOPR proposes that all public utilities certify that they have a basic security program consistent with certain minimum requirements recommended by NERC's Critical Infrastructure Protection Advisory Group. NOPR at P 576-577 and Appendix G. These requirements are proposed to ensure that public utilities have a "basic security program protecting the electric grid and market from the impact of acts, either accidental or malicious, that could cause wide-ranging harmful impacts on grid operations." NOPR at P 576. The NOPR also requires customers receiving transmission service, including non-public utilities, to demonstrate that they have a basic security program.

LADWP generally agrees that system security is a critical element of the reliable operation of the interconnected power system (generation and transmission) and that utilities with control of or access to the transmission grid should establish adequate standards to ensure the physical and cyber-space integrity of the system. LADWP also supports the proposed adoption of a self-certification system as an effective and nonburdensome means to ensure compliance with certain minimum requirements.

There are, however, important questions relating to the implementation of the proposed system security policy that the Commission should clarify. First, it is unclear how the Commission will assess the self-certifications to determine compliance or noncompliance, and what process is in place to resolve disagreements in security definitions and assessments. The form for self-certification found in Appendix G of the NOPR lists several security standards that utilities should adopt. The Commission should clarify the standards for judging compliance. Is failure to comply with a single standard sufficient to trigger a finding of non-compliance? Must there be substantial non-compliance? The Commission should also clarify the consequences of failing to comply. Since the Commission proposes to require filing of a certification as a condition of receiving transmission service, the consequences of non-compliance might arguably include the loss of access to the market, with the potential for causing contractual breaches. LADWP is concerned that such a penalty may be too harsh, especially if it is triggered by the failure to comply with a single standard. The Commission should consider case-by-case sanctions that are proportionate to the extent of the utility's non-compliance.

NERC has suggested changes to the initially proposed Security Standards, such as delaying the due date for implementation of the Security program, confidential treatment of data provided to the Commission, phased-in penalties for compliance, and consideration of changes in business environments and organizational changes when

attempting to comply with Security requirements. LADWP supports these concepts. LADWP also seeks clarification on two additional points. The Commission should specify which officials or employees of a utility would be qualified to sign the self-certification. The Commission should also clarify whether the requirement of background checks for employees would also extend, in some form, to contractors and visitors. On this issue, the Commission should consider the possibility that periodic background checks on employees may be inconsistent with labor union agreements or with provisions regulating civil service.

Louisville Gas and Electric Company and Kentucky Utilities Company

H. Security Issues

Overall, LG&E/KU believe the Security Standards for Electric Market Participants are a good start in defining minimum best security practices for the electricity sector. However, certain elements of these standards require further definition and clarification. First, there may be some confusion surrounding the term *security* as it has been and is currently being used in the industry. Historically, security has been used by NERC to refer to the reliability, availability and fault tolerance of the electricity system. With the increased risk of malicious acts against the power grid and related assets following September 11, 2001, and an increasing awareness of a need for 'cyber security', the term security is now commonly being used to refer to the need to protect those market assets that are potential targets for malicious physical or cyber attacks. The extensive use of the term security by the industry in two distinctly different ways will undoubtedly cause confusion, especially for those not familiar with NERC's use of the term. The FERC should clarify the definition for the benefit of all market participants.

Second, with regard to Compliance, the SMD NOPR stipulates that participants shall be compliant by January 1, 2004. There is a tremendous amount of work and expense that would be required to meet this requirement, counseling in favor of a prioritized and phased compliance approach.²

² The requirements for security awareness training alone are significant, and it would be very difficult to implement a comprehensive and effective training program for all personnel within a one-year timeframe. Training will require time for the development of an appropriate curriculum, associated course materials, and the coordination and scheduling of personnel to participate.

Third, the SMD NOPR assumes that security rules will be implemented seamlessly across physical and cyber boundaries, ignoring the fact that the organizations responsible for each type of security are distinctly different. Recommended guidelines that would facilitate coordination between physical and cyber security efforts would help to make compliance with the proposed rules in the proposed timeframe more obtainable. It would also permit coordinated uniform responses to raised alert levels and increase the effectiveness of the resulting security measures.

Fourth, in the Security Scope section of the SMD NOPR, a requirement for the definition of the security perimeter is mentioned. The definition of the security perimeter is nebulous, and is generally considered by security experts to be an outdated concept. More and more, this is extended through vendor and business partner connections, clients accessing systems from "anywhere, anytime", etc. LG&E/KU suggest that, rather than focusing on defining this "perimeter", the SMD should focus on defining individual security zones based on criticality and/or sensitivity of the assets. These security zones would then be the basis for definition and implementation of the appropriate security protective devices or other mitigation measures.

Fifth, LG&E/KU is concerned that the guidelines refer to the NERC Security Guidelines for the Electricity Sector Version 1. These guidelines are separate from FERC and there is a concern that there could be conflicting direction. Significant cost can also be expected to conduct the periodic background checks required for employees working in a critical area

Sixth, the guidelines stipulated under the Systems Management section are generally consistent with what LG&E/KU have been proposing in internal assessments for the Company's SCADA/DCS ("Supervisory Control And Data Acquisition / Distribution Control System") systems. However, there are significant issues that are yet unresolved that would prevent compliance with some of these stipulations. For instance, firewall and IDS ("Intrusion Detection System") software, though somewhat effective, do not address the proprietary protocols involved with some of these systems. Also, most if not all vendors do not support aggressive patch management, that is, they do not certify patches in a timely manner to work with their software. In general, most of these requirements are only applicable for those systems running commercial operating systems (not proprietary systems software). LG&E/KU also question how far the physical environmental controls should apply; many of the current systems do not have backup power supplies or protection from loss of cooling or similar problems.

Seventh, the requirements for development of incident response procedures are not clear. These standards do not include detail as to what is required to be compliant here. For instance, is just having a "master switch" for isolating the network from an outside

connection in the event of a "harmful or unusual incident" adequate, or are backup connections required, such as dial-up contingencies, backup ISDN ("Integrated Services Digital Network") lines, or the like?

Minnesota Department of Commerce

M. SYSTEM SECURITY

MDOC appreciates the Commission's concern about system security and appreciates the Commission spelling out what it believes constitutes security standards. However, the Commission's approach to ensuring compliance through the implementation of Appendix G of its SMD proposal appears to need more refinement. In particular, it is hard to imagine organizations professing non-compliance on their own. In addition, it would be important to work with local agencies if emergencies arise.

Mirant Americas, Inc. and Mirant Americas Energy Marketing, L.P.

L. System Security

Mirant agrees with the Commission that system security is critical to the reliable operation of the interstate transmission grid. Mirant, however, is concerned with the proposed annual self-certification process (SMD NOPR on Page 576). There are several issues that need to be fully vetted before the certification form should be implemented. Mirant proposes that the Commission host a technical conference to work through issues such as background verifications for bargaining unit personnel, certifying compliance on a local level rather than a corporate level and the standardization of policies among the various security agencies (NERC, DOE, Homeland Security, etc.)

Nevada Power Company and Sierra Pacific Power Company

M. System Security

page 306 ¶ 579

We expect that these standards will be revised and refined over time in light of changes in technology and operational experience with the standards. Therefore, the regulations will also identify the specific version number of the system security standards. When NERC revises the standards, the revisions will be filed with the Commission. The Commission will issue a Notice that it is considering revising the updated system security standards, and we will seek comments on the proposed changes. These security standards for electric market participants can be found in Appendix G, along with the proposed self-certification form, discussed above.

New York Independent System Operator, Inc.

XIV. SYSTEM SECURITY (PP 575 – 579, 594)³

The NYISO commends the Commission for taking the lead in the development of security regulations and supports its use of the NERC security standards as they are developed. The Commission should, however, clarify precisely what role (if any) ITPs are to play in reviewing their members' and customers' compliance with the standards. It should also clarify that the NERC security standards include a physical security, as well as a cyber-security component, at least with respect to the physical security of critical computer and information systems.

The NOPR states that transmission-owning utilities must provide ITPs with "assurances" of compliance with the NERC standards, as must customers that wish to take transmission and market services. Providing the assurance will normally involve filing a copy of the Commission's security self-certification form or presenting it to an ITP. Alternatively, customers may work with the ITP to "develop an alternative arrangement for ensuring that the customer has a basic security program in place."⁴ The NOPR does not say whether ITPs are required to evaluate the quality of the assurances they receive or take other actions to test system security. In addition, it does not specify whether there will be an adjudicative process to resolve compliance issues, or what ITPs are expected to do when service to non-compliant customers is terminated.

The Commission should eliminate these ambiguities in the final rule. It should carefully consider what obligations to impose on ITPs, since their transmission and market expertise will not necessarily endow them with security expertise. If ITPs are assigned extensive security responsibilities they will probably have to hire specialized staff and may lose their focus on administering efficient wholesale power markets. The NYISO believes that ITPs should not be required to verify the accuracy of market participants' self-certifications. In the event that they are given this responsibility, they should not be subject to liability for failing to detect invalid self-certifications.

³ In addition to the views expressed herein, the NYISO also supports the position of the *Joint Comments* on these issues.

⁴ NOPR at P 577.

New York Transmission Owners

SYSTEM SECURITY [SMD NOPR P 575-579]

In P 575, the Commission properly recognizes that system security is critical to the reliable operation of the interstate transmission grid and that it is necessary to safeguard the electric grid and market resources and systems by establishing minimum cyber-security standards for public utilities that own, control or operate facilities used for transmitting electric energy in interstate commerce as well as entities that use these facilities. The NYTOs have reviewed and join in the comments on cyber security standards that are being filed by the North American Electric Reliability Council (“NERC”). The NYTOs support NERC’s comments, including NERC’s proposed modifications to the cyber reliability standards published in Appendix “0” to the NOPR, and NERC’s comments on application, compliance and certification issues. The NYTOs’ comments on cyber security standards herein address the security standards as set forth in Appendix “G” to the NOPR and the discussion concerning those standards in P 575-579 of the NOPR.

COMMENT: Minimum Cyber Security Standards Are Appropriate And Should Reflect Electric Industry Standards As Referenced In North American Electric Reliability Council (“NERC”) Cyber Security Guidelines.

The NYTOs agree that the operations of the wholesale electric grid and market are highly interdependent and failures in one area of the grid or market can potentially have repercussions elsewhere. Therefore, the NYTOs agree that minimum cyber security standards are appropriate for all entrants that participate in the wholesale electric system and market. The “Security Standards for Electric Market Participants” (“Cyber Security Standards”) (NOPR, Appendix “C mirror the Security Guidelines that were recently developed by NERC’s Critical Infrastructure Advisory Group. The NYTOs agree that the Commission’s Cyber Security Standards should be revised and refined over time to reflect both changes in technology and operational experience with the standards as such changes are reflected in future revisions to the NERC’s Security Guidelines. The NYTOs also agree that interested parties should have the opportunity to provide the Commission with comments on such revisions before changes to the standards reflecting such revisions are adopted. In addition, to the extent that these initial Cyber Security Guidelines are materially modified as a result of this comment process, the NYTOs request an opportunity to provide comments on such modifications.

COMMENT: The Standards Should Be Clarified To Focus On The Security Of Cyber Facilities And Those Physical Facilities That Are I Integral To Cyber Security; Definitions Of Terms Should Be Provided.

While the intent of the “Security Standards for the Electric Market Participants” is to focus on cyber related security, the current terminology in these standards can be confusing. Therefore, the NYTOs encourage the Commission to amend the title to “Cyber Security Standards for Electric Market Participants,” and to incorporate language more specifically focused on the cyber component of the electric grid operations and market interactions. One simple step toward this end would be to replace “security” with “cyber security” wherever it appears in the standard.

The Cyber Security Standards do not contain definitions of key terms such as the cyber assets covered by the standards. The standards should also be clarified to clearly define their applicability to physical facilities in terms of their relation to the cyber asset security perimeter. To that end, the NYTOs propose that the Cyber Security Standards incorporate the following definitions:

- “Critical Cyber Facilities” — The computers, software, data (as stored and transmitted), servers, routers, modems, and communications channels (whether owned or leased) that are used to control the bulk power system (including generation assets) and for the sharing of appropriate market data and information.
- “Physical Security Locations —The dedicated locations that house bulk power/generation control centers, and computing facilities that host market data, operational control and communication functions that support the market.
- Physical Security Perimeter — The computer rooms, access points into these rooms, electrical and backup service to these rooms, and communication feeds that support cyber assets.

COMMENT: The Requirement For Training Should Be Clarified.

The Personnel section of Cyber Security Standards establishes Security Program training requirements for “any personnel who are authorized access within the security perimeter or are authorized access to administer, operate or maintain assets within the security perimeter.” The Commission should clarify the scope of this training requirement to state as follows: “any personnel who are authorized access without escort within the physical security perimeter or are authorized access to administer, operate or maintain critical cyber assets within the security perimeter.” The NYTOs request clarification if the proposed language is not consistent with the Commission’s intentions. In addition, the

language requiring “security awareness training ... for all staff” is vague and does not appear to add significantly to achieving the goals of the Standards. It should be deleted.

COMMENT: Promotional And Periodic Background Checks Should Not Be Required Unless Circumstances Warrant.

The provisions mandating background checks for critical asset operators and administrators — upon promotion to such positions and at five-year intervals — should be modified to state that market participants should maintain the ready capability to conduct background checks when circumstances warrant. Utilities typically conduct standard pre employment background checks to assist in employment decisions. However, a program for across-the-board, periodic, post employment, standard background security checks is not likely to reveal significant incremental information (e.g., terrorist affiliation, disgruntled work situation) that would be particularly useful in determining a person’s suitability to access critical cyber assets. In case of terrorist suspicions, the Federal Bureau of Investigation is far more qualified to conduct a meaningful investigation going beyond the standard background-check resources available to a utility. The background check program currently envisioned in the Cyber Security Standards would entail a significant expenditure of resources that would not be cost effective.

The NYTOs do not support the mandatory application of federal agency disqualifying criteria to personnel with access to critical cyber assets. The Standards provide no indication that such disqualifying criteria have been identified and analyzed for applicability. To the extent that such criteria would automatically disqualify a person from such access, they could be arbitrary and may conflict with New York’s strong public policy encouraging the employment of persons previously convicted of an offense that is not fundamentally related to the duties and responsibilities of the position (Executive Law, § 753).

To promote the security of electric operations when derogatory information is developed on an individual who has access to cyber facilities the Commission may want to require that each company should put into effect and follow internal adjudication procedures, consistent with applicable law and regulation, to expeditiously determine suitability for continued access. Language indicating that those who promulgate malicious acts toward the industry should be prosecuted to the full extent of the law, including prosecution by FERC and law enforcement agencies, adds no value to the Cyber Security Standards and should be deleted.

COMMENT: The Annual Compliance Checklist Should Be Revised To Reflect These Comments.

The NYTOs propose that the following items from the “Annual Self-Certification of Compliance with FERC Security Standards” work sheet be deleted or modified:

- “Critical asset administrators and operators have had background screening within last five years” — For reasons discussed in the comments, this language should be changed to “Background checks are conducted when circumstances warrant.”
- “Physical procedures for system security have been developed and implementation monitored for compliance” — This item should be clarified so as to refer to physical facilities associated with cyber security as follows: “Procedures for the security of physical facilities integral to cyber security have been developed and implementation monitored for compliance.”

North American Electric Reliability Council

IV. PART TWO — CYBER-SECURITY STANDARDS

NERC supports the Commission’s adoption of cyber-security standards. Wholesale electric grid operations are highly interdependent, and a failure of one part of the generation, transmission or grid management system can compromise the reliable operation of a major portion of the regional grid. Similarly, the wholesale electric market – as a network of economic transactions and interdependencies – relies on the continuing reliable operation of not only physical grid resources, but also the operational infrastructure of monitoring, dispatch and market software and systems. Because of this mutual vulnerability and interdependence, it is necessary to safeguard the critical cyber assets that support electric grid and wholesale market operations by establishing minimum standards for all those who participate in any way in electric wholesale market operations. Doing so will guard against a lack of cyber security for one critical asset compromising security and risking grid and market failure for the grid or market as a whole.

NERC’s Critical Infrastructure Protection Advisory Group (“CIPAG”) developed the draft security standards that were included as Appendix G to the Commission’s standard market design notice of proposed rulemaking. After reviewing the comments filed in response to the NOPR and based upon further discussion within the industry, the CIPAG is recommending changes to Appendix G. A draft of the revised Appendix G is included with these comments as Attachment A. These comments explain the significant revisions that NERC proposes for Appendix G.

A. Application

NERC recommends removal of the “Application” section from Appendix G and instead including a discussion of the applicability of the standards within the final rule itself. NERC, the CIPAG, and the CIPAG Working Group on SMD Cyber-Security Standards believe it is inappropriate for the standards to specify who may be subject to the standards. We believe this is more properly the responsibility of the Commission. Moreover, unnecessary confusion could result if there are any inadvertent differences between the Commission’s definition of entities subject to the standards and any such definition stated within the standards. For that reason, we have removed the “Application” section from the standards and inserted the term “Responsible Entity,” which we have defined as those participants in electric wholesale market operations that the Commission requires to comply with the cyber-security standards.

We recognize that the Commission does need to address the issue of who it intends to be subject to the standards. Thus, we suggest inserting the following new paragraph or its equivalent at an appropriate location within the final rule:

“These standards are intended to ensure that appropriate mitigating plans and actions are in place, recognizing the differing roles of each participant in the wholesale market and the differing risks being managed. Therefore, the cyber-security standards shall apply to any entity filing an SMD Tariff, and all other entities subject to filing a tariff with the Commission, that own or operate relevant systems and equipment as described in the cyber-security standards attached in Appendix G. These entities would be “Responsible Entities” as defined in Appendix G.”

B. Compliance

NERC recommends removing the “Compliance” section from Appendix G and instead including a discussion of compliance in the final rule itself. NERC, CIPAG, and the CIPAG Working Group on SMD Cyber-Security Standards believe it is inappropriate for the standards to attempt to define when the standards become effective, as that is clearly set forth in the SMD NOPR and should be included in the final rule as well. Moreover, there are important policy issues regarding initial implementation, notification and enforcement that are more properly the responsibility of the Commission. Therefore, we have removed the “Compliance” section from the standards. However, we believe that the Commission would benefit from the result of our discussion of these important issues.

First, there is serious concern about the timing of the first effective date for these standards. Many companies no longer have the ability to increase their 2003 budget for

additional equipment, software, or personnel that may be required in order to implement the standards by January 1, 2004. Second, most participants believed that there should be some process to bring noncompliant entities into compliance before their access to the wholesale market was terminated. This was most critical for the providers of transmission services, who cannot be replaced. There were also questions relating to the possible imposition of unnecessary breaches of contract if a noncompliant wholesale market participant were to immediately lose access to the wholesale market. A related, third, issue arose because wholesale market participants are undergoing rapid and (for the foreseeable future) continuing changes, such as mergers. A new corporate owner may have different cyber-security systems and procedures that may not easily be merged with those of a pre-existing company. Finally, all participants were concerned that self-certification forms that included specific information about particular issues of noncompliance could be released under the Freedom of Information Act (FOIA) or otherwise, thus becoming roadmaps to an attack. NERC also recognizes that the Commission from time to time may need to be able to review sufficient records to determine whether and to what extent there has been noncompliance.

In light of these considerations, NERC suggests inserting the following new paragraphs or their equivalent at an appropriate location within the final rule:

“The cyber-security standards shall become effective on January 1, 2004. However, the Commission notes that budgets for 2003, for many entities who shall be subject to these standards, have already been finalized. Thus, it is not appropriate to expect more than substantial compliance by January 1, 2004. Entities submitting their first annual self-certification may modify the form attached in Appendix G to reflect that circumstance. However, we do expect complete compliance by January 1, 2005. Further, we expect Responsible Entities to retain sufficient records to allow Commission staff to verify compliance with the cyber-security standards.’

“After January 1, 2005, if a Responsible Entity is at any time unable to certify to complete compliance, it shall immediately contact the Commission to apprise us of the situation and the entity’s plans for remediation. We shall treat all vulnerability information gathered during any such communication as confidential business secrets under the Freedom of Information Act. Failure to comply with the cyber-security standards may lead the Commission to impose remediation and/ or monitoring requirements, such as mitigating or compensating controls, that shall ensure compliance as soon as reasonably possible, and by some date certain. Continued noncompliance may lead to more severe Commission action, up to and including loss of direct access to the wholesale market.’

“The Commission recognizes that there may be a material change to the security environment of a Responsible Entity, separate and apart from a failure to comply with the cyber-security standards. This could arise from a major change in corporate structure, such as a merger, or a major change in business operations. In such cases, it may not be possible for a Responsible Entity to file its annual self-certification on January 1 of a particular year. Should such a major change occur, the entity subject to the required self-certification shall ask the Commission for an appropriate extension of the upcoming self-certification deadline.”

In order to implement the above language, we revised the self-certification form attached to the Cyber-Security Standards. (While some industry participants questioned the level of corporate representative that would be necessary or sufficient to sign the self-certification form, the form does not reflect a change in that respect.) We have also added a record-retention requirement to the standards themselves, at the end of the “Governance” section.

C. Definitions

NERC recommends addition of a Definitions section in Appendix G.

D. Electronic Security Perimeter

CIPAG has prepared the diagrams included as Attachments B-1 and B-2 to these comments to illustrate the concept of an electronic security perimeter. These diagrams are also available on the NERC web site as a PowerPoint file: “Electronic Security Perimeter Diagrams.ppt,” at <http://www.nerc.com/~filez/cipfiles.html>.

E. References

NERC recommends removal of the section “References” from Appendix G and instead including the following comments in the appropriate location in the final rule.

“The North American Electric Reliability Council (NERC) has established and maintains Security Guidelines for the Electricity Sector. NERC also provides a list of additional sources for security best practices. These references shall be helpful in developing organization-specific security standards and procedures for critical wholesale market resources.”

F. Self-Certification Form

NERC recommends changing the heading of the self-certification form at the end of Appendix G from “Annual Self-Certification of Compliance with FERC Security Standards” to “Annual Self-Certification of Compliance with FERC Cyber-Security Standards” as shown in the revised Appendix G.

NERC appreciates the opportunity to provide these comments on the SMD NOPR. We look forward to working with the Commission and the industry to ensure that the reliability and security of the bulk electric systems in North America are maintained as competitive markets evolve.

North American RTOs and ISOs

F. The RTOs and ISOs Endorse the Need for Security Standards

With respect to security, the Commission is proposing to establish “minimum standards for public utilities that own, control or operate facilities used for transmitting electric energy in interstate commerce as well as entities that use these facilities.”⁵ The standards would be administered through an annual self-certification.⁶

The RTOs and ISOs recognize the need for the establishment of security measures. Such measures cannot be static, but must be revised and refined, as the Commission has proposed to do, in light of changes in technology and operational experience.⁷ The Commission should, however, make clear that the ITP has no independent obligation to verify the accuracy of a self-certification submitted by market participants. As indicated below in the discussion of the need for pro forma tariff provisions limiting the liability of ITPs, any such obligation should not unfairly expose ITPs to additional potential liability in this area. Indeed, the Commission may want to consider whether such self-certifications should be filed directly with the Commission or some other appropriate governmental agency.

⁵ *SMD NOPR* at P 575.

⁶ *Id.* at P 576.

⁷ *Id.* at P 579.

Open Access Technology International, Inc.

IV.M System Security

Directed Comments

[¶579...When NERC revises the standards; the revisions will be filed with the Commission. The Commission will issue a Notice that it is considering revising the updated system security standards, and we will seek comments on the proposed changes.]

OATI strongly agrees with the Commission's stated role in noticing and soliciting public comment on all revisions to security policies or standards proposed by NERC. However, OATI believes the development of security standards should be subject to the standards review and delegation process as outlined in the NAESB-NERC Memorandum of Understanding and be mandated to be conducted in an open, fair, balanced, and inclusive process.

The self-certification process envisioned by NERC is a first step toward raising awareness of the extreme importance of cyber security and implementation of security policies within each organization. OATI is concerned, however, that the current self-certification form only asks the organization to identify that it has devised and assigned classifications to its cyber resources. At a minimum, organizations should be required to document their classification system and identify those systems that qualify under the security policy as critical resources. NERC may seek to take further responsibility over those organizations with direct responsibility for grid reliability and review the appropriateness of such classifications to ensure all "critical" systems have been classified as such.

The Security Standards in Appendix G represent a good start at raising the level of awareness that must be accorded to cyber security. The OSC has gone further in proposing a standard security infrastructure and protocol to be used in securing all OASIS Phase 2 transactions. This standard relies on current public-private key cryptology standards and implementation of a Public Key Infrastructure (PKI) governed by the provisions of the Certificate Policy for Energy Market Access and Reliability Certificates (e-MARC). The OSC has turned this proposed certificate policy over to the NERC Critical Infrastructure Protection Advisory Group (CIPAG) for review and development of an industry wide standard.

OATI believes very strongly that a method for strong mutual authentication of parties to a transaction (or any party-to-party communications) is absolutely essential to

secure the electric industry's cyber resources. For the most part, OATI endorses the principles embodied in the e-MARC policy. OATI has expended significant effort to establish itself as one, if not the first, industry participant offering services under the draft e-MARC certificate policy developed by the OSC. This effort is used across all OATI products and installed client base to raise the level of cyber security on OASIS, electronic tagging/scheduling, and OATI market systems. Without the ability for full participation by interested entities, the industry will be deprived of real-life implementation experiences--successes and failures--that are the result of applying similar security practices as those proposed within the authority delegated to NERC by FERC through the SMD NOPR § M, System Security and Appendix G, Security Standards for Electric Market Participants.

While OATI recognizes that industry participants such as the OSC have worked diligently to develop a draft of a possible industry-wide cyber security standard such as the e-MARC policy, OATI is concerned that such a policy will be implemented and enforced without fair, open, balanced and inclusive industry participation. In SMD NOPR § M, System Security and Appendix G, Security Standards for Electric Market Participants, open industry debate might only occur after the filing and noticing of new security standards with the Commission. OATI is very concerned that to date the NERC CIPAG process to define industry-wide security standards has not been open to participation by all interested industry participants, and feels very strongly that all industry participants must have the opportunity to be included in the process of developing these standards before they are filed with the Commission. OATI believes that the NERC CIPAG is the proper industry group to develop and implement such physical and cyber security standards envisioned within the SMD NOPR. However, OATI also believes that all such work by the NERC CIPAG must be fair, open, balanced and inclusive of all interested industry participants. The final results of the work of the NERC CIPAG, acting under the responsibility delegated to it by FERC, must be industry standards that are commercially viable and developed through fair, open, balanced and inclusive participation by all interested industry entities.

Finally, fundamental to the reliance on a public key infrastructure for secured communications are the policies and procedures established between parties and the level of trust that can be placed behind those policies and procedures, particularly with regard to the central role served by a third-party Certificate Authority. It is the adherence to these policies and procedures and the contractual obligations set in place between parties by the certificate policy, and not the cryptographic technology itself, that are the cornerstone of security. However, one cannot impose impractical and non-commercially viable policies and procedures on industry participants. Because of this reliance on trust, we suggest that all ITPs incorporate appropriate wording into each of their operating agreements that involve the electronic transfer of information that stress the need and obligation to

administer all terms and conditions of the contractual arrangements established under the e-MARC (or other adopted) certificate policy. Further, OATI feels there is a need for the electric industry to establish an independent organization having the responsibility to qualify entities supplying Certificate Authority services, audit such entities as required in the certificate policy, and oversee proper administration of all processes and procedures set by the certificate policy to ensure the level of trust needed across industry participants.

OATI fully supports the efforts of the OSC and CIPAG to champion the use of PKI and standardized protocols for the secure communications in OASIS, if such standards are developed in a fair, open, balanced, and inclusive environment that allows all interested parties to participate fully, and believes that these efforts must continue into the implementation of SMD as part of the standardized market participant interface.

Pacific Northwest Utilities

H. Security Provisions (P 575-79).

1. General Comments.

The Companies generally agree with the objective of increasing security for critical infrastructure. However, Appendix G does not specifically identify the "requirements" (*e.g.*, by reference to a specific version of a particular NERC standard) that would be applicable to a market participant. Nor is it clear that security requirements should be within the scope of any SMD rule at this time. NERC committees are working diligently to create a risk-based physical security methodology for utilities similar to the one proposed here. When a NERC proposal is complete, the Commission should issue a notice of proposed rulemaking, incorporating any specific NERC guidelines or other requirements the Commission proposes to adopt as system security standards.

If a final rule calls for a security plan to be immediately implemented but is not more specific about what the plan should include, it will be impossible to comply with and certify compliance, for the reasons set forth above. On the other hand, if specific requirements are specified for the first time in a final SMD rule, it will likely be impossible to comply within the time frame suggested in the SMD NOPR. Although the Companies currently have electric utility security programs that cover both physical security and information technology ("IT") security, significant investments in security equipment, staffing, and training for each utility would be necessary for both physical and IT security if various NERC recommendations were to become Commission requirements.

A compliance plan outlining good-faith compliance efforts and plans for completion of implementation efforts should be filed on a revised effective date of no sooner than the first January that occurs at least 12 months after issuance of the final order (presumably no earlier than January 2005). This time frame should allow participants a reasonable amount of time to plan for compliance, make any necessary changes, and prepare and conduct required training.

2. Compliance with Security Provisions.

A window of time should be allowed for participants to come into compliance. (As written, a participant would lose its access to the market immediately upon becoming noncompliant or when the officer of the utility indicates that the participant is not in compliance.)⁸ Moreover, some instances of noncompliance may be minor and correctable in a relatively short amount of time. Except in unusual circumstances, prompt corrective action should be the focus of the Commission's efforts.

3. Personnel Issues Raised by Security Provisions.

This section raises a number of labor law and employee-relations issues that are not covered by existing law. For example, utilities may have obligations under labor-relations laws that are incompatible with the proposal. Federal entities may have obligations under federal law that are incompatible with the proposal.

The SMD NOPR states that "individuals shall be disqualified from administering, operating or accessing critical assets if the individual meets any disqualifying criteria."⁹ A final SMD order would need to specify such disqualifying criteria and be coordinated with existing laws and treaties (*e. g.*, by ensuring criteria are lawful and avoiding duplication of existing U.S. Department of Energy requirements for maintaining detailed records for foreign nationals).

4. Access Control.

Key-card access for facilities should not be mandated without careful consideration. For example, key-card access may be less reliable under adverse weather conditions. Manual systems (handwritten logbooks) with physical locks and keys would seem to satisfy the requirement as written, if controls are put into place to require

⁸ SMD NOPR, Appendix G at 3.

⁹ *Id.* at 2.

forfeiture of keys upon reassignment or termination of employment.

More importantly, Appendix G should not put an undue emphasis on employee access, which historically has not proven to be a major risk factor. It is well recognized that the general public has access to transmission lines, and anyone wishing to harm critical devices within the substation may be able to do so without entering the perimeter.

5. Self-Certification of Compliance with Security Provisions.

Appendix G contemplates that an executive would certify, for example, that “[u]nauthorized personnel inside security perimeters are escorted at all times.”¹⁰ However, it would be impractical for an executive to answer “Compliant” to this question if he or she had to have personal knowledge of each visit by unauthorized personnel. Any certification contemplated by Appendix G should be revised to confirm that the policy exists and that, based on the certifier’s knowledge and belief, the policy has been complied with (or that follow-up action consistent with the policy has been taken with respect to failures to comply).

The Companies recommend rewording the checklist so that the focus is on implementation of appropriate policies rather than on whether, over a period of a year, there has been a single incident of policy breach. The Companies also recommend rewording checklist item 14 to be more consistent with the wording in the “Planning” section, as follows: “Development and testing of critical electric market systems are conducted on processors separate from production systems.”

PJM Interconnection, LLC

H. System Security (PP 575-79)

PJM endorses the comments filed by the joint RTO/ISOs concerning system security. PJM agrees with the Commission that it is appropriate to prescribe minimum security standards for public utilities that own, control, or operate facilities used for transmitting electric energy in interstate commerce as well as entities that use those facilities. Standards to safeguard transmission systems are particularly important in light of recent events.

The Commission’s security proposals would benefit from the following

¹⁰ *Id.* at 2.

clarifications. First, PJM recommends that the Commission add language to the self-certification provisions to state that the self-certification forms shall be kept confidential by both the ITP and the Commission. Allowing self-certification forms to be accessed by the public could provide an unintended roadmap for unauthorized access to critical transmission facilities.

Second, the Commission should clarify that the ITP does not have an independent obligation to verify the accuracy of self-certification forms submitted by market participants. To require ITPs to verify self-certified data of this type unreasonably could expose ITPs to liability. Verification, if any, of the accuracy of market participants' self-certification forms should be the responsibility of an appropriate government agency.

Finally, the Commission should clarify that testing of electric market systems may be conducted in system environments with logical separation from operational systems and appropriate security controls in place. The proposed language in Appendix G requiring testing in environments that are "not interconnected" with operational systems is too restrictive and would require unnecessary and costly architectural charges in existing environments.

PSEG Companies

M. System Security Issues

The NOPR states that system security is critical and proposes to implement standards for system security that would be observed by industry entities¹¹. The PSEG Companies agree that system security is critical; however, it is equally important that any new security standards not unduly interfere with or disrupt the operations of wholesale power markets.

The Commission has proposed adopting the North American Electric Reliability Council's ("NERC") recently-recommended minimum requirements for securing information assets that support grid reliability and market operations.¹² The NOPR proposes that transmission providers make an annual self-certification in a form attached to the NOPR as Appendix G and that customers must demonstrate that they have a basic security program in place to be eligible to receive transmission service.¹³

¹¹ SMD NOPR at ¶¶ 575-579.

¹² SMD NOPR at ¶ 576.

¹³ SMD NOPR at ¶¶ 576-577.

The PSEG Companies have several concerns about this aspect of the SMD NOPR. First, the proposed standards would apply to all sectors of the power industry, imposing significant costs. However, it is unclear in the NOPR whether NERC or the Commission has done any cost analysis with respect to the proposed security standards. Any standards that would impose significant new costs may have negative market implications. In this vein, it is unclear that NERC is the proper entity to develop the standards, because its focus is on bulk power system reliability. Moreover, the proposed standards largely involve computer system security – both hardware and software. The Commission has recently endorsed the North American Energy Standards Board (“NAESB”) as the preferred organization for established business standards and protocols for the wholesale electric industry.¹⁴ NAESB’s forte is developing such information technology standards for the industry. Accordingly, it would be more appropriate for the Commission to direct NAESB to develop security standards, rather than NERC.

In sum, the Commission should adhere to the following principles in the system security standards it may adopt in its Final SMD Rule. First, it must ensure that the standards are the minimum practicable to accomplish their purpose, with minimum financial and operational impact on the market. Second, it should ensure that requirements are equally applicable to all covered entities. Finally, the Commission should insure that standards are clear and performance is measurable against objective criteria, to minimize the risk of liability in event of an incident with subsequent claims for damages alleging negligence or failure to take adequate measures to ensure security.

Reliant Resources, Inc.

System Security

The NOPR recognizes that wholesale electric grid operations are interdependent and that the failure of one element (e.g., a generator) can compromise the reliable operation of a large portion of the system. The NOPR further recognizes that the reliable operation of the grid depends on computer software and systems and that it is necessary to establish minimum standards for protecting these information assets. The NOPR proposes that all public utilities that have tariffs on file with the Commission and the customers that use those tariffs must self-certify that they have met the standards established by NERC’s Critical Infrastructure Protection Advisory Group.

¹⁴ See Electricity Market Design and Structure, Order on a Standards Development Organization for the Wholesale Electric Industry, issued May 16, 2002 in Docket No. RM01-12-000; Order Providing Guidance on the Formation of a Standards Development Organization for the Wholesale Electric Industry, 97 FERC ¶ 61,289 (2001). NAESB’s wholesale electric quadrant is now fully-constituted and operational.

RRI agrees that the terrorist attacks of September 11, 2001 require that additional security measures be implemented in order to protect the national electric grid from attack. RRI wholeheartedly supports the self-certification process contained in the NOPR and urges the Commission to implement the proposal in the Final Rule.

Southern California Edison Company

M. System Security

The NOPR recognizes that NERC's Critical Infrastructure Protection Advisory Group (CIPAG) had developed a set of recommended minimum requirements (Standards) for securing information assets that support grid reliability and market operations and the physical environments in which these information assets operate. NOPR at ¶ 576. Such Standards would be administered through an annual self-certification due January 31, 2004, and every January 31 thereafter. FERC proposed to require that all public utilities that have tariffs on file with the Commission must file the self-certification by January 31, 2004, and every January 31 thereafter. Id. at ¶ 577.

Additionally, on and after February 1, 2004, as a condition of receiving transmission service provided by a public utility, a customer must demonstrate that it has a basic security program in place. The customer can satisfy this requirement by supplying the public utility with a copy of the executed self-certification form. Id. The draft Standards included in the NOPR, however, were not properly reviewed and are being revised substantially by Security Committee representatives from NERC and EEI.

The Final Rule should acknowledge that the inclusion of the draft Standards was premature. SCE has attached, as Exhibit 1, a draft of relevant documents being developed by NERC, EEI and others, which include comments on the security provisions of the NOPR and the revised Standards. SCE understands that Exhibit 1 is currently being re-drafted to incorporate changes suggested by FERC Staff. SCE has been an active participant in the NERC/EEI process and understands that the changes proposed to date are consistent with the framework described in the draft in Exhibit 1. Because the revised draft is not yet available to SCE, SCE's has included a previous version of the draft comments, for informational purposes only, to indicate our support for the NERC/EEI work product. SCE expects to be able to support the NERC/EEI final work product, but reserves its rights to comment until the proposal is finalized.

Southern Company Services, Inc.

D. System Security.

Southern Companies have several concerns related to the system security proposals. See SMD NOPR at PP 575-580 and Appendix G. Southern Companies agree that minimum standards should be developed for securing information assets that support grid reliability and market operations. Southern Companies support industry development and adherence to those standards, but the Commission should not otherwise become involved in prescribing system security standards. In addition, the development and deployment of minimum standards is not feasible in the time frames described in the NOPR, in particular because of budget and training considerations. Thus, “cyber” security standards should be considered separately from the SMD NOPR. Southern

Companies are also concerned about providing information without an exemption from FOIA requests. Absent such an exemption, security for critical systems and infrastructure could be significantly compromised.

The NOPR also needs to recognize and differentiate between general IT systems and control systems. The current control systems, which often operate in real-time or near real-time, do not have adequate access control mechanisms, and the use of any type of encryption would dramatically impact the reliability and timeliness of data for monitoring and control. Simply put, imposing security on such generation control systems could prevent their ability to engage in real-time or new real-time operations. The Commission should thus provide clarification on security measures applicable to IT systems as opposed to control systems. In addition to these concerns, the control system vendors must become involved and develop the next generation of control systems to meet the new security requirements.

Finally, particularly regarding the standards set out in Appendix G, the Commission provides no clarification regarding what constitutes “critical resources,” and it fails to require participants to define which cyber assets are critical for wholesale market operations. Also, because the vendors of such control systems do not always support the system management procedures related to disabling services and patch management, participants may have difficulty ensuring the reliability of the control systems in question. This situation is difficult to address and may not allow compliance with the SMD NOPR’s standards.

TXU Operating Companies

L. System Security

NERC’s Critical Infrastructure Protection Advisory Group has recently developed a set of recommended minimum standards for securing information assets that support grid reliability and market operations and the physical environments in which these

information assets operate. The Commission proposes to require that all public utilities that have tariffs on file with the Commission must file the self-certification by January 31, 2004, and every January 31 thereafter.

TXU agrees that a requirement to certify system security should be included in SMD, but this requirement should allow for regional flexibility in implementation so long as the result is a secure grid system. In addition, TXU suggests that the Commission require that market settlements be run separately from system operations. In the event that the market operations system is attacked or fails, the transmission grid can continue to operate until the market system is restored.

United States Department of The Interior (Bureau of Reclamation)

3. Security Issues

The Federal agencies currently have a robust electric utility security program that covers both physical security and Information Technology (IT) security. Reclamation is working with other utilities and industry groups to create and implement common security standards.

Consequently, Reclamation has concerns about the timing of any security requirements in the proposal. For example, the physical security requirements of the SMD may be premature since National Energy Regulatory Committee (NERC) committees are working diligently to create risk-based physical security methodology for utilities similar to the proposal.

Wisconsin Electric Power Company

G. System Security -- Appendix G

Wisconsin Electric supports the System Security Standards as proposed by the Commission, as well as security and compliance reviews for critical energy infrastructure components. It is appropriate for the North American Electric Reliability Council ("NERC") to be developing these standards. Some of the details, definitions and timeframes for compliance still need further development, however. Additionally, Wisconsin Electric offers the following comments on the noted sections below:

Page 1, "Purpose": There is confusion over what "market software and systems" (Line 6) includes. "Market resources" and "market assets" referenced later in the appendix (Line 8) causes the same confusion. Wisconsin Electric requests that the Commission clarify what it intends for the meaning of these terms.

Page 3, “Application”: In certain circumstances, Wisconsin Electric has the capability to electronically dispatch power from a few power plants that are not owned and operated by Wisconsin Electric. We ask the Commission to clarify that the owners of these particular power plants will be responsible for compliance to these security standards.

Page 4, “Security Scope”: Wisconsin Electric requests that the Commission clarify that “security perimeter” only applies to the cyber asset locations and the connectivity to these assets that is owned by Wisconsin Electric.

Page 4, “Asset Classification and Control”: This section is not required based on the controls that are proposed for cyber assets located in the security perimeter in the second paragraph of “Security Scope.” The programs, policy and standards developed to protect market functions inside the security perimeter will determine criticality. Wisconsin Electric requests that the Commission remove this section due to its redundancy.

Page 5, “Personnel”: Wisconsin Electric requests that the Commission consider using the following parameters for establishing the “security perimeter:” Security perimeter (cyber assets locations) should encompass computer rooms, access points into these rooms, electrical and backup service to these rooms, and communication feeds. Security perimeter (cyber assets connectivity) shall also encompass ID/password requirements and controls for computer connectivity to cyber systems noted here. The development of a security program will be for the users of systems within the security perimeter. This includes security awareness training.

Due to local, state, labor union, and other jurisdictional laws, Wisconsin Electric requests that the Commission find that background checking for administrators and operators should be left up to each company’s internal administrative procedures.

Page 6, “Systems Management”: Wisconsin Electric requests that the Commission reword item 1) to read: “Have a documented password security policy that is enforced for all cyber assets located in the security perimeter.”