NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

Permanent Cyber Security Standard – SAR Drafting Team

August 21, 2003
8 a.m.–4 p.m.

NERC Office
116-390 Village Boulevard
Princeton, NJ 08016

Meeting Agenda

1. Welcome and Administrative Items
2. Review Conduct of Meeting — Participation of Guests
3. Review Role and Responsibilities of SAR Drafting Team
4. Review Comments received on Urgent Action Cyber Security Standard and Standard Drafting Team Responses
5. Discuss Comments Submitted on Permanent Cyber Security SAR and Draft Responses
6. Revise SAR
7. Summarize Action Items and Next Meeting Date
8. Adjourn

Cyber Security SAR Drafting Team Roster

Michael Allgeier
Data Security Officer
Lower Colorado River Authority (LCRA)
3700 Lake Austin Blvd.
Austin, TX 78703
Office Telephone: 512 473-3200 ext. 2449
Mobile Telephone: 512 779-6459
Fax:
Michael.allgeier@lcra.org

David Ambrose
SCADA System Manager
Western Area Power Administration – Rocky Mountain Regional Office
5555 E. Crossroads Blvd.
Loveland, Colorado 80538
Office Telephone: 970-461-7354
Mobile Telephone: 970-980-6831
Fax: 970-461-7213
ambrose@wapa.gov

Larry Bugh
Manager, Information Technology
ECAR
220 Market Ave. S., Ste 501
Canton, OH 44702
Office Telephone: 330.580.8017
Mobile Telephone: 330.704.0716
Fax: 330.456.5408
larryb@ecar.org

Greg J. Fraser
Manager, System Support Department
Manitoba Hydro
System Support Department
Box 815
Winnipeg, MB Canada R3C 2P4
Office Telephone: (204) 487-5379
Mobile Telephone:
Fax: (204) 487-5394
gjfraser@hydro.mb.ca

Roger L. Lampila
IT Security Administer
New York Independent System Operator
3890 Carman Road
Schenectady, NY 12303
Office Telephone: 518 356 6043
Mobile Telephone: 518 475 7843
Fax: 518 356 6118
rlampila@nyiso.com

John S.F. Lim, CISSP
Systems Manager
Consolidated Edison Co. of New York, Inc.
4 Irving Place, Room 349-S
New York, NY 10003
Office Telephone: 212-460-2712
Mobile Telephone: 917-690-5406
Fax: 212-387-2100
limj@coned.com

John G. Maguire
Senior Security Analyst
PJM Interconnection, LLC
955 Jefferson Drive
Norristown, PA 19403
Office Telephone: 610-666-4420
Mobile Telephone: 610-633-8109
Fax:
maguij@pjm.com

Paul McClay
Manager of Information Security
Tampa Electric Company
PO Box 111, Tampa, FL 33601
Office Telephone: 813-225-5287
Mobile Telephone: 813-376-2340
Fax: 813-225-5302
pfmcclay@tecoenergy.com

Kurt Muehlbauer
Manager of Information Assurance
Exelon Corporation
227 West Monroe, Room 1056
Chicago, IL 60606
Office Telephone: 312.394.3772
Mobile Telephone:
Fax: 312.394.8888
kurt.muehlbauer@exeloncorp.com

David L. Norton, CISSP
Sr. Information Security Analyst
Entergy Transmission
639 Loyola Avenue, MS: LMOB17A
New Orleans, LA 70113-3125
Office Telephone: 504-310-5763
Mobile Telephone: 504-237-5657
Fax: 504-310-5762
DNORT91@entergy.com

Cyber Security SAR Drafting Team Roster

James Sample
Manager of Information Security Services
California ISO
151 Blue Ravine Road
Folsom, CA 95630
Office Telephone: 916-608-5891
Mobile Telephone: 916-802-7537
Fax:
jsample@caiso.com

Phil Sobol
Cyber Security Specialist
Aquila, Inc.
20 W 9th, Kansas City, MO 64105
Office Telephone: 816-467-3303
Mobile Telephone:
Fax: 816-467-3238
phil.sobol@aquila.com

Howard Tarler
Chief, Bulk Transmission Systems Section
New York State Dept. of Public Service
3 Empire State Plaza
Albany, NY 12223-1350
Office Telephone: 518 486 2483
Mobile Telephone: 518 441 3878
Fax: 518 473 2420
Howard_tarler@dps.state.ny.us

John D. Varnell
Manager of technology
Tenaska Power Services Co.
1701 E. Lamar Blvd.
Arlington, TX 76006
Office Telephone: 817-462-1037
Mobile Telephone: 817-312-7261
Fax: 817-462.1035
jvarnell@tnsk.com

William R. Wagner
IS Director, Information Security and Business Continuity
Calpine Corporation
104 Woodmere Road
Folsom, California 95630
Office Telephone: 916-608-3799
Mobile Telephone: 916-716-2511
Fax: 916-294-0921
wwagner@calpine.com

Bob Wallace
Manager–IT Security
Ontario Power Generation
700 University Avenue
Toronto, Ontario, Canada
M5G 1X6
Mail Stop: H10 D11
Office Telephone: (416) 592-8297
Mobile Telephone: (416) 988-3244
Fax: (416) 592-5514
Bob.wallace@opg.com

Chuck Noble
Requestor
ISO New England
One Sullivan Road
Holyoke, MA 01040
Office Telephone: (413) 540-4232
Fax: (413) 535-4109
cnoble@iso-ne.com

Lou Leffler
Staff Coordinator
North American Electric Reliability Council
116-390 Village Boulevard
Princeton, NJ 08540
Phone: 609-452-8060
Fax: 609-452-9550
Lou.Leffler@nerc.net

Lynn Costantini
Staff Coordinator
North American Electric Reliability Council
116-390 Village Boulevard
Princeton, NJ 08540
Phone: 609-452-8060
Fax: 609-452-9550
Lynn.Costantini@nerc.net

Responses to comments submitted during the balloting of the urgent action cyber security standard

The cyber security standard drafting team thanks all those who submitted comments with their ballots on the urgent action cyber security standard. After careful review and consideration of all comments received, the drafting team still believes it is appropriate to move forward with the recirculation ballot of this standard. This course of action dictates that the standard be posted, unchanged from the version posted for the first ballot, for the recirculation ballot. In response to the comments, changes have been made to the implementation plan for this standard to clarify what NERC intends to do with respect to compliance with the standard.

Many of the comments submitted will be very helpful in drafting a permanent and more detailed cyber security standard. All comments received during the development of the urgent action standard will be forwarded to the drafting team that will soon be working to develop a permanent cyber security standard.

Registered members of the standard ballot pool for the urgent action cyber security standard are encouraged to review the comments below and the responses of the drafting team before casting their vote in the recirculation ballot. For ease of review, a summary of commonly raised issues appears first. Specific answers to each comment follow the general responses, organized alphabetically by the commenting entity.

List of most commonly raised issues:

1) Compliance plan
2) Ambiguity in the standard
3) Coordination with other requirements
4) Personnel and background checks
5) Use of Urgent Action Provision
6) Incident response and reporting
7) Applicability
8) Definition of critical cyber assets

Compliance Plan

Numerous comments were received regarding compliance with this proposed standard. General responses to these comments follow.

Compliance Monitor

The NERC Compliance Enforcement Program (CEP) comprises the ten Regional compliance enforcement programs. As with other standards included in the NERC CEP, the Regions would have responsibility for monitoring compliance with this standard. Each Region is therefore the compliance monitor and would be responsible to monitor compliance of its members.

Substantial or Partial and Full Compliance

NERC has not attempted to define ‘substantial compliance’ and we recognize that full compliance by all entities is not a reasonable expectation during the first year of the implementation of this standard. However, NERC’s goal is to have full compliance with all of its standards in order to preserve the reliability of the bulk electric systems of North America.

Compliance assessments for this standard will be conducted via self-certification. The determination of compliance with this standard, whether partial, substantial, or full, is therefore the responsibility of each entity completing a self-certification. No penalties, sanctions or letters will be issued in response to entities self-assessing themselves as non-compliant with this standard in 2004. Aggregated information listing the number of compliant and non-compliant entities will be shared with NERC. No individual entity compliance information will be included. Regional compliance monitors will treat all self-assessments as confidential.

Please see the detailed implementation plan for this standard, available at:
http://www.nerc.com/~filez/standards-cyber.html

Effective Date of the Standard for Compliance

The first self-certifications of compliance with this standard will be due during the first quarter, 2004.

Penalty Matrix, Financial Penalties, or Other Sanctions

Several commenters indicated confusion about the inclusion of the NERC penalty matrix with the proposed standard. Further, several commenters indicated confusion about issuing of letters of non-compliance. It was noted in each sanctions section of the standard that this matrix was included for reference only. The sanctions section of each requirement within the standard indicated that there would be no financial penalties assessed for this standard, but that letters of non-compliance would be issued. However, in recognition that cyber security is an issue for which NERC does not currently have any requirements, the implementation plan associated with this standard states that NO sanctions (monetary or letters) will be issued in response to non-compliance self-reported in 2004.

The purpose of including the penalty matrix in this proposed standard was to explain the potential distribution of letters of non-compliance to the standard, should the standard be extended for a second year. Letters of non-compliance will not be issued in response to the initial self-certification. This standard will be valid for only one year following NERC Board adoption, unless the standard is extended for one additional year. It would only be in the second year that the potential exists for the issuance of letters of non-compliance, but no financial sanctions would be imposed. As noted, a new implantation plan associated with the extended standard would be developed should there become a request for extension.

Confidentiality of Compliance Assessments and Audits

Several comments expressed a concern over the confidentiality of the compliance assessment results. This is a broad issue of concern to NERC, and is not specific to this standard.

To address this concern, the NERC Compliance Enforcement Program treats individual entity results as confidential information, known only to the regional compliance monitor. Each compliance monitor has established non-disclosure provisions within its compliance enforcement program to ensure that sensitive information is not released.

Comments were received expressing concerns over the release of information through the Freedom of Information Act (FOIA) provisions. NERC and its compliance monitors are not subject to the Freedom of Information Act.

Comments were also received expressing a desire to have any self-certification or other compliance information related to this standard protected under FERC Order 630 as Critical Energy Infrastructure Information (CEII). FERC Order 630 only applies to information filed with the FERC. NERC does not

intend to file with FERC any specific information related to individual entity compliance with this standard.

Submitting Multiple Reports

NIST and other standards were considered during the development of the proposed cyber standard. The NERC standard does not conflict with currently existing standards developed by other organizations. Compliance with the NERC standard will require that responsible entities complete a self-certification form developed by the compliance monitor, even if such an entity meets NIST requirements.

Document Development

Some comments were received expressing concern over developing the necessary documentation to support an audit ensuring protection of critical cyber assets related to the reliability of the bulk electric system.

The standard requires documentation to demonstrate compliance that should be readily available (given confidentiality concerns) within any corporation practicing due diligence to protect their critical cyber assets from a cyber attack. The development of new documentation to comply with this standard is not anticipated. No audits will be conducted in 2004.

Record Retention

Some comments expressed concern over the record retention requirements. With the implementation of this standard on an urgent basis, much will be learned about record retention for the various types of information. Lessons learned will be used in the development of the final cyber security standard.

Document Tracking for Updates

A comment was received concerning the ability to track updates of specific documents and how compliance with this requirement would be measured. While this is not an issue for the urgent action standard, as it will be replaced after one year, this will be considered in the development of the permanent standard.

Audits of Compliance

As stated in the implementation plan (available at: http://www.nerc.com/~filez/standards-cyber.html), no audits will be conducted in 2004.

Subjective Interpretation by the Compliance Monitor

Some comments were received expressing concern regarding the possible conflict that could result as the result of a compliance audit. Specifically, the comment raised the possibility that a company may find itself at one level of compliance while an auditor may find it at another.
This is a broad issue, applicable to all NERC standards. To address this concern, each Regional compliance enforcement program has developed a dispute resolution procedure which can be implemented should such a situation occur. Because no audits will be conducted for this standard in 2004, this is not a concern in this case.

Reporting Burden

One comment was received expressing concern that this standard will require the time of high-level security personnel, which is an ineffective use of their time.

In the case of this standard, completing a self-certification annually should not significantly burden high-level security personnel, yet it will provide the opportunity to assure themselves and their organization that the protection of critical cyber assets is meeting the standard.

Role of the Regions

NERC's Regions will act as compliance monitors for this standard, as stated in the implementation plan for this standard.

Field Test for Urgent Action Standards

One comment suggested that a field-test period should be allowed for an urgent action standard. The purpose of a field test is to test the provisions of the standard as well as the compliance monitoring aspects, through formal compliance reviews and audits. As such, the use of a field test conflicts with the use of urgent action for the development of emergency standards.

Standard is Document Based not Performance Based

One comment expressed concern that parts of the standard were based on providing documents rather than on actual performance.

Indeed, some parts of the standard, such as those requiring a documented cyber security program, are document based. Others, such as those requiring that physical and electronic protection be implemented at all times, are performance based.

Both types of standards are needed to maintain reliability. One type looks at the preparedness for a cyber attack while the other is looks at actual implementation. If performance was the only measure, bad performance may only be discovered after a cyber attack has occurred and reliability has been impacted.

Ambiguity in the Standard

One of the most frequently voiced criticisms of the proposed cyber security standard is that the standard is "too vague," and not prescriptive enough to allow for adequate planning, budgeting or implementation.

The intent of this standard is to create a set of minimum cyber security requirements that can be consistently implemented in a timely manner to protect the reliability of the bulk electric system. The overriding feature of the standard is that although it mandates security, it does so with maximum flexibility to account for differences in the types of entities in the electricity industry and the cyber systems they employ.

This standard is purposely not a "how to" document. The standard is in concert with generally accepted best practices (e.g. the NERC Cyber Security Guidelines, NIST Standards, ISO17799 Standard) and represents a common sense, proactive, first-step approach to cyber security across the industry. As a permanent standard is developed it is natural to expect that much more specificity will be included.

A number of comments centered on the perceived lack of industry input to the standards development. The root of the standard was the Federal Energy Regulatory Commission's (FERC) Notice of Public Rulemaking: Standard Market Design, Appendix-G, as revised by the NERC Critical Infrastructure Protection Advisory Group (CIPAG).

The FERC published Appendix-G for industry review and comment over an extensive period during the summer-fall 2002. NERC's Board of Trustees and FERC endorsed CIPAG's suggested revisions to Appendix G. CIPAG's revised Appendix G was the subject of two FERC Technical Conferences (winter 2002–03). The Cyber Security Standard Drafting Team used this material as the genesis for NERC's proposed Cyber Security Standard.

Coordination with Other Standards

Commenters noted that some existing cyber "standards and best practices" (e.g. NIST and ISO) may actually go beyond the NERC cyber security standard. Specifically, if an organization meets the more stringent requirements of another organization, must it also comply with the NERC standard? Yes, compliance with the NERC standard would be required with the applicability understandings stated in these responses. The NERC standard is intended to provide an achievable level of cyber security for the defined critical cyber assets.

Another comment suggested that the electricity industry could wait for promulgation of a cyber security rulemaking. As stated in the section on Ambiguity the NERC Cyber Security Standard essentially is the FERC envisioned rulemaking. The FERC has essentially accepted this approach as a good step in their intended direction toward cyber security. NERC expects the FERC to include the NERC Cyber Security Standard in their rulemaking by reference.

NERC's Critical Infrastructure Protection Advisory Group (CIPAG) proposed this draft standard for urgent action in the NERC standards development process because it believes that the electric industry needs to take action now to increase its cyber security and that the timing of a final FERC rule for a standard market design, as well as its schedule for implementation, is uncertain.

Personnel and Background Checks

Commenters generally agree that it is appropriate to maintain up to date access lists and to remove people when they no longer need access to critical cyber systems. Although not mentioned in the standard itself, they support the need for immediate termination of such access when a person has been involved in misconduct or demonstrates mental instability or other behavior suggesting that they may pose a threat to the system. However, given the broad scope of persons to whom this could apply, there was a strong concern that the 24 hour requirement was inappropriate and impractical particularly if such access was terminated after hours, on weekends, or involved contractors (including programmers, IT support, or even janitorial staff) where the system owner/operator may not even be aware of that employment change for an extended period of time in excess of the 24 hour window.

NERC acknowledges the validity of these comments and will address them more fully in the final standard. In evaluating initial compliance as discussed under the heading Compliance Monitor, we will expect that a system will be in place to periodically update access authorization lists on at least a quarterly basis. That protocol will also ensure that access be suspended as soon as possible and no later than 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems. Routine administrative changes resulting from retirements, resignations, leaves, etc. should be handled within the normal course of business but not in excess of three business days after occurrence. In the case of contractor/vendor employees, they shall be required to promptly advise the system owner/operator when such changes occur and system access should be updated as soon as practical but no later than three business days after notification.

Many comments were received on the requirement for background screening. The general concern was that they were unclear as to who was covered under this requirement. There was concern that such screening could, in some cases, conflict with collective bargaining agreements. There was concern for lack of consideration to "grandfathering" of existing employees.

NERC acknowledges that the standard, as drafted, does not specifically reference bargaining agreements. However, such agreements are generally covered under State law and particularly under Federal labor laws such as the National Labor Relations Act. Moreover, the ultimate legal authority in this area is the Federal Fair Credit Reporting Act, which defines the rights of employers in terms of background investigations conducted for prospective and even existing employees.

The vast majority of American organizations conduct background investigations for prospective new employees consistent with the Fair Credit Reporting Act. Such investigations generally confirm prior employment and education, a driving history and criminal conviction check, and even credit history where appropriate. There is an existing NERC security guidance document on conducting background investigations to help organizations develop protocols in this area.

This standard will require that organizations, at a minimum, conduct investigations of new employees upon entering employment where they could have access to critical cyber systems. While they are free to do so, this standard is sufficiently generic that organizations are NOT required to conduct background investigations of existing employees given the fact that they have had the opportunity to observe and evaluate the behavior and work performance of those employees after they have been employed for a period of time.

Certainly the scope of a background investigation should be adjusted based on the level of access that people have to critical cyber assets.

There was also concern expressed regarding the ability to perform timely background screening for third party personnel who performed infrequent and/or emergency visits, particularly off-hours and weekends. This could include computer vendor maintenance personnel, plumbers, electricians, etc., where the individual assigned to respond may not be known far enough in advance to perform screening.

NERC recognizes the important role of third party emergency services in maintaining the reliability of bulk power system operations. The requirement for background screening is to provide a level of assurance that only trustworthy individuals are granted unsupervised access to critical cyber assets. Therefore individuals without a background screening must be escorted at all times during the period of access inside the security perimeter.

Use of Urgent Action Provision

Under certain conditions, the NERC Standards Authorization Committee (SAC) may designate a proposed standard or revision to a standard as requiring urgent action. Urgent action may be appropriate when a delay in implementing a proposed standard or revision can materially impact reliability of the bulk electric systems. The SAC must use its judgment carefully to ensure an urgent action is truly necessary and not simply an expedient way to change or implement a standard. Only the SAC, on a request-by-request basis, can approve such requests.

A request for urgent action is a valid part of NERC's ANSI accredited standards development process.

The use of the **Urgent Action** process for the cyber security standard, which was unanimously endorsed by the SAC in April 2003, is justified for the following reasons:

1. There is a recognition that companies subject to this standard will have varying amounts of work required to become compliant with a very minimum set of cyber security requirements. In some cases, budget authority will be required before the necessary expenditures can be made, necessitating an annual budget cycle process. For this reason, the Urgent Action standard proposes to not require immediate full compliance with all requirements. In the mean time, critical cyber assets continue to be exposed to vulnerabilities and exploits as evidenced below. To delay start of an implementation program for the 18 months to two years it will take to put a permanent standard in place serves only to unnecessarily continue exposing the critical systems to risk of attack and compromise. The proposed Urgent Action cyber security standard will get companies moving in the right direction while the permanent standard is perfected through the collaborative commenting and voting process. By the time the final standard is approved, all companies subject to the interim standard should be well positioned to fully meet the requirements of the permanent standard with little, if any additional effort required. More importantly, two years have not been lost getting to this point. If the interim standard is not approved, the delays resulting from the standard approval process will push out full compliance until at least 2007. We cannot afford to wait that long to put a common set of minimum-security requirements in place.

2. Over the past two years, there have been a number of cyber incidents that have or could have directly impacted the reliable operation of the bulk electric system, including the following:

    a. The most recent incident was on January 25, 2003, when the SQL/Slammer worm devastated companies the world over. The Electricity Sector Information Sharing and Analysis Center, with assistance from cyber security experts from the CIP Advisory Group, investigated a known instance where an electric utility company lost control of their EMS/SCADA system for several hours. While nothing serious happened as a result, the EMS/SCADA system was not able to communicate with substations and plants, forcing the company operations staff to resort to manual operation of their transmission and generation assets until control could be restored. By the company's own admission, this incident would not have happened if the requirements of the proposed Urgent Action standard had been implemented.

    b. In September 2001, the Nimda worm was circulated widely throughout the world. We know of an electric utility whose EMS/SCADA network was compromised by the Nimda worm. The worm then propagated itself to the internal project network of a major EMS/SCADA vendor via the vendor's support communications circuit, devastating the EMS vendor's internal network and launching further attacks against the EMS/SCADA networks of all other customers of the vendor with support communications circuits.

    c. In August 2001, the Code Red II worm successfully compromised the internal network of a company that provides services to NERC and numerous electric utility companies. This worm then attacked the connected customers of this company, successfully compromising an exposed web server at one of the utility control centers. It is important to note that the compromised server was presumed to be protected, as it was not exposed to the Internet. This attack was propagated via the private frame relay network connecting the service company, the impacted utility, and the other connected utility companies.

3. In February 2003, Symantec issued a report claiming that in the last half of 2002, the Power and Energy sector suffered more cyber attacks (average per company) than any other sector and that 70 percent of the attacks were rated as severe. There is little supporting documentation to confirm this statistic or to identify whether critical assets were being attacked, however it is consistent with other published and generally accepted reports of cyber activity. More telling is a report issued in May 2002 by the Critical Infrastructure Assurance Program claiming that there was evidence of a coordinated cyber reconnaissance effort directed against the critical assets of at least two electric utilities participating in the Department of Defense-sponsored program. The report and follow-up discussions with the CIAP personnel revealed that the probing appeared to come from the People's Republic of China, Hong Kong, and South Korea, with each probe building upon information previously garnered. Even if all of the attacks actually originated in Chicago, it is significant to note that the critical assets of the affected companies were being targeted.

Incident Response and Reporting

General Comment:

Incident Response is different than Incident Reporting. All entities should have in place Incident Response procedures covering all aspects of the response required for any kind of failure, whether natural or malicious. The intent of Measure 2.1 for requirement 1214 (Electronic Incident Response Actions) and 1215 (Physical Incident Response Actions) is to ensure that these incident response plans are in place. Incident response plans for "naturally" failed disks and routers are as important as incident response plans for obvious malicious events. There should even be an incident response plan for spurious reboots and memory lock-ups of critical computers.

Measure 2.2 for requirement 1214 and 1215 deals with whether to report the incident once it has been responded to. The referenced document NERC-NIPC Indications, Analysis, and Warnings Program Standard Operating Procedure (IAW) is a voluntary program, intended to provide information on known malicious or unknown cause events. This document does not require mandatory reporting of incidents. What IS required in measure 2.2 is that for each incident class, a conscious decision is made as to whether to report the incident. The class of incident is not as important as the reason for the incident. Is it possible for a router to fail due to malicious causes? Is it possible for a disk to fail because of a virus on the host computer? It probably is in both cases, but it is not a foregone conclusion in either case. Measure 2.2 requires that the applicable processes be put in place to require that the reporting decision be made, and not to let the reporting decision fall through the cracks because the entity didn't think it was important enough to report.

We should in the next version of the standard include a definition for "Reportable Cyber Security Incident" to further clarify the difference. A Reportable Cyber Security Incident is a Cyber Security Incident that is of known malicious cause or where there is reason to suspect that the cause might be malicious.

Applicability

Q: How do I know if this standard applies to my company?

A: The standard is written at a high level and must accommodate numerous types of entities across North America. For this reason, it is not possible to tailor the standard to address specific entities. Any entity performing the reliability authority, balancing authority, interchange authority, transmission service

provider authority, transmission operator, generator or load serving entity function, as defined in the NERC Functional Model, who also has critical cyber assets must comply with the standard.

The implementation plan associated with this standard states that only control areas and reliability coordinators will be required to complete self-certification forms indicating their level of compliance with this standard in 2004.

Definition of Critical Cyber Assets

The standard defines critical cyber assets as:

> "*Those computers, including installed software and electronic data, and communication networks that support, operate, or otherwise interact with the bulk electric system operations. This definition currently does not include process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations.*"

The implementation plan for this standard states that it only applies to control areas and reliability coordinators in 2004. The determination of whether or not a system or software is a critical cyber asset according to the definition above is at the discretion of these entities.

The drafting team believes that a reasonable interpretation of a critical cyber asset is any system that processes or controls energy management functions, including bulk system security analysis and the initiation of generation and/or transmission control signals.

Remote data collection and control components associated with remote terminal units, process control systems, and distributed control systems, are not considered critical cyber assets in this standard.

Start of Comments & Responses

Alabama Electric Cooperative AEC
Segment: 4
Rep: Kenneth J Skroback
Negative

I have concerns about the conflicting FERC Appendix G and this NERC document. I know that a modified Appendix G has been submitted to FERC as NERC comments, but it has not yet been endorsed by FERC. FERC has mandated that Appendix G be implemented by 1-1-04, and I don't see anything that NERC can do to expedite implementation before that date. I cannot see myself voting to accept the current document during either ballot period. Therefore, I would suggest that NERC scrap the current emergency standard and proceed with the permanent standard with implementation due at the 1-1-05. The FERC requirement should provide the same substantial compliance by 1-1-04 as the NERC standard. FERC endorsement of the revised Appendix G might also persuade me to vote for the standard.

Response: FERC has indicated that NERC's continuing development of cyber security requirements is desirable, and has previously stated its preference for letting the industry develop such a standard via the NERC process.

Allegheny Energy Supply Company AESC
Segment: 5
Rep: Kenneth Githens
Affirmative

Allegheny Power AP
Segment: 1
Rep: Terri J Grabiak
Affirmative

AE is voting "yes" based on the information provided at the May 5 web cast on NERC's Cyber Security Urgent Action Request.

AE's understanding is as follows:

* Partial compliance acknowledgement by Q1 2004 will be acceptable assuming that plans/processes have been established that will facilitate compliance by Q1 2005.

Response: This is consistent with the implementation plan for this standard.

*Documented pre-employment background checks for employees and non-employees conducted in accordance with Company business practices/purchase order agreements can be "grandfathered" for personnel requiring cyber and/or physical access to the identified critical cyber assets.

Response: The standard does not require that documented pre-employment background checks already conducted be repeated.

*Establishing systems management policies and procedures for Host and/or Network Intrusion Detection services will satisfy the Q1 2004 requirements for critical cyber assets.

Response: This statement is consistent with the standard.

If the above assumptions are not correct, AE would like to be notified.

American Public Power Association
Segment: 3
Rep: Michael Hyland
Negative

Although I agree with the concept of having cyber security guidelines and best practices, I do not believe that an Urgent SAR is required at this time. A few reasons:

- There has been no indication that LSE's cyber security has failed the bulk system. Theory may state this, but it is not a case of a smaller rural LSE's shutting the lights off on the bulk system.
- This Urgent SAR appears to be more of a knee jerk reaction to certain FERC demands/request from the CIPAG. The FERC process is moving forward, and if not fast enough, FERC has the ability to step it up via a separate NOPR.
- This Urgent SAR places real, undue costs on entities that are not likely to be targeted, except by some theoretical scenario. Even in these scenario's, the chance for a small defined LSE to take down the bulk grid is remote. The costs for some entities that are covered by this Standard are not stand alone corporations with computer rooms, etc. Instead, this standard unjustly affects systems that generate as part of joint action, and have limited staff. Again – there is no cost / benefit analysis to show that these systems are a real threat to the nation grid rather than their local community's they serve. These same systems have back up plans devised over 100 year of service.
- The Urgent SAR, by definition did not go through the proper due process. There is no need for a rushed standard at this time. The idea/concept of cyber security is no more dangerous to the Bulk grid at this time than a miscalculated ATC. Why rush? Allow the due process, and review that this standard deserves.
- Rushing the cyber side of security before physical security makes no sense. Even after 9/11, we learned one major thing — physical trumps cyber, and this does nothing to fix the real situation in which we reside — physical vulnerability. The grid is more susceptible to gun shots, small explosives, etc., and here we are addressing cyber? Rushing/Urgency is warranted in some cases, but this is not one of them.

I vote no, similar to the reasons why I voted no during the CIPAG approval process. This cyber standard is being steamrolled forward, and for reasons which I feel do not warrant a title of Urgent. We have more Urgent matters to attend to in the NERC/NAESB realm, and cyber security is not one of them.

Response: Please see the general response to comments questioning the use of urgent action for this standard. The drafting team believes it adequately addresses this comment.

Aquila Inc. dba Aquila Networks UCU
Segment: 5
Rep: Philip Scott Sobol
Affirmative

"The definition of Critical Cyber Assets currently does not include process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations." NERC - Overview of Proposed Cyber Security Standard May 5, 2003

We believe that SCADA systems should be specifically addressed in this Urgent Action Request. Operations personnel could argue that because PCS and DCS systems are not in the scope of this request, then SCADA systems should not be. When referring to these systems, there needs to be a clear definition as to what NERC is defining as a PCS or DCS system and what components are included. By the above definition, does this mean that SCADA systems are not considered Critical Cyber Security Assets?

Phil Sobol CISSP, CISA
Cyber Security Specialist

Response: Please refer to the general response to comments regarding the definition of critical cyber assets in this standard. The drafting team believes this response adequately addresses the comment.

BC Hydro and Power Authority BCHA
Segment: 1
Rep: Seiki Harada
Affirmative

Comments on the Proposed
NERC Cyber Security Standard 1200

BC Hydro and Power Authority

1) BC Hydro supports the proposed standards, recognizing that:
   - NERC, as the industry leader, needs to come to an agreement quickly
   - This set of standards may not be perfect but is a good start.

2) The section on the Definition of "Critical Cyber Assets" state, in part, "This definition currently does not include process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations." There are some major Distributed Control Systems that may have significant impacts on the stability of the bulk supply of electricity, depending upon where and how used. Thus, not all DCS' should be ruled out of scope.

Response: Please refer to the general response to comments regarding the definition of critical cyber assets in this standard. The drafting team believes this response adequately addresses the comment.

Regarding background screening, Section 1207 states, in part, "The responsible entity shall conduct background screening of personnel consistent with the degree of access they are granted, in accordance with federal, state, provincial, and local laws." In addition to the laws, we should also recognize the limitations posed by existing contracts (e.g., collective agreements with bargaining units).

Response: Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment. It is assumed that most bargaining unit limitations are enforceable through federal, state and provincial labor laws.

Bonneville Power Administration — Power Business BPAP
Segment: 5
Rep: Francis J Halpin
Affirmative

We have concern over the necessity of submitting multiple reports. We would ask NERC to consider the possibility of reducing the reporting requirement for entities already required to file reports as a result of being subject to similar standards (NIST for example). One thought would be to do a side-by-side comparison of the two standards. If NIST requirements, for example, were found to be meet the minimum requirements of the NERC standard then allow a copy of the NIST report to serve as a proxy for the NERC report.

We also have concern over the possibility that information on physical and cyber security measures contained in reports and other documents become public knowledge through FOIA procedures.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes this response adequately addresses these comments.

Boston Edison Company BECO
Segment: 1
Rep: Charles Salamone
Negative

NSTAR (Boston Edison) is in favor of the NERC Cyber Security Standards and the self-certification process. However, we are not in agreement with the proposed sanctions and we feel that further work is required to identify the specific assets that are included in this standard. NSTAR also agrees with the comments provided by NPCC concerning this standard.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment. Please also see responses to NPCC.

Carolina Power & Light Company CPL
Segment: 3
Rep: Ben Crisp
Negative

Carolina Power & Light Company CPL
Segment: 1
Rep: Verne Ingersoll II
Negative

Carolina Power & Light Company CPL
Segment: 6
Rep: James Eckelkamp
Negative

Carolina Power & Light Company CPL
Segment: 5
Rep: Wayne Lewis
Negative

Florida Power Corporation FPC
Segment: 3
Rep: Gary Macey
Negative

General Comments:
Assuming minimal comments, we recommend that NERC send the Urgent Action SAR to the CIPAG for prompt revisions and then a re-ballot of the revised Standard as another Urgent Action SAR again.

If the comments are too varied and voluminous, then we would like to see this standard go through the normal procedure where comments and give and take iron out an agreement on expectations and where different segments can offer alternatives.

Response: The NERC standards process does not permit the proposed standard to be revised if it is subject to a recirculation ballot. All comments received in response to this standard will be considered by the drafting team for inclusion in the permanent standard.

As stated by the NERC May 5th Web-cast leaders, most utility companies can now substantially comply with the "intent" of this standard, but not with the audit paperwork and documentation on most its Cyber assets. It does not make sense to add new procedures and documentation unnecessarily while the final standard is being drafted and going through due process.

Definitions — Critical Cyber Assets

- Need further clarification of statements regarding what systems should be included, such as SCADA, EMS, ICCP, Tagging, IDC, Oasis — does this include upstream systems that may electronically feed source data to these control systems? Is this any system that if compromised would cause a change in generation or alter power flow on the transmission grid? For instance, plants have controls and equipment limitations that limit the possibility of large ramps in output from AGC. Therefore, why has AGC and scheduling systems been considered critical cyber assets from the perspective of this Standard? This is more of "Business continuity" decision than an electric reliability issue. PC's that

are used to manage and control the power systems and are seeded with a standard environment - how far back to corporate would be included in this definition? Answering these questions on scope will be key to complying with other areas.

Response: Please refer to the general response to comments regarding the definition of critical cyber assets in this standard. The drafting team believes this response adequately addresses the comment.

Definitions — Cyber Security Incident

- Does this include normal equipment failures such as loss of a disk, failure of a router?

Response: Please refer to the general response to comments regarding cyber security incident response and reporting. The drafting team believes this response adequately addresses the comment.

1203 — Electronic Security Perimeter

- This section indicates that a document should verify that all critical cyber assets are within the electronic security perimeter. Is it permissible for non-critical assets to be inside the electronic security perimeter? Or does anything inside the electronic security perimeter make it a critical asset by proximity? The sample diagram that was filed with FERC in November 2002 should be added to the Standard to help clarify the intent.

Response: It is permissible for non-critical assets to be within the electronic security perimeter. While being within the electronic security perimeter does not make the asset critical by definition, it does require that the non-critical asset be afforded the same degree of protection as the critical asset. This is based upon the principle of the weakest link. If a non-critical asset within the electronic security perimeter is not properly protected and is compromised, then the electronic security perimeter has been breached and all systems within the perimeter are at risk.

1206 — Physical Access Controls

- Section 1206 (b) (1) looks as if it was cut/paste from section 1204 (b) (1). Section 1206 should reference the physical security perimeter — not the electronic security perimeter.

Response: It appears the commenter was looking at the March 27, 2003 draft of the proposed standard. The reference to the electronic security perimeter was corrected in the April 9, 2003 version that was officially posted for pre-ballot review.

Can each utility define the physical security perimeter as they see fit or is there some minimal requirement for the physical security perimeter as it relates to the electronic security perimeter? For example, is there an implication that any hardware within the electronic security perimeter must physically exist behind certain minimal security levels within the physical security perimeter?

Response: The utility is expected to define the physical security perimeter as necessary to ensure the critical assets are properly protected. There is an assumed relationship between the physical and electronic security perimeters in that an asset, critical or not, that is defined to be within the electronic security perimeter but not protected from uncontrolled physical access could be compromised.

1207 — Personnel

- Are control room operators subject to background screening under this standard as they have actual generation and breaker control access to bulk power system?

- An entity may not be able to comply with this area because of Bargaining Unit issues. What relief is there for this circumstance?

Response: Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment.

1210 — Information Protection

- Does proper adherence to section 1210 imply that sensitive information should not be stored on corporate file servers but should probably be stored on carefully secured file servers inside the electronic security perimeter? Does it mean that this information should never be emailed to distribution groups for review because this would breech a secured environment? Does it mean that printed draft copies need to be shredded? Does it means that printed copies in either notebooks or filing cabinets must be stored behind physical access controls that allow only personnel that have been cleared for proper security access? It almost sounds like printed copies become a security liability. Is this the section's intention?

Response: The intent of this section is to ensure that sensitive information is properly protected from unauthorized disclosure. This section does not imply that sensitive information cannot be stored on corporate file servers. Sensitive information should not be publicly accessible, such as from a corporate public web server or FTP server. The sensitive information should not be stored in an unencrypted form on a server, corporate or otherwise, if that server is not reasonably protected from unauthorized access. Sensitive information should not be transmitted electronically "in the clear."

1211 — Training

- Does this section imply that all people involved in the training process and the training materials developed in the training process must adhere to guidelines in sections 1207 and 1210?

Response: Section 1211 requires that personnel with access to critical assets receive proper training on the policies and procedures for protecting the assets. This does not require that the training staff be subjected to background checks (reference to Section 1207), nor does it imply that the training materials themselves are automatically considered sensitive information that must be protected (reference to Section 1210). However, the training materials should be reviewed just like any other information to determine if they contain sensitive information that must be protected. For example, if a training document contains the details of the cyber assets within the security perimeters, or the recovery plans for those assets, then that portion of the training material should be protected under the requirements of Section 1210.

1213 — Test Procedures

- Is isolated test environment interpreted simply as "non-production" development systems that still may have capability to electronically transfer files from/to control system LAN? Or is it meant to be more restrictive requiring electronic isolation of a "sandbox" development system which cannot electronically transfer files from/to the production control system LAN?

Response: Electronic isolation is not required by this standard; rather, a controlled non-production system is to be used for testing.

The term "isolated test environment" should not imply that the test environment must be outside the electronic security perimeter.

Response: The standard does not require that the test environment be outside the electronic security perimeter.

1215 — Recovery Plans

- The given definition for Cyber Security Incident is too vague. Is it limited to loss of hardware, corruption of software, use of the facilities for a limited time or does it include the complete loss of building and communications?

Response: Please refer to the general response to comments regarding incident response and reporting. The drafting team believes this response adequately addresses the comment.

Retention Periods

The three-year retention periods are excessive. When an audit is performed it is only the most recent compliance period that should matter. One might be non-compliant for several three periods due to differences of interpretation instead of actual failure to comply.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment.

Proposed Compliance Schedule

The posted compliance schedule states that utilities' 2005 Self-assessment must be fully compliant. This differs from what was stated on the May 5th Web-cast where it was stated utilities were not required to be fully compliant until the 2005 compliance year (with a self assessment report made at the beginning of 2006). This language needs to be clarified.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment.

Other General Comments:

Each section in the standard has a "Compliance Monitoring Process". The process mentions that the responsible entity shall keep data for three years. Is it implying that we need to be able to document all changes made to a document during the three-year period, produce time-stamped versions of the documents and show a system time-stamped trail of version history? If so, does the process imply that we should be using some type of formal document control system that is capable of system time-stamping each version? Or is it adequate to maintain documents that have a manually time-stamped history section?

The "Compliance Monitoring Process" sections also state that "the compliance monitor shall keep audit records for three years". Who is the "compliance monitor"? We assume it is the applicable region. The documents that may be part of the audit records would probably be highly sensitive and secure in their nature since they contain the very essence of security measures in place at a utility. Is the expectation that anyone involved in the compliance monitoring process and/or audit process must strictly adhere to 1207 and 1210 sections in order to view these documents? If so, will the compliance monitor be required to demonstrate adherence before being allowed access to security information? Is this a wise policy to share secure information with auditors? These sections may need to be more descriptive about which documents the compliance monitor/auditor can keep — if any. Change this process to only allow onsite viewing of the documents.

Response: The compliance monitor for this standard is the applicable NERC Region, as suggested by the commenter. No audits will be conducted in 2004. Please see the general response to comments regarding compliance with this standard. The drafting team believes it addresses this comment.

City of Tallahassee TAL
Segment: 5
Rep: Alan Gale
Negative

1) If the committee expects that the industry is already 85% compliant, and full compliance is not expected within the next year, why is this an urgent action?
2) The standard is not clear enough to decide what is and what is not covered. Contradictory information was provided via the web cast.

Response: Please see the general responses to comments regarding ambiguity in this standard and to comments regarding the use of urgent action for this standard. The drafting team believes these responses adequately address these comments.

3) Standard 1214 contradicts the referenced NIPC guide which requires only "malicious" acts to be reported. I would suggest our standard be malicious or unknown causes. This would eliminate a lot of "routine" failure reports.

Please see the general response to comments regarding incident response and reporting. The drafting team believes it adequately addresses this comment.

4) What constitutes compliance is unclear. It appears I can say "I have a procedure" with no meat to it and still be well on my way to compliance. I do not believe this is the standard we want to belly up to.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment.

Con Edison Company of New York CEPD
Segment: 3
Rep: Stuart Nachmias
Negative

Con Edison Company of New York CEPD
Segment: 1
Rep: Charles Rusowicz
Negative

Con Edison Company of New York CEPD
Segment: 6
Rep: Rebecca Adrienne Craft
Negative

Consolidated Edison Co. of New York NYCE
Segment: 5
Rep: Edwin E. Thompson PE
Negative

Con Edison votes against the proposed urgent action Standard 1200 — Cyber-Security for the following reasons:

Any proposed standards must be developed with the full participation of the parties responsible for operating the critical cyber assets defined in the proposed standard. The permanent cyber security standard process currently underway allows such participation and may result in significant changes to the urgent action Standard 1200. While it is important that the cyber standard be established promptly, it is equally important that it is done properly and done with business practicality considerations.

Response: Please see the general response to comments questioning the use of urgent action for this standard. The drafting team believes it adequately addresses this comment.

The proposed standards do not take into consideration the impact that the standards may have on existing security measures or those in the process of being implemented.

Response: This standard sets minimum cyber security requirements. If cyber security measures that meet or exceed the requirements of this standard are already in place, the requirements of this standard have been fulfilled.

The vulnerabilities of the computers and communications networks associated with the operation of the bulk power system are not identified in the proposed standards. It is critical that such vulnerabilities be identified before establishing a remedy for them and that the prescribed remedies consider cost of implementation relative to the risk being addressed.

The definition of “critical cyber assets” needs to be supplemented in terms of the impacts sought to be avoided.

Response: A vulnerability assessment is not required in this standard. This standard is intended to address well-known vulnerabilities with network systems.

The compliance monitoring process is not clearly defined and exposes entities to sanctions based on the subjective interpretation of the Compliance Monitor.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment. There will be no sanctions (financial penalties or letters) associated with non-compliance to this standard in 2004.

Atlantic City Electric ACE
Segment: 3
Rep: Katharine Jessen Olinchak
Affirmative

Conectiv Energy Supply CNCT
Segment: 5
Rep: Gloria Ogenyi
Affirmative

Conectiv Power Delivery
Segment: 1
Rep: Paul Rychert
Affirmative

Potomac Electric Power Company PEPW
Segment: 3
Rep: Richard Kafka
Affirmative

1207, 2.3 Personnel — Background screening of personnel who have access to critical cyber assets should be a tiered process such that personnel who have physical access only would have a low level of background checks while personnel who have physical and unrestricted electronic access would have a high level of background checks.

Response: The type and method of conducting background checks is outside the scope of this standard. A tiered approach to background checks is not precluded by this standard and is at the discretion of the organization conducting the checks.

Cyber Security Incident Definition, and, 1214 Electronic Incident Response Actions — Cyber Security Incidents and Electronic Incident Response Actions be limited to actual or suspected security related events that disrupt the proper operation of a critical cyber asset. As currently defined “Any event or failure (malicious or otherwise) that disrupts the proper operation of a critical asset” is too broad such that an ordinary (non security related) hardware, software, etc. failure that disrupts the operation of a critical cyber asset would need to be reported to the electricity sector ISAC.

Response: Please see the general response to comments related to incident reporting. The drafting team believes it adequately addresses this comment.

Consumers Energy CETR
Segment: 4
Rep: David Frank Ronk
Negative

Consumers Energy CETR
Segment: 3
Rep: Jeanne M Kurzynowski
Negative

General response to this commenter: The NERC standards process does not permit the proposed standard to be revised if it is subject to a recirculation ballot. The team drafting the permanent cyber security standard will receive all comments submitted by voters.

Change the requirement for background checks to establish a human reliability program that could include background checks, 2 man rules, drug tests, etc based on the policy developed by each company as part of section 1201.

Response: Please see the general response to comments regarding background checks. The drafting team believes this response adequately addresses this comment.

Change the requirement for testing and acceptance in an isolated test environment to a change management process that documents the test environment and why it was chosen along with acceptable roll back plans.

Response: Please see general response above.

Under Information Protection, the recognition that information about the critical cyber assets can be controlled but that general building information on the buildings that house these assets are generally available to a larger population of employees and contractors that have to work on these facilities.

Response: It is not the intent of this standard to prevent access to this information by employees and contractors who have a valid need to know.

Duke Energy North America DENA
Segment: 6
Rep: Michael Gildea
Negative

Duke Power DUKE
Segment: 1
Rep: Greg Stone
Negative

Duke Power DUKE
Segment: 5
Rep: Randy Herrin
Negative

Duke Power DUKE
Segment: 3
Rep: Scott Henry
Negative

Greater clarification needs to be made around compliance to the new standards. It would seem appropriate that full compliance should not be required until 2005 and as such, no noncompliance letters should be issued unless furnished to a utility only to provide guidance. Any documented partial compliance provide by a utility or identified by an audit should not be public information or the safety of the EMS could be jeopardized. This should fall under the FERC Order 630 as CEII and exemptions 2 & 7 of the FOIA. Agreement should be made by the FERC CEII Coordinator as to the ruling on this information prior to any audit. Provide clarification on the expected compliance schedule and the applicability of Order 630 and the exemptions provided under sections 2 and 7 of the FOIA.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment.

The requirement for background checks lacks adequate guidance to ensure consistency. More specific guidance should be provided as to the type of background checks required.

Response: Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment.

Standards 1214 and 1215 require reporting incidents, cyber or physical, that should also be protected under order 630. Additional requirements are required by DOE on Form 417. Can these be combined to simplify the reporting process?

Response: Please see the general response to comments regarding incident response and reporting. The drafting team believes it adequately addresses this comment. The current version of Form 417 does not address all necessary reporting information required in this standard.

An audit of cyber security will require access to information that utilities must carefully protect. This information is not shared outside the company and access is very limited within the company. What protection will the audit process have to ensure auditors meet the highest level of security including formalized nondisclosure agreements? How can a company validate the auditors' security?

With the compliance/audit process being managed in the region(s), how will a consistent approach be assured, especially when utilities work across regions?

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment. No audits will be conducted in 2004.

Additional comments of Scott Henry:

I commend the Standards Drafting Team on its significant effort to draft a reasonable standard in a short amount of time. Generally, I support NERC's effort to develop industry standards related to cyber security. I am also supportive of the areas of the proposed standard that are clear. There are components of the standard that are unclear and could result in confusion by the industry. Clarifying the following issues would provide greater clarity and a better standard.

Thanks for the opportunity to comment. And again, many thanks to the standards drafters for their diligent efforts.

Scott Henry

Exelon Energy Delivery - PECO & ComEd
Segment: 1
Rep: Michael J. Donnelly
Affirmative

Exelon Energy Delivery EED - PECO & ComEd
Segment: 3
Rep: John Blazekovich
Affirmative

Exelon Generation Company LLC EXGN
Segment: 5
Rep: Linda Clarke
Affirmative

Exelon Generation Company LLC EXGN
Segment: 6
Rep: Regina Carrado
Affirmative

PECO Energy Company
Segment: 3
Rep: John Leonard
Affirmative

Contact:
Kurt Muehlbauer
Exelon Corporation
227 W. Monroe
Chicago, IL 60606
312.394.3772
kurt.muehlbauer@exeloncorp.com

Exelon fully supports the protection of critical cyber assets that impact the reliability of the bulk electric system operation. Exelon respectfully submits the following comments to seek clarification on the standard and for consideration as the permanent standard is created.

Compliance Monitoring Process
The May 5, 2003 web cast presentation states that partial compliance is acceptable for January 2004. Exelon requests guidance on what level of compliance will be deemed acceptable for this self-certification period.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment.

Exelon understands that the standard is written at a high level and must accommodate numerous types of entities across North America. We seek clarification on how issues regarding which cyber assets should be considered in-scope and how differences in interpretation of the standard will be resolved.

Protection of confidential information associated with critical cyber asset

Each of the 16 cyber security standards requires entities to demonstrate compliance through self-certification annually. In addition, standards 1214 and 1215 require submittal of information as a result of a physical or electronic incident. Exelon is concerned that the information provided through self-certification or incident reporting may identify security vulnerabilities. If information associated with the protection of critical cyber assets is disclosed, it can be used to compromise the security of the critical cyber assets that the standards are intended to protect.

NERC should communicate to all entities providing information under these standards how the information will be used, under what conditions it will be disclosed to parties other than NERC, whether notification will be given to the entity that the information has been disclosed, and what steps will be taken to protect physical and electronic copies of the information maintained by NERC. A confidentiality agreement should be executed between NERC and each entity before information is required to be reported to NERC.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment.

1207 — Personnel

Measure 2.2 requires updating the list of all personnel granted access to critical cyber assets within 24 hours of any change. Exelon agrees that the list should be updated within 24 hours for cases where a person loses his/her access rights due to cause. We believe that routine administrative transfers should be managed within three business days or less.

Measure 2.3 requires background check screening of personnel consistent with the degree of access they are granted. Please confirm that it is not the intent of this standard to conduct background checks on existing personnel.

Response: Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment.

4) 1214 & 1215 – Electronic/Physical Incident Response Actions

Both of these standards require incidents involving critical cyber assets to be reported to the Electricity Sector Information Sharing and Analysis Center (ISAC) in accordance with the National Infrastructure Protection Center (NIPC) Indications, Analysis, Warnings (IAW) Program Standard Operating Procedure (SOP). The referenced document posted on the NERC web site (Rev. 4.0; 2/25/02) states that reporting is voluntary. Attachment A, Criteria & Thresholds for Reporting Incidents, of this SOP is labeled as 'Draft'.

Exelon requests clarification on whether or not reporting is in fact voluntary and if entities will be required to conform to the draft criteria and thresholds for reporting incidents. We also request clarification moving forward on who owns this SOP and the process by which it is updated.

The definition of a Cyber Security Incident includes any event or failure (malicious or otherwise) that disrupts the proper operation of a critical cyber asset. Exelon believes that this definition is too broad since it could be interpreted to include events that are common in a production environment. e.g., a disk failure or a system reboot. Exelon proposes the following definition of a Cyber Security Incident: An event or significant failure that disrupts the proper operation of a Critical Cyber Asset, causing the reliability of the bulk electric system to be adversely affected.

Response: Please see the general response to comments regarding incident response and reporting. The drafting team believes it adequately addresses this comment. The NERC process does not permit a modification to the standard, if it is to be recirculated for ballot.

Florida Municipal Power Agency FMPA
Segment: 3
Rep: Joseph Krupar
Negative

While a comprehensive cyber security standard is needed for the bulk electric system the proposed standard is not definitive enough for my support as an urgent action standard. One example that this standard needs more work is that during a recent conference call a question was asked if RTUs were included because they seemed to fit the description of a critical cyber asset. The answer given was that RTUs were not included. But later if a wide area network were used to communicate with RTUs then they may be included. There is too much interpretation of the urgent action cyber security standard. It is recommended that the urgent action cyber security standard become a white paper and work progress on the final cyber security standard.

Response: Please see the general response to comments questioning the use of urgent action for this standard and the general response to comments regarding the definition of critical cyber assets. The drafting team believes these responses adequately address this comment.

Florida Power & Light FPL
Segment: 1
Rep: Marty Mennes
Negative

I support the overall concept of NERC's Cyber Security Standards for the electric industry and concurs that such standards would afford value to the security of the electric sector. Moreover, my company places acute emphasis on security, whether physical or cyber, and welcomes the opportunity to corroborate with its industry partners in establishing more secure working environments in either arena. I also recognize the effort of the NERC CIPAG and champions the CIPAG's commitment to the focus of uniform cyber security for our industry.

However, it is our sincere belief that regardless of the urgency of the aforementioned standards or the perception of urgency thereof, standards affecting the electric sector in this delicate area should include ample vetting by the industry at large to ensure proper focus and scope.

It is our belief that NERC's current Urgent Action SAR lacks clarity and scope in that it lends itself to ambiguity in its wording, and confusion amongst its audience. It is essential that any standard intended to address the security needs of the electric sector be clear, consistent, and evenly applied throughout.

We respectfully request that the NERC CIPAG reassess the scope, purpose and specific requirements stated within the published standard, and consider how the standard will impact the industry should ambiguity and confusion prevail. We also recommend that the CIPAG seek industry participation, guidance, and feedback when drafting such standards. In addition, it is suggested that the CIPAG plan proactively to provide an ample comment / modification period prior to filing future standards.

Although much of the cyber security standard speaks to administrative issues, much of which are academic, we have split our response into three areas, those being 1) governance and 2) specific requirements and 3) additional concerns. We have included the original verbiage from the standard for the readers benefit in [*italic text*] and have highlighted areas of concern in [***bold italic text***]. Comments and recommendations are highlighted in [red underlined text]. Thus, listed below are several areas, which we feel require written clarification into the standard, in a manner absent of ambiguity and/or interpretation:

Response: Please see the general response to comments regarding the use of urgent action for this standard and for comments regarding ambiguity in the standard. The drafting team believes it adequately addresses the comments above.

The specific comments made below mirror those of FRCC. Please see the responses to FRCC's comments.

1). GOVERNANCE:

I.) Applicability:
"These cyber security standards apply to entities performing various electric system functions, as defined in the functional model approved by the NERC Board of Trustees in June 2001. NERC is now developing standards and procedures for the identification and certification of such entities. Until that identification and certification is complete, these standards apply to the existing entities (such as control areas, transmission owners and operators, and generation owners and operators) that are currently performing the defined functions.

II.) Critical Cyber Assets:
Those computers, including installed software and electronic data, and communication networks that support, operate, or otherwise interact with the bulk electric system operations. This definition currently does not include process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations.

Comments: Given the aforementioned scope of applicability, this standard applies to transmission owners and operators, and generation owners and operators, however, confusion still remains in that the definition of "critical cyber assets" excludes specific areas. Further written clarification is require to determine whether entities dealing in areas such as market function would be required to comply with this standard.

III.) Cyber Security Incident*:*
***Any** event or **failure** (malicious or **otherwise**) that disrupts the proper operation of a critical cyber asset.*

Comments: The words "**any**" and "**otherwise**" in this definition lead to broad interpretations. Under this definition, any disruptive event albeit non-intentional or malicious, would be classified as an "incident." A simple reboot of a system meets the criteria defined within "any" and also in "otherwise." Consequently, reboots, disk failures, or memory lockups – do - disrupt the "proper operation of a critical cyber asset", yet they are common to production environments. Under this definition any of these common events would constitute an "incident" dealing with a cyber assets. Also, the term "**failure**" should be clearly defined. As stated above, failures of cyber assets that are caused by non-malicious activities (i.e. software testing, or hardware failure) would be a reportable offense under section 1214.2.2 of this standard.

Recommendations:
Cyber Security Incident: An~~y~~ event of unknown origin or a significant failure ~~(malicious or otherwise)~~ that disrupts the proper operation of a critical cyber asset, causing the reliability of the bulk electric system to be adversely affected.

IV.) Purpose:
*To reduce risks to the reliability of the bulk electric systems **from any compromise of critical cyber assets.***

Comment: This purpose statement is important, because it clearly articulates that the intent of this standard is "to reduce risk to the reliability of the bulk electric **system**" from cyber incidents or physical incidents as they relate specifically to the "critical cyber assets." One area of concern herein is the verbiage "***from any compromise of critical cyber assets."*** This definition lends itself to include non-malicious production glitches, which are often a reality in production environments. The definition also broadens the scope of the standard to include not only the reliability of the **overall system** itself, but also the reliability of **each cyber asset**.

Moreover, section 1214.2.2 - Electronic Incident Response Actions requires that complying entities:

"shall require that incidents involving critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure."

Comments: Such incidents (as defined in the *NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure*) would include recognized sabotage, alleged sabotage, or possible

sabotage, obvious attempts to gain unauthorized access, intelligence gathering, unauthorized physical surveillance, intrusions or impairments of "critical cyber assets", threats to security, software, operations or physical facilities, or loss of 500 MW of generation for 30 minutes or more, or loss of 230 kV or larger for 60 minutes or more.

Clearly the wording in this section requires further review and reflection on what this requirement is asking the industry to do.

Recommendations:
Purpose: To reduce risks to the reliability of the bulk electric systems from intentional and/or malicious acts, which significantly ~~any~~ compromise ~~of critical cyber assets~~ the reliability of the system.

SPECIFIC REQUIREMENTS:

1204. Electronic Access Controls

1. Requirement
The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function ***shall identify and implement electronic access controls for access to critical cyber assets within the electronic security perimeter.***

Comments: Depending on how granular the documentation process needs to be, the impact on manpower and cost can range from minimal to significant.

1207. Personnel

1. Requirement
The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function ***shall identify all personnel, including contractors and service vendors, granted electronic or physical access to critical cyber assets.***

2. Measures

2.1. *The responsible entity shall maintain a list of all personnel granted access to critical cyber assets, including the* ***specific*** *electronic and physical access rights to the security perimeter(s).*
Comments: Access control lists are achievable, however the key words here is "**specific**." Ambiguity surrounds how detailed this access control list is expected to be. Is it intended to be simple domain access, or is it to the application level.

2.2. *The responsible entity* ***shall review the document referred to in 1207.2.1 at least quarterly and update the document within 24 hours of any change.***

Comment: Section 1207.1 calls for contractors and service vendors to be governed by this standard. This may not be possible for contractors and service vendors unless such notifications are worked into contracts ahead of time.

As an example: Consider a member of the cleaning staff sub-contracted to work at an entity. Said contractor has physical access to the "perimeter" and is dismissed on Friday at 5:00PM by his/her employer. The complying entity may not know of the event for several days after the fact, if ever depending on the individual. Hence, violating the 24-hour requirement set forth in section 1207.2.2 of these standards.

2.3. *The responsible entity* ***shall conduct background screening of personnel consistent with the degree of access they are granted, in accordance with federal, state, provincial, and local laws.***

Comments: Background screenings may not be possible for contractors and service vendors who would be governed under this section. Additionally, some States have laws preventing this process even for employees. Thus, bringing us back to the uniformity issue and possibly making entities in those States, the "weakest link."

1208. Monitoring Physical Access

1. Requirements

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function ***shall monitor physical access to critical cyber assets 24 hours a day, 7 days a week.***

Comments: Although physical access monitoring is possible in most areas, there is no verification that tailgating will not occur. To prevent such tailgating violations, an anti-passback system would be required at perimeter access points, in addition to personnel training. Consequently, monitoring yields logs and logs tend to become voluminous. At what point does maintaining vast amounts of logs become counter productive, as these logs may only prove that John Smith entered through the West door (assuming he did not tailgate)?

1209. Monitoring Electronic Access

1. Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function ***shall monitor electronic access to critical cyber assets, 24 hours a day, 7 days a week.***

2. Measures

2.1. *The responsible entity* ***shall maintain a document identifying electronic access monitoring tools and procedures. This document shall verify that the tools and procedures are functioning and being used as planned.***

2.2. *The responsible entity* ***shall document electronic access to critical cyber assets via access records (e.g., logs). Access records shall be verified against the list of access control rights.***

Comment: Again, such monitoring can yield voluminous logs. measure 2.2 of this requirement call for verification against a list of access controls, which could prove to be easier said than done.

1212. Systems Management

1. Requirement
The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function ***shall establish systems management policies and procedures for configuring and securing critical cyber assets. At a minimum, these policies and procedures shall address:***

1.1. The use of effective password management that periodically requires changing of passwords, including default passwords for newly installed equipment;
1.2. The authorization and periodic review of computer accounts and access rights;
1.3. The disabling of unauthorized, invalidated, expired, or unused computer accounts and physical access rights;
1.4. The disabling of unused network services and ports;
1.5. Secure dial-up modem connections;
1.6. Firewall management;
1.7. Intrusion detection processes;
1.8. Security patch management;
1.9. The installation and update of anti-virus software;
1.10. The retention and review of operator logs, application logs, and intrusion detection logs; and
1.11. Identification of vulnerabilities and responses.

Comments: Areas such as "security patch management" could present significant problems with vendor specific applications and the vendor's reluctance to support patches or O/S versions other than those currently operational. This area could force entities into non-compliance.

1213. Test Procedures

1. Requirement
The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function ***shall establish test procedures and acceptance criteria to ensure that critical cyber assets installed or modified comply with the security requirements in this standard. Test procedures shall require that testing and acceptance be conducted in an isolated test environment.***

Comments: A more detailed definition of the terms "**test**" and "**modification**" is required.
The aforementioned definition leads to the following questions:
1). To what extent is testing an application, which requires real-time data inputs, allowed?
2). If said test yield a failure of a "critical cyber asset" is that a reportable incident?
3). To what extent are common system administration modifications (changes) considered applicable to this standard.

1214. Electronic Incident Response Actions (as referred to previously)

1. Requirement
The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function ***shall define electronic incident response actions, including roles and responsibilities assigned by individual or job function.***

2. Measures

2.1. *The responsible entity* ***shall maintain a document defining the electronic incident response action, including actions, roles and responsibilities.***

2.2. The document in 1214.2.1 **shall require that incidents involving critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the *NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedur*e.**

Comments: Such incidents (as defined in the *NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedur*e) would include:

- recognized sabotage,
- alleged sabotage, or possible sabotage,
- obvious attempts to gain unauthorized access,
- intelligence gathering,
- unauthorized physical surveillance,
- intrusions or impairments of "critical cyber assets",
- threats to security, software, operations or physical facilities, or loss of 500 MW of generation for 30 minutes or more, or loss of 230 kV or larger for 60 minutes or more.

Yet, under the definition of Critical Cyber Asset, "***Any*** *event or* ***failure*** *(malicious or* ***otherwise****) that disrupts the proper operation of a critical cyber asset. Clearly these two definition clash and yield confusion.*

ADDITIONAL CONCERNS:

The current standard fails to clearly describe the following:

- how the auditing process will occur,
- who specifically will conduct the audits,
- Mr. Chuck Noble's definition of "*substantial compliance*" as articulated during his presentation at the April NERC CIPAG meeting in Orlando, Florida
- how disagreements in the interpretation of compliance will be arbitrated and whom,

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment. No audits will be conducted in 2004.

- will FERC adopt the standard in whole or in part,
- will FERC supercede the standard or sections thereof.

Response: FERC's actions are beyond NERC's control; the drafting team cannot answer these questions.

FRCC
Segment: 2
Rep: Linda Campbell
Negative

Orlando Utilities Commission OUCT
Segment: 3
Rep: Thomas Washburn
Negative

Tampa Electric Company TEC
Segment: 3
Rep: Ronald Donahey
Negative

Seminole Electric Cooperative SEC
Segment: 4
Rep: Steven Wallace
Negative

The FRCC agrees with the need and supports the idea of developing a cyber security standard to protect the bulk electric system. The FRCC thanks the CIPAG for their work and efforts to focus the electric industry on cyber security standards to protect the bulk electric system. However, for the reasons stated below we cannot support approving this as an urgent action standard.

The standard does not include enough specific information to determine the applicability of many of the requirements. Many questions have been raised and the answers were either not known, unclear, or contradictory. This uncertainty does not allow entities to truly know what they need to do to be compliant and "self-certify" their performance, or to be able to determine the dollars necessary and budget accurately for any funding that might be needed. It is essential that any standard intended for security of the electric sector be clear and consistent. Some of the specific concerns and recommendations are listed below.

1. Confusion still remains in the definition of "critical cyber assets". Further clarification of statements regarding what systems should be included, such as SCADA, EMS, ICCP, Tagging, IDC, Oasis is needed. Does this include upstream systems that may electronically feed source data to these control systems? Further written clarification is required to determine whether entities dealing in areas such as market function would be required to comply with this standard.

Response: Please see the general response to comments regarding the definition of critical cyber assets. The drafting team believes it adequately addresses this comment.

2. The words "any" and "otherwise" in the definition of "cyber security incident" lead to broad interpretations. Under this definition, any disruptive event albeit non-intentional or malicious, would be classified as an "incident." A simple reboot of a system meets the criteria defined within "any" and also in "otherwise." Consequently, reboots, disk failures, or memory lockups do — disrupt the "proper operation of a critical cyber asset", yet they are common to production environments. Under this definition any of these common events would constitute an "incident" dealing with a cyber assets. Also, the term "failure" should be clearly defined. As stated above, failures of cyber assets that are caused by non-malicious activities (i.e. software testing, or hardware failure) would be a reportable offense under section 1214.2.2 of this standard. We would recommend the definition be changed to the following: An event of

unknown origin or a significant failure that disrupts the proper operation of a critical cyber asset, causing the reliability of the bulk electric system to be adversely affected.

Response: Please see the general response to comments regarding incident response and reporting. The drafting team believes it adequately addresses this comment.

3. The purpose statement is important, because it clearly articulates that the intent of this standard is "to reduce risk to the reliability of the bulk electric system" from cyber incidents or physical incidents as they relate specifically to the "critical cyber assets." One area of concern however, is the verbiage "from any compromise of critical cyber assets." This definition lends itself to include non-malicious production glitches, which are often a reality in production environments. The definition also broadens the scope of the standard to include not only the reliability of the overall system itself, but also the reliability of each cyber asset. We would recommend the purpose be changed to the following: To reduce risks to the reliability of the bulk electric systems from intentional and/or malicious acts, which significantly compromise the reliability of the system.

Response: The drafting team does not envision a non-malicious production "glitch" as a compromise of a critical cyber asset. Clearly the failure of a critical asset due to something as common and non-malicious as a hard disk crash is not a security concern, although much if not all of the recovery plans required by Section 1216 would be appropriate for both malicious and non-malicious events.

4. Standard 1207 — Personnel.

Measurement 2.1 requires "specific" access control lists. Is it intended to be simple domain access, or is it to the application level?

Response: The referenced measure simply requires that a list of personnel and their access rights be maintained. Implementation and application levels are not addressed. Measure 1207.2.1:

"The responsible entity shall maintain a list of all personnel granted access to critical cyber assets, including the specific electronic and physical access rights to the security perimeter(s)."

Measurement 2.2. requires review of the document referred to in 1207.2.1 at least quarterly and update the document within 24 hours of any change. Section 1207.1 calls for contractors and service vendors to be governed by this standard. This may not be possible for contractors and service vendors unless such notifications are worked into contracts ahead of time.

As an example: Consider a member of the cleaning staff sub-contracted to work at an entity. Said contractor has physical access to the "perimeter" and is dismissed on Friday at 5:00PM by his/her employer. The complying entity may not know of the event for several days after the fact, if ever depending on the individual. Hence, violating the 24-hour requirement set forth in section 1207.2.2 of these standards.

Measurement 2.3 requires background screening of personnel. Background screenings may not be possible for contractors and service vendors who would be governed under this section. In addition, some entities may not be able to comply with this requirement because of Bargaining Unit issues. What relief would there be for these circumstances?

Response: Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment. It is assumed that most bargaining unit limitations are enforceable through federal and state labor laws.

5. Standards 1208 and 1209 — Monitoring Physical and Electronic Access

Couldn't these two requirements be combined into one? These requirements states that monitoring will take place 24 hours per day, 7 days per week, and that logs on access to critical assets will be collected and verified against lists of authorized users. Access logs are voluminous, and if the standard is to be interpreted literally, it would be impossible to monitor, verify, and report on such logs; other than on a small-random-sample basis without the use of automated correlation tools. What constitutes compliance for monitoring of physical and electronic access? Is existence of logs for forensic purposes and periodic review sufficient? For how long must Video and other Physical data be stored to prove compliance?

Response: The intent of Section 1208, in conjunction with sections 1205 and 1206, is to ensure that only authorized personnel (who have completed the required background check and have an approved need) are granted unescorted access to the critical assets. There are a number of ways that physical access can be monitored and verified per the standard. The most common is an electronic access control system (such as a card reader) with individualized access credentials. The person requesting access presents the credentials (swipes the badge) at which time the access control system validates the credentials, determines whether or not the person is permitted entry, and unlocks the door as appropriate. An electronic log entry of this action, identifying the date, time, person (badge identifier), and which door was accessed is recorded. The electronic system is doing the authentication and the monitoring and thus satisfies the requirements of the standard. Should something unexpected happen, the logs can be quickly reviewed to determine who had access. If there is a concern that the person requesting access is not using their assigned badge, a CCTV monitoring and recording system can also be employed and would serve as an additional "log" source. The minimum data retention requirement is six months, as specified in Section 1208, Paragraph 4.2. Employing both the electronic access control system and the CCTV system exceeds the minimum requirements of this standard. Employing just a CCTV system without pre-entry validation of the credentials (such as by a local or remotely sited security guard) would not meet the standard. As with physical access monitoring, the use of electronic authentication that supports logging is an acceptable method to satisfy the requirements of Section 1209. The person requesting electronic access presents a set of credentials such as username and password (the standard does not mandate multi-factor authentication). The credentials are validated and the user rights list associated with that identity defines what the user can do. The system will continuously monitor the user's activities in that it will not permit the user to access data or perform functions for which there is no authorization. At a minimum, recording of the log-on and log-off events will satisfy the logging requirement. The use of additional operating system logging, as well as application, database, firewall, and IDS logging is also acceptable and encouraged. To the extent that activity logging is employed, the standard is applicable, particularly with respect to data retention.

6. Standard 1210 — Information Protection

Does proper adherence to this standard imply that sensitive information should not be stored on corporate file servers but should be stored on carefully secured file servers inside the electronic security perimeter? Does it mean that this information should never be emailed to distribution groups for review because this would breech a secured environment? Does it mean that printed draft copies need to be shredded? Does it mean that printed copies in either notebooks or filing cabinets must be stored behind physical access controls that allow only personnel that have been cleared for proper security access? This section needs to be clarified.

Response: The intent of this section is to ensure that sensitive information is properly protected from unauthorized disclosure. This section does not imply that sensitive information cannot be stored on corporate file servers. Sensitive information should not be publicly accessible, such as from a corporate

public web server or FTP server. The sensitive information should not be stored in an unencrypted form on a server, corporate or otherwise, if that server is not reasonably protected from unauthorized access. Sensitive information should not be transmitted electronically "in the clear."

7. Standard 1212 — Systems Management

Requirement 1.7 calls for intrusion detection processes, but to what extent is not defined in the document. Generally accepted industry standards would indicate the use of commercial network or host based intrusion detection. While these tools will detect standard IP protocol based attacks, they are not designed to detect attacks that might be based upon older or proprietary protocols used in many utility control systems. The electronic monitoring required in standard 1209 could also be perceived as a form of intrusion detection; however, manual review of system logs is not an effective IDS control due to the volume of data in such logs, and lack of timely response to events. Please clarify what is required for compliance to intrusion detection processes.

Response: The standard specifically does not define intrusion detection technology for the very reasons cited in the comment. It is up to the utility company to evaluate its electronic security perimeter and critical assets therein, determine the risk and nature of an attack against those assets, and devise a reasonable intrusion detection process where technically feasible that will enable the company to detect and deter an attack before damage can be done. The approach should be commensurate with the risk and resulting consequences of an attack.

Requirement 1.8 calls for security patch management. This could present significant problems with vendor specific applications and the vendor's reluctance to support patches or O/S versions other than those currently operational. This area could force entities into non-compliance.

Response: The standard does not require that all security patches be implemented, rather that a "process" be in place to "manage" the implementation of the patches. The process should include investigation, testing, implementation, back out plans and appropriate documentation of decisions made throughout the process. It's perfectly acceptable to make a conscious decision to not implement a patch, as long as you have a good reason, and have taken other steps to mitigate the problems fixed by the patch. Case in point: if you can't implement the SQL Slammer patch for some reason, you should document your reasons, and upgrade or install network access control around the SQL nodes. This should include both network and possibly host-based controls restricting the known attack vectors and only allowing network access from known required other nodes on the network. This is not perfect, but is certainly better than the two alternatives of patching and breaking an application or not doing anything, and leaving the node open to attack.

8. Standard 1213 — Test Procedures

Is isolated test environment interpreted simply as "non-production" development systems that still may have capability to electronically transfer files from/to control system LAN? Or is it meant to be more restrictive requiring electronic isolation of a "sandbox" development system which cannot electronically transfer files from/to the production control system LAN?

Response: Electronic isolation is not required by this standard; rather, a controlled non-production system is to be used for testing.

9. Standard 1214 — Electronic Incident Response Actions

Such incidents (as defined in the NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure) would include:

- recognized sabotage,
- alleged sabotage, or possible sabotage,
- obvious attempts to gain unauthorized access,
- intelligence gathering,
- unauthorized physical surveillance,
- intrusions or impairments of "critical cyber assets",
- threats to security, software, operations or physical facilities, or loss of 500 MW of generation for 30 minutes or more, or loss of 230 kV or larger for 60 minutes or more.

Yet, under the definition of Critical Cyber Asset, "Any event or failure (malicious or otherwise) that disrupts the proper operation of a critical cyber asset. Clearly these two definitions clash and yield confusion.

Response: Please see the general response to comments regarding incident response and reporting. The drafting team believes it adequately addresses this comment.

The NERC Reliability Standards Process Manual states "Urgent action may be appropriate when a delay in implementing a proposed standard or revision can materially impact reliability of the bulk electric systems." If many entities are already doing much of this work, and full compliance is not expected until 2005, how does this meet the urgent action requirement?

Regardless of the urgency or the perceived urgency, standards as important to the reliability of the bulk electric system such as these, should be developed with enough time to include the full review and comment of the industry so that proper focus and scope is achieved. The FRCC would recommend adopting this proposed standard as a reference document or white paper while the full standards process is utilized to develop the standard. In doing so, the industry will have the opportunity to comment and help clarify all of the questions that have been raised. The industry needs a cyber security standard, but it needs to be developed through the full standards setting process so that all of the issues can be addressed.

Response: Please see the general response to comments questioning the use of urgent action for this standard. The drafting team believes it adequately addresses this comment.

Gainesville Regional Utilities GVL
Segment: 5
Rep: Mark Lee Bennett
Negative

There are a couple of reasons I voted Negative.
1. The entire SAR is filled with Ambiguity, Some needs to Identify what exactly are Critical Cyber Assets and not leave to the individual utility.

Response: Please see the general response to comments regarding the definition of critical assets for further clarification.

2. The rush job in getting passed seems unnecessary according to the timeline.
3. The uncertainty does not allow entities to truly know what they need to do to be compliant and "self-certify" their performance, or to be able to determine the dollars necessary and budget accurately for any funding that might be needed. I would recommend adopting this proposed standard as a reference document or white paper while the full standards process is utilized to develop the standard. Once all this cyber information is in place what laws protect it from the Public's eye or someone out there that may have terrorist tendencies being able to Identify all of a utilities critical assets? It's like providing a menu for terrorists.

Response: Please see the general responses to comments questioning the use of urgent action for this standard and comments related to compliance to this standard. The drafting team believes these responses adequately address these comments.

Gainsville Regional Utilities GVL
Segment: 3
Rep: Roger Allen Westphal
Negative

Please see TECO Segment 5 comments. Additionally:

Notes from FRCC: The FRCC agrees with the need and supports the idea of developing a cyber security standard to protect the bulk electric system. However, for the reasons stated below we cannot support approving this as an urgent action standard.

1. The standard does not include enough specific information to determine the applicability of many of the requirements. Many questions have been raised and the answers were either not known, unclear, or contradictory. This uncertainty does not allow entities to truly know what they need to do to be compliant and "self-certify" their performance, or to be able to determine the dollars necessary and budget accurately for any funding that might be needed.

2. It has been stated repeatedly that the CIPAG believes that many entities are already implementing a lot of the requirements included in this standard. Partial compliance is acceptable by January 2004, and full compliance is not expected until January 2005. The NERC Reliability Standards Process Manual states "Urgent action may be appropriate when a delay in implementing a proposed standard or revision can materially impact reliability of the bulk electric systems." If many entities are already doing much of this work, and full compliance is not expected until 2005, how does this meet the urgent action requirement?

The FRCC would recommend adopting this proposed standard as a reference document or white paper while the full standards process is utilized to develop the standard. In doing so, the industry will have the opportunity to comment and help clarify all of the questions that have been raised. The industry needs a cyber security standard, but it needs to be developed through the full standards setting process so that all of the issues can be addressed.

Response: Please see appropriate responses to TECO Segment 5 comments and FRCC comments.

Hydro One Networks Inc
Segment: 3
Rep: Mike Penstone
Negative

Hydro One Networks Inc.
Segment: 1
Rep: Ajay Garg
Negative

Hydro One Networks Inc. votes against the approval of this standard. The standards fails to clearly identify that this standard applies to the elements that may have an adverse impact on the security, reliability and operations of the interconnected Bulk Power System.

The following points highlight the outstanding issues supporting this decision and also identified through NPCC internal review process;

The Monetary Sanction Matrix- There is an issue with the inclusion of this monetary sanction matrix and what its implications are. The NPCC CMAS has expressed concern over its inclusion and maintains letters of increasing severity for non-compliance are more effective in ensuring compliance. Failure of NERC to gain authority through reliability legislation will result in NERC Pursuing actions to implement "Plan B", a "voluntary" approach affording NERC the authority to perform these types of monetary sanctions and CMAS has indicated that the standard with the included matrix should not be supported by NPCC.

Hydro One suggests that sanctions related issues should be taken out of the "Standard" and dealt separately.

The existing standard as written fails to describe how the compliance process/auditing will work. The standard also does not specify the Region's role in the assessing of the compliance. It must be assumed that this standard will be assessed for compliance in the same manner as the existing NERC Compliance Program, i.e. NERC assesses the Regions, the Regions assess the Areas and the Areas assess the market participants. This needs clarification.

Response: Please see the general response to comments regarding compliance to this standard. The drafting team believes it adequately addresses the comments above.

Further clarification needs to be provided on what assets are considered to be covered under this standard. Who determines this and resolves any disputes which might result if an entity needs to make an investment in order to be compliant?

Response: Please see the general response to comments regarding the definition of critical assets. The drafting team believes it adequately addresses this comment. The entity required to comply must determine whether they have critical cyber assets. The decision to authorize capital investment to achieve compliance is a corporate one.

This standard as written, identifies its applicability to Transmission Operators and not Transmission Owners. This is problematic for a number of reasons. The weakest link in the operation of the Grid represents the vulnerability. If the owners of the equipment, who ultimately have final supervisory control of the devices, are not subject to the standard's requirement, then their systems represents the most likely vulnerability to the grid. The Control Areas also feel that if in fact the standard does not

apply to these entities but transfers the responsibility to the ISO's, CAs, for systems which they do not own, then the standard places unreasonable requirements to force compliance on their market participants. The Transmission Operators do not have the authority, in some cases, in their agreements to address this. There are also issues down at the market participant level that would make this standard extremely costly to implement for some.

Response: Please see the revised implementation plan for this standard. In 2004, only control areas and reliability coordinators will be required to assess their compliance to this standard.

There is a general difficulty in dealing with any critical asset owned by a "third party" (e.g. a communication system). More clarification is needed in this area. The standard also does not address shortcomings regarding third party software vulnerabilities.

Response: The standard does not address communications between perimeters, but rather deals with communication within a perimeter. Assets within the perimeter must be protected, regardless of their ownership.

The concept of a testing environment also needs clarification with respect to systems that realistically can't be replicated to create a "sandbox environment", i.e. SCADA System. The standard needs to be clarified in this area to state that "tabletop exercises" may suffice when practical test environments are not possible.

Response: The test environment need not exactly replicate the production environment, but should approximate the production environment. For example, a development/test EMS/SCADA can be configured with a test RTU or, as another approach, it may be possible to cut over an RTU for brief periods of time. The purpose for requiring the test environment is to permit testing of operating system updates, application updates, database model updates, and other modifications to the critical assets before they are installed on the production systems. A tabletop exercise, alone, is not sufficient for this testing. Modifications that cannot be tested in a development environment should be documented as part of the change management process as an exception to the standard, with sign off as required in Section 1201 of the standard.

The standard requires all entities to report full compliance or "substantial compliance" by the first quarter of 2004. The purpose of this first compliance self-certification is to establish a benchmark to determine if entities are making progress as they go forward in time. Concern exists that an entity reporting "substantial compliance", although not being specific in what area an inadequacy may exist, may be identifying some inherent weakness in the Cyber Security area of their system and identifying themselves as being more vulnerable than a fully compliant entity. Further, entities may have to incur substantial costs for a temporary standard, which is not clearly thought, while the new and a permanent standard may be substantially different.

Response: Please see the general response to comments regarding compliance to this standard. The drafting team believes it adequately addresses this comment.

The Standard contains some requirements that would require employee screening and although this is desirable, collective bargaining agreements (union contracts), federal, state and provincial regulatory requirements/restrictions make a meaningful generic set of requirements difficult to develop.

Response: Please see the general response to comments regarding background checks. The team believes it adequately addresses this comment.

Generally there are many positive attributes embedded in the proposed standard, however, it requires further development and requires clarification especially in the area of compliance, resources and costs.

In summary, it is agreed that there is an urgent need for a Security Guide as a Good Utility Practice while a permanent Standard is developed through SARs process.

Hydro-Quebec HQT
Segment: 1
Rep: MICHEL ARMSTRONG
Negative

The existing standard as written fails to describe how the compliance process/auditing will work. The standard also does not specify the Region's role in the assessing of the compliance. It must be assumed that this standard will be assessed for compliance in the same manner as the existing NERC Compliance Program, i.e. NERC assesses the Regions, the Regions assess the Areas and the Areas assess the market participants. This needs clarification.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment. No audits will be conducted in 2004.

Further clarification needs to be provided on what assets are considered to be covered under this standard. Who determines this and resolves any disputes which might result if an entity needs to make an investment in order to be compliant?

Response: Please see the general response to comments regarding the definition of critical assets. The drafting team believes it adequately addresses this comment. The entity required to comply must determine whether they have critical cyber assets. The decision to authorize capital investment to achieve compliance is a corporate one.

This standard as written, identifies its applicability to Transmission Operators and not Transmission Owners. This is problematic for a number of reasons. The weakest link in the operation of the Grid represents the vulnerability. If the owners of the equipment, who ultimately have final supervisory control of the devices, are not subject to the standard's requirement, then their systems represents the most likely vulnerability to the grid. The Control Areas also feel that if in fact the standard does not apply to these entities but transfers the responsibility to the ISO's, CAs, for systems which they do not own, then the standard places unreasonable requirements to force compliance on their market participants. The Transmission Operators do not have the authority, in some cases, in their agreements to address this. There are also issues down at the market participant level that would make this standard extremely costly to implement for some.

Response: Please see the revised implementation plan for this standard. In 2004, only control areas and reliability coordinators will be required to assess their compliance to this standard.

There is a general difficulty in dealing with any critical asset owned by a "third party" (e.g. a communication system). More clarification is needed in this area. The standard also does not address shortcomings regarding third party software vulnerabilities.

Response: The standard does not address communications between perimeters, but rather deals with communication within a perimeter. Assets within the perimeter must be protected, regardless of their ownership.

The concept of a testing environment also needs clarification with respect to systems that realistically can't be replicated to create a "sandbox environment", i.e. SCADA System. The standard needs to be clarified in this area to state that "tabletop exercises" may suffice when practical test environments are not possible.

Response: The test environment need not exactly replicate the production environment, but should approximate the production environment. For example, a development/test EMS/SCADA can be configured with a test RTU or, as another approach, it may be possible to cut over an RTU for brief periods of time. The purpose for requiring the test environment is to permit testing of operating system updates, application updates, database model updates, and other modifications to the critical assets before they are installed on the production systems. A tabletop exercise, alone, is not sufficient for this testing. Modifications that cannot be tested in a development environment should be documented as part of the change management process as an exception to the standard, with sign off as required in Section 1201 of the standard.

The standard requires all entities to report full compliance or "substantial compliance" by the first quarter of 2004. The purpose of this first compliance self-certification is to establish a benchmark to determine if entities are making progress as they go forward in time. Concern exists that an entity reporting "substantial compliance", although not being specific in what area an inadequacy may exist, may be identifying some inherent weakness in the Cyber Security area of their system and identifying themselves as being more vulnerable than a fully compliant entity.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment.

The Standard contains some requirements that would require employee screening and although this is desirable, collective bargaining agreements (union contracts), federal, state and provincial regulatory requirements/restrictions make a meaningful generic set of requirements difficult to develop.

Response: Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment.

Thank you for your attention to these concerns.

Illinois Power Co
Segment: 1
Rep: Shawn Schukar
Negative

Illinois Power is opposed to the Cyber Security Standard as written. While the need for cyber security should be a top priority for any company, Illinois Power does not feel that the proposed standard will effectively raise current security levels, and even adds a serious point for security to be compromised. Additionally, the amount of administrative overhead is excessive and adds little benefit.

The administrative responsibilities referred to in the measures and compliance monitoring Sections will require the time of high-level security personnel. This is an ineffective use of their time. This is a critical resource that should not be burdened with this requirement. Additionally, the policies and procedures will continually be lagging the implementation of new technologies, causing noncompliance.

Response: This standard sets minimum cyber security requirements. If cyber security measures that meet or exceed the requirements of this standard are already in place, the requirements of this standard have been fulfilled. The drafting team does not interpret the standard to require the addition of new administrative overhead.

The standard is purposely silent on the technology needed, to preserve the flexibility of those who must comply.

Having all security concerns for each company documented and collected at NERC or a person at NERC having all the knowledge about all weaknesses for all the companies adds a new point of concentration that might compromise security and increase liabilities to NERC. Security audit entities carry a high insurance for compromises at their end. With this standard, NERC cyber security becomes the one of the weakest links for many companies regardless of the strength of its cyber security. Because of concentration, compromises of Cyber security at NERC may be much farther reaching than any compromise at the individual company. As such any standard should recognize the need for limitation on information exposure outside the cyber security group at the company and should provide protection for any information exposed to NERC auditors. This protection should include both requirements that the information must be protected for years after the audit and even after an auditor leaves NERC and financial protection for the companies from NERC if this information is not protected.

Response: Confidentiality of compliance materials is addressed in the general response to comments regarding compliance to this standard. The drafting team believes it adequately addresses this comment.

ISO New England Inc ISNE
Segment: 2
Rep: Kathleen Goodman
Negative

Kathleen M. Goodman
Operations Compliance Coordinator

May 16, 2003

TO: Mr. Tim Gallagher
Director, Standards
NERC

Subject: ISO New England comments on the Urgent Action Cyber Security Standard (1200)

ISO New England strongly supports the initiative to provide industry controls for security of critical cyber assets. However, the NERC Cyber Security Standard, as currently proposed for urgent action, raises a number of issues that need to be addressed. Therefore, ISO New England cannot support adoption of this Standard under the urgent action adoption and implementation. ISO New England requests that the permanent standard, currently under development, fully consider all of the comments offered here.

- Within NPCC, the NERC Compliance process is conducted by NERC through NPCC, from NPCC through the Areas, and from the Areas to its members. This process is used in NPCC because NERC and the Regions may not have authority over all Area members and because the Areas are in constant contact with stakeholders. The Cyber Security Standard as written fails to describe how the compliance process will work and does not specify the various parties role in assessing compliance. Therefore, it must be assumed that this standard will be assessed for compliance in the same manner as the existing NERC Compliance Program. Utilizing this assumption, an infrastructure must be established and training provided to stakeholders on the new standard to ensure that all parties have an adequate opportunity to plan, budget for, and ensure compliance with the new standard.

- Appropriate time factors were not considered for this Standard's implementation. If compliance is measured based on the timeframe given in the NERC presentation materials, by the time there is a full compliance assessment, the permanent standard will be (or will be close to) ready. Also, the due process for the permanent standard, with stakeholder comments being sought during the drafting phase, removes any guarantees that the permanent standard will be similar to the Urgent Action Standard. Further, ISO New England believes it will harm the credibility of the compliance program, which our Participants currently support, if we ask our members to certify (even partial compliance) with a standard that was only approved four to six months earlier. ISO New England supports a phased-in implementation, with a minimum of a one-year pilot program, for all new Standards such as this one.

- The Standard, as posted, includes a matrix containing monetary sanctions. By a "yes" vote, there is an implied acceptance of the Standard in its entirety. However, it has always been the NPCC and ISO New England position that we do not support monetary sanctions due to the proven

effectiveness of non-monetary sanctions, which NPCC now uses. ISO New England reserves the right to not support any new NERC Standards that have monetary sanctions associated with them.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses the three comments above. The implementation of this standard will be consistent with the current provisions of the NERC Compliance and Enforcement Program. No penalties or sanctions will be applied in 2004, nor will any audits be conducted.

- Critical Asset identification is unclear. ISO New England and other Areas require further clarification of exactly which assets must meet the standard.

Response: Please see the general response to comments regarding the definition of critical cyber assets. The drafting team believes it adequately addresses this comment.

- ISO New England believes that there should be time allocated to develop a training effort to be put forth by NERC, the Regions, and the Areas before implementing a totally new compliance measure.

Response: Please see the general response to comments regarding compliance to this standard. The revised implementation plan for this standard states that in recognition of the fact that NERC does not have any existing requirements for cyber security, entities will not have to complete their self-certification forms until 2004 and that no penalties will be levied for noncompliance. Additionally, no audits will be conducted in 2004.

- Additionally, ISO New England believes the proposed standard is not sufficiently clear in some of its definitions and metrics, such that an accountable organization cannot effectively determine if they are adequately compliant. Specifically, ISO New England requests consideration of the definitions and metrics described below:

    - The definition for Critical Cyber Assets is too broadly worded, so that every cyber asset not excluded in the Standard's second sentence could by default be considered critical.

    - The definition for Cyber Security Incident is too broadly worded, so that even the simplest, non-security related equipment fault would require reporting.

    - It is not sufficiently clear whether the required documentation for security perimeters, access controls, monitoring, and information protection are meant to be overview documents or detailed procedures, which are themselves highly critical.

Response: Please refer to the general responses to comments regarding the definition of critical cyber assets and the general response to comments regarding incident response.

The documentation, which can be one or multiple related documents, needs to be sufficiently detailed to adequately describe the physical and logical environment in which the critical cyber asset resides, and to demonstrate that the requirements of the standard have been satisfied. The approach is left to the discretion of the entity. The documents, to the extent that they contain sensitive information, need to be protected from unauthorized disclosure.

- It is not clear what kind or types of maps are being referenced under Information Protection that would pertain to critical cyber assets.

Response: Maps, in this context, are depictions of the local and wide area networks such as might be used to demonstrate the electronic security perimeter.

- Under 1207 Personnel, section 2.2, mandating 90-day reviews is unnecessarily burdensome and inconsistent with its benefit. An annual review would be sufficient.

- Under 1208 and 1209 for monitoring access, there is no definition of what constitutes the act of monitoring.

Response: There are a variety of ways to monitor access to the critical assets and the standard, by design, does not attempt to prescribe specific methodologies.

- Under 1211 Training, clarity needs to be included as to whether the employee receives training annually, or whether the training program is reviewed annually. Also, clarification that training for certain, sensitive security processes, such as firewall management, cyber forensics, etc., is limited to those with a responsibility to perform such functions. Training of persons not in such a role of responsibility would, in and of itself, present a possible security risk.

Response: The intent on the standard is to provide security awareness training upon employment and periodically thereafter, at least annually, for any person who will physically or electronically access a critical asset. This is not technical task training as would be conducted for firewall administrators. Technical task training should be limited to those individuals with a direct responsibility for performing that task. The training material should be reviewed annually to ensure that it is kept current with company practices.

- Under 1213 Test Procedures, establishing a fully mirrored, isolated (stand-alone) test environment is cost prohibitive and cannot be sustained by ISO New England, its Satellites or SCADA centers. Requiring procedures for establishing controlled test environments would be more appropriate.

Response: This standard does not require a fully mirrored, isolated test environment; rather, a controlled, non-production system is to be used for testing.

While ISO New England strongly believes and supports the need for a Cyber Security Standard and generally there are many positive attributes embedded in the proposed Urgent Action Standard, the Standard requires further development and clarification especially in the area of compliance and definitions/measures.

LG&E Energy Transmission Services LGEE
Segment: 1
Rep: Bradley Young
Negative

Louisville Gas & Electric LGE
Segment: 6
Rep: Daryn Barker
Negative

Louisville Gas & Electric LGE
Segment: 5
Rep: Charles Martin
Negative

Overall, we believe that the intent of the new security standards is good, and implementation of the majority of these will ultimately result in better protection of the nation's energy infrastructure. However, the very broad scope of the standards as currently proposed, along with the ambiguity over specific inclusions/exclusions, will likely result in faulty, excessive, and inconsistent actions to address security concerns through 2004 and into 2005.

Response: Please see the general response to comments questioning the use of urgent action for this standard. The drafting team believes it adequately addresses this comment.

MAAC
Segment: 2
Rep: Bruce Balmat
Affirmative

MAAC supports the idea of developing a Cyber Security Standard to protect the bulk electric system. MAAC's support and its "Yes" vote, however, come with a number of concerns. The definition of "Critical Assets", what systems and entities the standard applies to, monitoring specific access control, and personnel background checks are but a few of the areas where uncertainty abounds with this proposal. There are likely to be a number of "No" votes due to this uncertainty.

Response: Please see the general response to comments regarding the definition of critical cyber assets. The drafting team believes it adequately addresses this comment.

Many entities have already established cyber security requirements, but many smaller entities have not, and are not sure whether the proposed standard applies to them. MAAC would suggest that monitoring of entities during the trial period (until a standard has been developed using the new NERC process) be limited to those entities performing the Reliability Coordinator functions and to those entities acting as Control Areas. Critical information and applicability of the standards measurements can be gained prior to rolling out the standard.

Response: Please see the general response to comments regarding compliance to this standard. The drafting team believes it adequately addresses this comment. The revised implementation plan states that only control areas and reliability coordinators must comply with this standard in 2004.

The importance of cyber security is recognized by all, but the approach of "little steps for little feet" probably is appropriate here. Don't try to incorporate everything for everyone in an "urgent" fashion as the first step. Perhaps this would help with the concerns of some of the folks with negative votes.

Manitoba Hydro
Segment: 1
Rep: Douglas Chapman
Affirmative

1. In the purpose the statement "To reduce risks to the reliability of the bulk electric system from any compromise of critical cyber assets" implies that "any" risk should be acted upon while in the definition of critical cyber assets certain cyber assets are excluded without explanation of their impact to the reliability of the bulk electric system. Also, in the definition of critical cyber assets the phrase "interacts with the bulk electric system operations" seems to imply any cyber assets in contact with the bulk electric system with no reference to the asset impact to the reliability of the bulk electric system.

These vague statements create confusion when attempting to identify critical cyber assets as required by "1202 — Critical Cyber Assets". The definition of "Critical Cyber Assets" needs clarification in the Urgent Action Standard. Items to consider are listed as bullets below and in point 2, also below

- as mentioned above, the term "interact" should be changed, since it does not imply any reliability risk. Replacing this term with "ensure interconnected electric grid operation survivability" might clarify the definition.
- an element of survivability is captured in "ensure capability to recover from a blackout"
- the importance of each critical cyber asset surviving or continuing operation during simultaneous threat scenarios should be considered

Response: Please see the general response to comments regarding the definition of critical cyber assets for clarification. The drafting team believes it adequately addresses this comment.

2. Item 1214 — Electronic Incident Response Actions 2.2

Note that the NERC document entitled: Security Guidelines for the Electricity Sector: Treat and Incident Reporting contains the statement.

"A critical facility may be defined as any facility or combination of facilities, that if severely damaged or destroyed, would have a significant impact on the ability to serve large numbers of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the energy grid or would cause significant risk to public health and safety."

This provides another definition of a critical cyber asset – the definitions should be made as close as possible in all related NERC security documents.

Response: Please see the general response to comments regarding incident response and reporting. The drafting team believes it adequately addresses this comment.

Mirant Americas Energy Marketing LP MAEM
Segment: 6
Rep: Alan Johnson
Negative

Mirant Corporation
Segment: 5
Rep: Dorothea Stockstill
Negative

NERC Urgent Action Cyber Security Standard
Mirant Comments — May 19, 2003

Mirant agrees with and supports the stated purpose/industry need for a cyber security standard for the electric power industry. However, we believe that the standard as presently drafted is too vague and leaves too many questions unanswered, to be a meaningful standard. As such Mirant is compelled to oppose the implementation of the standard as written. Some of Mirant's specific concerns are as follows:

Compliance

- The lack of detail within the standard makes it difficult for an entity to understand exactly what it must do to comply with the standard, and hence to budget for any funds necessary to obtain compliance. It is essential that any standard intended for security of the electric sector be clear and consistent.
- The standard is not clear regarding what entity (NERC or the Regional Councils) will administer the compliance monitoring effort. Will an entity need to self-certify to NERC, the applicable regional reliability council(s) or both? The process should be made perfectly clear within the standard.

Response: Please see the general response to comments regarding compliance to this standard. The drafting team believes it adequately addresses this comment. The appropriate NERC Region will serve as the compliance monitor for this standard.

Employee Screening/Background Checks

- Over all it would not be difficult to develop a basic or "generic" process for conducting background checks. The difficulty lies in determining what to do with the information collected?
- The proposed standard is not clear regarding key questions such as:
  - Would periodic (annual, etc) follow-ups be required?
  - What does one do with existing employees who simply refuse to authorize a background check?
  - How does one address situations involving bargaining unit personnel (that may be contractually exempt)?
  - Since we are dealing with critical infrastructure protection, must all employees and contractors be US citizens?
  - How does the standard apply to contractors or leased labor? Consideration must be given to the cost of employee screening in addition to process and validation.

Conceptually background checks and employee screenings make sense. But the "who" and "how" questions must be answered within the standard prior to implementation.

Response: Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment.

Critical Cyber Asset

- Clarification is sought regarding what constitutes a critical cyber asset under this standard, particularly under those circumstances when particular configurations of SCADA, RTU, Distributed Control Systems, etc. are covered / not covered. From both the written standard and comments made during the May 5th Webcast, it is unclear as to the scenarios against which the standard is intended to protect by including or excluding particular configurations of the aforementioned systems.
- What happens if there is disagreement between an entity and the standard enforcement authority regarding asset classification? The standard does not include a process for addressing this concern.

Response: Please see the general response to comments regarding the definition of critical cyber assets. The drafting team believes it adequately addresses this comment.

Testing

- We would like to reiterate one of the comments made by NPCC regarding testing: "The concept of a testing environment also needs clarification with respect to systems that realistically can't be replicated to create a "sandbox environment", i.e. SCADA System. The standard needs to be clarified in this area to state that "tabletop exercises" may suffice when practical test environments are not possible."

Response: The test environment need not exactly replicate the production environment, but should approximate the production environment. For example, a development/test EMS/SCADA can be configured with a test RTU or, as another approach, it may be possible to cut over an RTU for brief periods of time. The purpose for requiring the test environment is to permit testing of operating system updates, application updates, database model updates, and other modifications to the critical assets before they are installed on the production systems. A tabletop exercise, alone, is not sufficient for this testing. Modifications that cannot be tested in a development environment should be documented as part of the change management process as an exception to the standard, with sign off as required in Section 1201 of the standard.

Finally, we concur with comments made by the FRCC that question the Urgent Action Status assigned to this standard. If many entities have already implemented many of the requirements included within the standard and full compliance with the standard is not required until January 2005, it doesn't seem that urgent action status is appropriate. We believe that the industry would be better served by developing a cyber security standard through the full standards setting process, enabling all issues to be fully addressed.

Response: Please see the general response to comments questioning the use of urgent action for this standard. The drafting team believes it adequately addresses this comment.

Respectfully Submitted,
Alan R. Johnson
Manager Business & Reliability Standards

Municipal Electric Authority of Georgia MEAG
Segment: 5
Rep: Roger Brand
Affirmative

Municipal Electric Authority of Georgia MEAG
Segment: 1
Rep: Jerry J Tang
Affirmative

While we agree with the standard, we would like the following issues considered.

Definitions Section:

1. Critical Cyber Assets should include that these standards do NOT apply to Nuclear Power Plants or energy management system RTUs.

Response: This standard does not apply to nuclear power plants. Please see the response to comments on the critical cyber asset definition for clarification.

2. Compliance Monitor could be clarified by indicating that this is the "regional" organization responsible for monitoring compliance with the NERC compliance program.

Response: As indicated by the commenters, the compliance monitors for this standard are the appropriate NERC Regions.

3. The definition of Cyber Security Incident is unnecessarily broad since it states 'malicious or otherwise' and therefore covers anything which affects the operation of the system. As written, it covers such non-security related events as hardware failures or planned outages. This definition, when taken in concert with the reporting requirements stated later in the standard, would require that each of these incidents be reported to the ES-ISAC. This would increase the 'noise level' of the ES-ISAC and thereby reduce its effectiveness considerably. The 'malicious or otherwise' language in the definition to should be changed to 'malicious or unknown' at the very least. If the incident had a known malicious cause (example: SQL Slammer worm) or after a reasonable amount of time (1 hr) a malicious cause can not be ruled out, then reporting the incident may be prudent.

Response: Please see the general response to comments regarding incident response and reporting. The drafting team believes it adequately addresses this comment.

Section 1207 — Personnel

1. Measure 2.2 which requires document updates within 24 hours is unrealistic. This should be a two step process. Security clearance should be removed within 24 hours under terminations for cause. Security clearance for terminations due to normal attrition should be removed within 5 working days. Any updates to documentation due to terminations should be updated within 5 working days.

Response: Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment.

2. Measure 2.3 is clarified so that individuals, such as control room operators, who have only the capability to use such assets, are not required by this standard to undergo background checks. We agree with and support this clarification.

Response: The clarification will be addressed in the development of the permanent cyber security standard. Thank you for the comment.

General

1. Much of the wording in the Standard is ambiguous and open to interpretation. For example: background checks are required with no guidance as to how they would be utilized.

Response: Please see the general response to comments regarding ambiguity in this standard. The drafting team believes it adequately addresses this comment.

2. For entities with older applications with less security functionality than the latest model it is not clear if the standard requires upgrading or modification or neither.

Response: The standard does not require equipment upgrades. However, in such situations, some alternative mitigating solutions must be identified and documented.

National Grid USA
Segment: 1
Rep: Herbert Schrayshuen
Negative

Niagara Mohawk NMPC
Segment: 3
Rep: Michael Schiavone
Negative

- The NPCC CMAS has indicated that there was no concrete evidence given in the proposed standard on how a "cyber" attack can jeopardize the security and reliability of the communication and computer systems used by the utility industry for the operation of the bulk power system.

Response: Please see the general response to comments questioning the use of urgent action for this standard. The drafting team believes it adequately addresses this comment.

- The Monetary Sanction Matrix — There is an issue with the inclusion of this monetary sanction matrix and what its implications are. The NPCC CMAS has expressed concern over its inclusion and maintains letters of increasing severity for non-compliance are more effective in ensuring compliance. Failure of NERC to gain authority through reliability legislation will result in NERC Pursuing actions to implement "Plan B", a "voluntary" approach affording NERC the authority to perform these types of monetary sanctions and CMAS has indicated that the standard with the included matrix should not be supported by NPCC.

- The existing standard as written fails to describe how the compliance process/auditing will work. The standard also does not specify the Region's role in the assessing of the compliance. It must be assumed that this standard will be assessed for compliance in the same manner as the existing NERC Compliance Program, i.e. NERC assesses the Regions, the Regions assess the Areas and the Areas assess the market participants. This needs clarification.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses the two comments above. The implementation of this standard will be consistent with the current provisions of the NERC Compliance and Enforcement Program. No penalties or sanctions will be applied in 2004.

- Further clarification needs to be provided on what assets are considered to be covered under this standard. Who determines this and resolves any disputes which might result if an entity needs to make an investment in order to be compliant?

Response: Please see the general response to comments regarding the definition of critical assets. The drafting team believes it adequately addresses this comment. The entity required to comply must determine whether they have critical cyber assets. The decision to authorize capital investment to achieve compliance is a corporate one.

- This standard as written identifies its applicability to Transmission Operators and not Transmission Owners. This is problematic for a number of reasons. The weakest link in the operation of the Grid represents the vulnerability. If the owners of the equipment, who ultimately have final supervisory control of the devices, are not subject to the standard's requirement, then their systems represents the most likely vulnerability to the grid. The Control Areas also feel that

if in fact the standard does not apply to these entities but transfers the responsibility to the ISO's, CAs, for systems which they do not own, then the standard places unreasonable requirements to force compliance on their market participants. The Transmission Operators do not have the authority, in some cases, in their agreements to address this. There are also issues down at the market participant level that would make this standard extremely costly to implement for some.

Response: Please see the revised implementation plan for this standard. In 2004, only control areas and reliability coordinators will be required to assess their compliance to this standard.

There is a general difficulty in dealing with any critical asset owned by a "third party" (e.g. a communication system). More clarification is needed in this area. The standard also does not address shortcomings regarding third party software vulnerabilities.

Response: The standard does not address communications between perimeters, but rather deals with communication within a perimeter. Assets within the perimeter must be protected, regardless of their ownership.

The concept of a testing environment also needs clarification with respect to systems that realistically can't be replicated to create a "sandbox environment", i.e. SCADA System. The standard needs to be clarified in this area to state that "tabletop exercises" may suffice when practical test environments are not possible.

Response: The test environment need not exactly replicate the production environment, but should approximate the production environment. For example, a development/test EMS/SCADA can be configured with a test RTU or, as another approach, it may be possible to cut over an RTU for brief periods of time. The purpose for requiring the test environment is to permit testing of operating system updates, application updates, database model updates, and other modifications to the critical assets before they are installed on the production systems. A tabletop exercise, alone, is not sufficient for this testing. Modifications that cannot be tested in a development environment should be documented as part of the change management process as an exception to the standard, with sign off as required in Section 1201 of the standard.

The standard requires all entities to report full compliance or "substantial compliance" by the first quarter of 2004. The purpose of this first compliance self-certification is to establish a benchmark to determine if entities are making progress as they go forward in time. Concern exists that an entity reporting "substantial compliance", although not being specific in what area an inadequacy may exist, may be identifying some inherent weakness in the Cyber Security area of their system and identifying themselves as being more vulnerable than a fully compliant entity. Further, entities may have to incur substantial costs for a temporary standard, which is not clearly thought, while the new and a permanent standard may be substantially different.

Response: Please see the general response to comments regarding compliance to this standard. The drafting team believes it adequately addresses this comment.

The Standard contains some requirements that would require employee screening and although this is desirable, collective bargaining agreements (union contracts), federal, state and provincial regulatory requirements/restrictions make a meaningful generic set of requirements difficult to develop.

Response: Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment.

Nebraska Public Power District NPPD
Segment: 1
Rep: Alan Boesch
Negative

Urgent Action Standard 1200 Cyber Security

DEFINITIONS

Critical Cyber Assets: Those computers, including installed software and electronic data, and communication networks that support, operate, or otherwise interact with the bulk electric system operations. This definition currently does not include process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations.

Response: Please see the general response to comments regarding the definition of critical cyber assets. The drafting team believes it adequately addresses this comment.

Cyber Security Incident: Any event or failure (malicious ~~or otherwise~~) that disrupts the proper operation of a critical cyber asset.

Response: Please see the general response to comments regarding incident response and reporting. The drafting team believes it adequately addresses this comment.

1207 Personnel
2.3.The responsible entity shall conduct background screening of personnel consistent with the degree of access they are granted, in accordance with federal, state, provincial, and local laws.

Response: If vendors have unescorted access to critical cyber assets, then background checks are necessary. Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment.

5. Levels of Noncompliance
5.1. Level one:
5.1.1. List of personnel with their access control rights list is available, but has not been updated or reviewed for more than three months but less than six months; or
5.1.2.One instance of personnel termination (employee, contractor or service vendor) in which the access control list was not updated within 24 hours.

Response: Please see the general response to comments regarding compliance to this standard. The drafting team believes it adequately addresses this comment.

1208 . Monitoring Physical Access
2. Measures
2.1. The responsible entity shall maintain a document identifying its tools and procedures for physical access monitoring. This document shall verify that the tools and procedures are functioning and being used as planned.
2.2. The responsible entity shall document physical access to critical cyber assets via access records (e.g., logs). Access records shall be verified against the list of access control rights or controlled by video or other physical monitoring.

Response: The intent of verifying access records against access control rights is to identify denied access attempts and respond accordingly, as well as to document the effectiveness of access controls.

1209 . Monitoring Electronic Access
2.2. The responsible entity shall document electronic access to critical cyber assets via access records (e.g., logs). Access records shall be verified against the list of access control rights.

Response: The intent of verifying access records against access control rights is to identify denied access attempts and respond accordingly, as well as to document the effectiveness of access controls.

1213 Test Procedures
1. Requirement
The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall establish test procedures and acceptance criteria to ensure that critical cyber assets installed or modified comply with the security requirements in this standard. Test procedures shall require that testing and acceptance be conducted in an isolated test environment.

Response: Testing in an isolated environment is necessary to protect production systems from unintended consequences related to the change. The test environment need not exactly replicate the production environment, but should approximate the production environment.

1216 Recovery Plans
2.2. The responsible entity shall maintain a document verifying that the action plan is ~~exercised via drill~~ reviewed via training at least annually.

Response: The drafting team believes it is imperative to test recovery plans so there is assurance that it will work as expected in an actual emergency.

New York Power Authority NYPA
Segment: 1
Rep: Ralph Rufrano
Negative

Outstanding issues contributing to NYPA's decision are:

Although NYPA supports the need for a NERC Cyber Security Standard, the following most applicable NPCC comments tailored to an NYPA perspective have been added.

The Monetary Sanction Matrix- There is an issue with the inclusion of this monetary sanction matrix and what its implications are. The NPCC CMAS has expressed concern over its inclusion and maintains letters of increasing severity for non-compliance are more effective in ensuring compliance.

The existing standard as written requires clarification to more fully describe how the compliance process/auditing will work. The standard needs to more clearly specify the Region's and Area's role(s) in the assessing of compliance.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses these comments. There will be no sanctions or penalties for non-compliance in 2004. The appropriate NERC Region will serve as the compliance monitor for this standard.

New York State Department of Public Service
Segment: 9
Rep: Paul B. Powers
Affirmative

- Implementation guidelines should: clarify the exact assets which are required to comply with the standard; and, clarify that sanctions for the emergency standard are not monetary.

Response: Please see the general response to comments regarding compliance to this standard. The drafting team believes it adequately addresses this comment.

- Reports that include identified deficiencies need to be treated as confidential information.

Response: Please see the general response to comments regarding compliance to this standard. The drafting team believes it adequately addresses this comment.

- Implementation phase should monitor whether transmission owners cooperate with the transmission operators in complying with the standard; if there are problems, transmission owners should be included as responsible parties in the permanent standard.

Response: Your comments will be forwarded to the drafting team developing the permanent cyber security standard.

- If the background check provision conflicts with local union contracts or regulatory mandates, the responsible party should report the conflict along with a strategy to rectify the situation; the report would be considered compliance for this temporary standard.

Response: Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment.

New York State Reliability Council
Segment: 2
Rep: Alan Adamson
Negative

The New York State Reliability Council (NYSRC) votes in the negative on the proposed Urgent Action Standard on Cyber-Security. The NYSRC's negative vote is based on the following reasons:

- The NYSRC supports the need for a NERC cyber-security standard, and appreciates NERC's interest in moving expeditiously in the consideration and adoption of a cyber-security standard. The NYSRC, however, also believes that an effective cyber-security standard must be based on a full understanding of the implications of the proposed standard, including how it will relate to cyber-security measures currently in effect, or in the process of being implemented, in the electric power industry. The NYSRC believes NERC should verify with the parties responsible for the operation of the nation's integrated power system, including utilities, generators, ISOs, and RTOs, that the proposed standard will be effective in increasing security beyond the security enhancing efforts that are now being implemented and will not interfere with or detract from those efforts.

Response: Please see the general response to comments regarding ambiguity in this standard. The drafting team believes it adequately addresses this comment.

- The NYSRC also notes that the proposed standard does not adequately explain how auditing and compliance assessment for the standard would be implemented. For example, the standard does not specify the Region's role in assessing compliance. We assume that the standard would be affected in a manner consistent with the existing NERC Compliance Program, i.e., NERC assesses the Regions, the Regions assess the Areas, and the Areas assess the market participants. However, the auditing and compliance process related to the standard should be clearly defined.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment. No audits will be conducted in 2004. There will be no sanctions or penalties for non-compliance in 2004.

Northeast Power Coordinating Council
Segment: 2
Rep: Edward Schwerdt
Negative

NPCC supports the initiative to provide an electric industry standard for the security of critical cyber assets; however, NPCC cannot support the proposed NERC Cyber Security Standard as written for the following reasons:

- NPCC does not support the inclusion of a monetary sanction matrix. The sanctions identified within the subsections of the standard reference letters for varying degrees of severity of non-compliance. This approach has proven to be effective in the Northeast.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment.

- The definition of a critical cyber asset needs further clarification.

Response: Please see the general response to comments regarding the definition of critical cyber assets. The drafting team believes it adequately addresses this comment's function.

- The standard applies to transmission operators who may not own the critical cyber asset.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment.

- Section 1213, testing environment, could place cost prohibitive requirements on entities.

Response: Testing in an isolated environment is necessary to protect production systems from unintended consequences related to the change. The test environment need not exactly replicate the production environment, but should approximate the production environment.

- The definition of a cyber security incident is too broadly worded, so that non-security related equipment faults could require reporting.

Response: Please see the general response to comments regarding incident response and reporting. The drafting team believes it adequately addresses this comment.

- Notification of an entity's non-compliance could publicize a potential weakness in the cyber systems of that entity.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment. Compliance information will be treated as confidential.

- Employee screening needs to consider federal, state, provincial, and collective bargaining agreement constraints.

Response: Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment.

- Compliance assessment/auditing responsibilities need further clarification.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment.

Northeast Utilities NU
Segment: 1
Rep: Roger C. Zaklukiewicz
Affirmative

Since no financial sanctions will apply, the sanctions table included with the Urgent Actions Standard should only include the Letter Sanction description and not the Fixed Dollar and Dollars per MW or Tables Section.

Confirmation that the audit teams utilized by NERC and the Regional Councils will have the appropriate clearances to view and evaluate sensitive, audit-related information.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment. No audits will be conducted in 2004. No penalties or sanctions will be issued for non-compliance in 2004.

NorthWestern Energy NWMT
Segment: 1
Rep: Ted Williams
Negative

We are especially concerned with sections 1207 - Personnel and 1208 — Monitoring Physical Access since the Standard does not unambiguously specify the intent. The document must clarify who and how these measures are expected to be implemented. The proposed language is not explicit regarding personnel that must receive background checks. The 'Common Questions' document provides some insight but the Standard must be revised to clarify the intent. The physical monitoring measure might be interpreted to require video surveillance of access doors. While this is a problem at our control center, it will quickly become impossible as the 'cyber boundary' moves to select substations. There must be a better way to verify compliance with physical access controls.

Response: Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment.

The standard does not require video surveillance; monitoring techniques employed are at the discretion of the entity.

Nova Scotia Power NSPI
Segment: 1
Rep: David D Little
Negative

Nova Scotia Power NSPI
Segment: 5
Rep: Mark William Savory
Negative

In support of the NPCC CP9 recommendation and based on information compiled from NPCC's Task Forces, and its Compliance Monitoring and Assessment Subcommittee (CMAS), and also on information discussed at a recent Canadian Electricity Association (CEA) meeting, I am voting against the proposed SAR.

The following points highlight the outstanding issues supporting this decision:

The Monetary Sanction Matrix- There is an issue with the inclusion of this monetary sanction matrix and what its implications are. The NPCC CMAS has expressed concern over its inclusion and maintains letters of increasing severity for non-compliance are more effective in ensuring compliance. Failure of NERC to gain authority through reliability legislation will result in NERC Pursuing actions to implement "Plan B", a "voluntary" approach affording NERC the authority to perform these types of monetary sanctions and CMAS has indicated that the standard with the included matrix should not be supported by NPCC.

The existing standard as written fails to describe how the compliance process/auditing will work, and does not provide sufficient guidance to allow an objective audit to be conducted. The standard also does not specify the Region's role in the assessing of the compliance. It must be assumed that this standard will be assessed for compliance in the same manner as the existing NERC Compliance Program, i.e. NERC assesses the Regions, the Regions assess the Areas and the Areas assess the market participants. This needs clarification.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses the two comments above. The implementation of this standard will be consistent with the current provisions of the NERC Compliance and Enforcement Program. No penalties or sanctions will be applied in 2004.

Further clarification needs to be provided on what assets are considered to be covered under this standard. Who determines this and resolves any disputes which might result if an entity needs to make an investment in order to be compliant.

Response: Please see the general response to comments regarding the definition of critical assets. The drafting team believes it adequately addresses this comment. The entity required to comply must determine whether they have critical cyber assets. The decision to authorize capital investment to achieve compliance is a corporate one.

There is a general difficulty in assuring compliance when dealing with any critical asset owned by a "third party" (e.g. a communication system). More clarification is needed in this area. The standard also does not address shortcomings regarding third party software vulnerabilities.

Response: The standard does not address communications between perimeters, but rather deals with communication within a perimeter. Assets within the perimeter must be protected, regardless of their ownerships.

The concept of a testing environment also needs clarification with respect to systems that realistically can't be replicated to create a "sandbox environment", i.e. SCADA System. The standard needs to be clarified in this area to state that "tabletop exercises" may suffice when practical test environments are not possible.

Response: The test environment need not exactly replicate the production environment, but should approximate the production environment. For example, a development/test EMS/SCADA can be configured with a test RTU or, as another approach, it may be possible to cut over an RTU for brief periods of time. The purpose for requiring the test environment is to permit testing of operating system updates, application updates, database model updates, and other modifications to the critical assets before they are installed on the production systems. A tabletop exercise, alone, is not sufficient for this testing. Modifications that cannot be tested in a development environment should be documented as part of the change management process as an exception to the standard, with sign off as required in Section 1201 of the standard.

The Standard contains some requirements that would require employee screening and although this is desirable, collective bargaining agreements (union contracts), federal, state and provincial regulatory requirements/restrictions make a meaningful generic set of requirements difficult to develop.

Response: Please see the general response to comments regarding background checks. The team believes it adequately addresses this comment.

Throughout the Urgent SAR for Cyber Security Standards, there are references to retention requirements for a variety of data from logs and processes. We have the following issues with these requirements:

a. There are retention variations throughout the standards. Some of the Standards require 6 months and others require 3 years of log retention. It is unclear to us as to the rationale for some of these retention periods.

b. In some cases, the required retention period does not align with our security management needs and therefore represents additional costs and effort for which we see no benefit nor improved security management.

We recommend that log retention periods be aligned with an entity's security needs and the compliance monitoring for this area accept a span of log retention anywhere from 6 months to 3 years based on an entity's need.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment.

The following comment is focused on the approach to Cyber Security Standards and is intended as input to the development of the permanent SAR for Cyber Security Standards.

We are concerned that the implementation of standards that make no allowance for an entity's risk/value drivers will not adequately nor appropriately provide the incentives and guidance required for an entity to manage their risks in the area of critical infrastructure management. Since the Urgent SAR for Cyber Security clearly positions itself around the reliability of the bulk electric systems, an entity's

compliance should be proportional to its ability to impact the reliability of the bulk electric system. When the focus is on standards versus risk management principles, there is always the chance that:

- Real risks may not be addressed because entities have not been required to demonstrate their relationship or impact to grid reliability through a risk analysis,
- The standards will be too much for some and will be burdensome,
- The standards are not sufficient for others but they will still appear to be in compliance with the standards.

Today with ever-changing energy markets, infrastructure and cyber risks, it is essential that there is something more fundamental and living at the foundation of any security standards we follow. We believe that the vehicle that could accomplish this is a risk analysis of each entity's influence on the stability and security of the bulk electric system. This analysis would form the fulcrum on which standards evolve.

It is our request that the development of the permanent SAR for Cyber Security take a risk/value approach, providing the tools to assist us analyze our risk profile in relation to the bulk electric system and then provide differential guidelines based on the result of this analysis. For example, a questionnaire that evaluated the risk to the bulk electric system and a simple classification system of low, med and high would allow each entity to evaluate and periodically re-evaluate their risks in this area. Then guidelines based on that low, med and high classification would allow focus on where the greatest risks are.

In summary, we agree that there is a need for a Security Standard and that generally there are many positive attributes embedded in the proposed standard, however, it requires further development and requires clarification especially in the area of compliance.

Response: These comments associated with risk analysis are noted and appreciated. These comments will be provided to the team drafting the permanent cyber security standard.

NYISO
Segment: 2
Rep: Karl Tammar
Negative

May 21, 2003

TO: Mr. Tim Gallagher
Director, Standards
North American Electric Reliability Council
SUBJECT: Comments on the Urgent Action Standard 1200 — Cyber Security

The NYISO has reviewed the Urgent Action Standard 1200 — Cyber Security Standard posted for balloting on through May 21, 2003. This document is a collection of comments associated with the standard to accompany a vote of 'No' for the first ballot.

The comments have been separated into two categories, one for issues directed at the standard and two for issues concerning approval of this standard as part of the existing compliance program. The NYISO feels that both issues are worth discussing in consideration of this being the first standard being balloted for the new Reliability Standards Process.

The NYISO fully supports a process that requires a standard level of effort towards cyber security for the electric power industry and we recognize the effort put forth by CIPAG in its development of this standard. However with the current NERC Compliance Program, we would like to raise the following issues concerning the standard and the compliance program it is be voted into.

Issues Concerning the Cyber Security Standard:

• Further clarification needs to be provided on what assets should be considered under this standard. Who determines this and resolves any disputes, which might result if an entity needing to make an investment in order to be compliant? A well-defined definition of cyber asset needs to be in place to ensure constant application of the standard. Regions and areas will require this clarification as they develop their programs to be able to ensure compliance with their participants.

Response: Please see the general response to comments regarding the definition of critical cyber assets. The drafting team believes it adequately addresses this comment.

• The current standard indicates that there will not be financial penalties assessed, however they are listed in the sanctions matrix attached to the standard. NY feels there are two options that should be considered in this and other standards: 1) The dollar amounts should be removed from the sanctions table attached to a standard or 2) If a common table is to be used, remove the table from each standard and include it in the process manual. Any variations to the common table may be discussed in the associated standard.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment.

• This standard as written, identifies its applicability to Transmission Operators and not Transmission Owners. This is problematic for a number of reasons. The weakest link in the operation of the Grid represents the vulnerability. If the owners of the equipment, who ultimately have final supervisory control of the devices, are not subject to the standard's requirement, then their systems represent the most likely vulnerability to the grid. The NYISO also feel that if in fact the standard does not apply to these entities

but transfers the responsibility to the ISO's, CA's, for systems which they do not own, then the standard places unreasonable requirements to force compliance on their market participants. The Transmission Operators do not have the authority, in some cases, in their agreements to address this.

Response: Please see the general response to comments regarding the definition of critical assets. The drafting team believes it adequately addresses this comment. The entity required to comply must determine whether they have critical cyber assets. The decision to authorize capital investment to achieve compliance is a corporate one.

• There is a general difficulty in dealing with any critical asset owned by a "third party" (e.g. a communication system). More clarification is needed in this area. The standard also does not address shortcomings regarding third party software vulnerabilities.

Response: The standard does not address communications between perimeters, but rather deals with communication within a perimeter. Assets within the perimeter must be protected, regardless of their ownerships.

• The concept of a test environment needs clarification. Establishing a fully mirrored, isolated test environment can be costly and difficult to sustain. Permitting for controlled test environments that also would allow the use of tabletop exercises for compliance is more realistic.

Response: The test environment need not exactly replicate the production environment, but should approximate the production environment. For example, a development/test EMS/SCADA can be configured with a test RTU or, as another approach, it may be possible to cut over an RTU for brief periods of time. The purpose for requiring the test environment is to permit testing of operating system updates, application updates, database model updates, and other modifications to the critical assets before they are installed on the production systems. A tabletop exercise, alone, is not sufficient for this testing. Modifications that cannot be tested in a development environment should be documented as part of the change management process as an exception to the standard, with sign off as required in Section 1201 of the standard.

• NY is unclear on why nuclear facilities are not included in this process. As with other assessments, if an entity is held to a higher standard by an organization (NRC) then the NERC process, that reporting requirement should be sufficient to indicate compliance at the NERC level. Will this exception open the door for other individuals with other reporting requirements?

Response: The NRC has regulatory authority over their jurisdictional entities and is in the process of developing its own cyber security requirements. Nuclear plants are not subject to this standard.

Issues Concerning the Compliance Program

• The standard requires all entities to report full compliance or "substantial compliance" by the first quarter of 2004. The purpose of this first compliance self-certification is to establish a benchmark to determine if entities are making progress as they go forward in time. Concern exists that an entity reporting "substantial compliance", although not being specific in what area an inadequacy may exist, may be identifying some inherent weakness in the Cyber Security area of their system and identifying themselves as being more vulnerable than a fully compliant entity.

• The content of this standard is new to NERC and its membership. Unfortunately the urgent action process does not define a field test. We believe a field test should be required do to the content of this standard. Cyber security issues have not been tested in any of the previous compliance programs and the

individuals involved with existing compliance programs are not familiar with cyber security issues. The field test step would allow entities to prepare for new requirements defined in the standards and avoid any exposure to non-compliance during that period. This would allow entities revise the standard and to prepare for full compliance enforcement.

• Compliance management in complex computing environments is a complex task. Information technology (cyber) changes at a rapid pace unlike the electric System Operations environment. The variety of hardware and software configurations adds to the cyber complexities.

• Staffing and maintaining technically competent people is significant. The NYISO is concerned about liability exposure should a defect not be detected during a compliance audit. Confidentiality to our computing environment is essential. Concerns regarding confidentiality within a process where competitive industry participants could have access is unacceptable. The NYISO prefers to limit our exposure to the premier third party auditors we, as the NYISO, have used in the past.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses these comments. No audits will be conducted in 2004.

Regards,
Karl Tammar
Administrator, Industry Affairs

Oklahoma Gas and Electric OKGE
Segment: 1
Rep: Mel Perkins
Affirmative

The issue of violations in consecutive evaluation periods is not a big item except in sections 1207, 1208, and 1209. Sections 1208 and 1209 are monitoring of physical and electronic access to the cyber system. Anytime that monitoring is accomplished by computer, ie card access, for either physical or cyber, it is susceptible to going down and failing to log information for a period of time. In fact, to expect a computer system to run for a full year with crashing is the height of optimism. So I think those two may have consecutive violations through no fault of the owner of the system.

Response: The drafting team will consider these concerns as it develops the permanent cyber security standard. Thank you for submitting them.

Section 1207 requires updating the access control list within 24 hours from the termination of an employee, contractor, or service vendor. The tight time frame could make it difficult to accomplish these changes in all cases, especially if the termination occurs on a Friday. I agree that the update is critical, especially if the termination is adversarial. But if the termination is the expiration of a contract or an employee retirement, it is not as critical. Perhaps the timing should be 72 hours under normal conditions and 24 hours (or one working day) for adversarial terminations.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes it adequately addresses this comment.

Otter Tail Power Company OTP
Segment: 1
Rep: Larry Larson
Affirmative

The compliance templates should be clear on what this applies to and to what extent. The FAQ stated that it doesn't apply to RTUs however, the definition of Critical Cyber Assets appears to include them.

Response: Please see the general response to comments regarding the definition of critical cyber assets. The drafting team believes it adequately addresses this comment.

Pacific Gas & Electric Company PGEU
Segment: 3
Rep: Kevin Dasso
Negative

Pacific Gas & Electric PGAE
Segment: 1
Rep: Chifong Thomas
Negative

The Pacific Gas and Electric Company is pleased to have had to opportunity to review the proposed Urgent Action Cyber Security Standard. As you may be aware, last year PG&E participated in the drafting of Appendix G of the proposed FERC Cyber Security Standard that was developed as part of the FERC Standard Market Design (SMD) initiative. As such, this company strongly supports the concept of a cyber security standard across the electricity sector and endorses NERC's efforts to promote such a standard.

At the same time, PG&E has concerns about of some of the language in the proposed standard and particularly with the manner in which we will be expected to achieve compliance. In general, we find the proposed language to be vague in some areas and some of the proposed measures to be unnecessarily burdensome and subject to interpretation while not materially improving the level of security. Our specific comments are attached.

We are sufficiently concerned that we are voting no on this initiative at this time until NERC can address these concerns which we think will be shared by a number of other companies. At the same time, we are willing to participate directly in any further efforts to resolve these concerns and refine these standards.

We look forward to the annual revisions in this Standard as NERC moves through its processes. If you have any questions, please contact Lyman Shaffer at 415 973-6920.

Response: Specific responses are embedded on the following pages.

These definitions will be posted and balloted along with the cyber security standards, but will not be restated in the cyber security standards. Instead, they will be included in a separate "Definitions" section containing definitions relevant to all standards that NERC develops.

1200 — CYBER SECURITY

(a) **Purpose**: To reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets.

(b) **Effective Period**: This urgent request standard will be in effect for one year from the date of NERC Board of Trustees adoption or until it is replaced by a permanent standard, whichever occurs first.

(c) **Applicability:** These cyber security standards apply to entities performing various electric system functions, as defined in the functional model approved by the NERC Board of Trustees in June 2001. NERC is now developing standards and procedures for the identification and certification of such entities. Until that identification and certification is complete, these standards apply to the existing entities (such as control areas, transmission owners and operators, and generation owners and operators) that are currently performing the defined functions. *(The underlying purpose of the development of this standard was to ensure that new market participants who would potentially access or otherwise interact with existing bulk transmission systems would have to meet minimal cyber security standards. The failure to include such participants limits the value of this proposed standard. To wait for the completion of the Standard Market Design NOPR to include such entities undermines the argument of the urgency for the development of this standard on an emergency basis. Perhaps language can be added which requires that any company or entity seeking to interact with such systems would be required to meet this standard or would otherwise be precluded from such interaction.*

Response: NERC recognizes the issue regarding market entities, but the primary role of NERC is centric to the reliability of the North American bulk electric systems. Specific application of standards to market entities is the role of FERC and NAESB. However, this does not mean that a bulk system operator can not set its own security requirements for cyber interconnection, particularly where such interconnection could allow potential negative impact on bulk power system operation.

The Appendix G development discussions leading up to this standard specifically excluded generation from the standard so why is it included in the applicability language.)

Response: The revised implementation plan for this standard states that only control areas and reliability coordinators will be required to complete self-certifications in 2004. Generation owners are not required to complete a self-certification in 2004.

1201 — Cyber Security Policy

(a) Requirement

(1) The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall create and maintain a cyber security policy for the implementation of this standard.

(2) The responsible entity shall assign a member of senior management with responsibility for leading and managing the entity's cyber security program. This person must authorize any deviation or exception from the requirements of this standard. Justification for any such deviation or exemption must be documented.

(b) Measures

(1) The responsible entity shall maintain its written cyber security policy stating the entity's commitment to protect critical cyber assets.

(2) The responsible entity shall review the cyber security policy at least annually.

(3) The current senior management official responsible for the cyber security program shall be identified by name, title, phone, address, and date of designation.

(4) The responsible entity shall maintain documentation justifying any deviations or exemptions authorized by the current senior management official responsible for the cyber security program.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the following available for inspection by the compliance monitor upon request:

(A) Written cyber security policy;

(B) The name, title, address, and phone number of the current designated senior management official and the date of his or her designation; and

(C) Documentation of justification for any deviations or exemptions. *(Shouldn't this involve substantive deviations rather than all deviations? This seems like an administrative nightmare if we ask a senior person to authorize any change in access control lists or other routine administrative matters. There should be some discretion here.)*

Response: If the routine process is compliant, there is no reason to document a deviation. If the routine process is not compliant, then the process must be documented as a deviation and an exception for the process must be authorized. If the process is deemed compliant but infrequent, occasion-specific deviation occurs, then each specific deviation must be noted. Note that if such deviation to the process is so frequent as to be a burden, perhaps redesign of the process would be a reasonable solution.

1203 — Electronic Security Perimeter

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall identify its electronic security perimeter(s).

(b) Measures

(1) The responsible entity shall maintain a document depicting the electronic security perimeter(s), all interconnected critical cyber assets, and all electronic access points to the interconnected environment(s). The document shall verify that all critical cyber assets are within the electronic security perimeter(s).

(2) The responsible entity shall review and update its document referenced in 1203(b)(1) at least annually or within 90 days of any significant modification of the network. *(I assume that networks get modified for a lot of reasons on a regular basis. This seems onerous administratively.*

Response: Some individuals involved in the drafting of the proposed standard that have IT operations experience felt that frequently updating changes is often easier than trying to identify all changes on an infrequent basis. If this evolves as a significant issue, it will be addressed in development of the permanent standard.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

(3) The responsible entity shall make the following available for inspection by the compliance monitor upon request:

(A) Document as described in 1203(b)(1); and

(B) Verification that necessary updates were made at least annually or within 90 days of a modification.

(e) Levels of Noncompliance

(1) Level one: Document exists, but document was not updated with known changes within the 90-day period.

(2) Level two: Document exists, but the document has not been updated or reviewed in the last 12 months.

(3) Level three: Document exists, but no verification that all critical assets are within the perimeter(s) described.

(4) Level four: No document exists.

(f) Sanctions

Sanctions will be letters only for noncompliance and shall be applied consistent with the NERC compliance and enforcement matrix (attached to the end of this urgent action standard for reference). No financial penalties will be assessed with this urgent action standard.

1207 — Personnel

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall identify all personnel, including contractors and service vendors, granted electronic or physical access to critical cyber assets.

(b) Measures

(1) The responsible entity shall maintain a list of all personnel granted access to critical cyber assets, including the specific electronic and physical access rights to the security perimeter(s).

(2) The responsible entity shall review the document referred to in 1207(b)(1) at least quarterly and update the document within 24 hours of any change. *(This seems onerous. Routine administrative transfers should be managed within two to three business days. Disciplinary transfers, layoffs, or cases where a person loses his/her access rights due to misconduct issues or instability, should be completed ASAP and no later than 24 hours.)*

Response: Please see the general response to comments questioning the use of urgent action for this standard. The drafting team believes it adequately addresses this comment.

(3) The responsible entity shall conduct background screening of personnel consistent wit the degree of access they are granted, in accordance with federal, state, provincial, and local laws. *(This is appears to be contrary to the discussions leading to the development of Appendix G. Companies should conduct background investigations of persons entering the company and the vast majority of them do so. The problem with this language is that it implies an obligation to background employees transferring into these positions or on a periodic basis thereafter. The practical impact of that position is that persons who have been otherwise satisfactory or even exemplary workers with no record of misconduct or other character defects at work may be barred from a position because of an arrest, temporary credit problem, or some other matter that is not germane to their job performance. This is particularly unsettling in a collective bargaining environment. Our belief is that the federal government should set standards in this area if they believe such actions are required rather than have the industry impose this condition. This can be corrected by stating that companies should have background investigation for new employees and protocols in place to intervene if there is evidence that the person has become unreliable.)*

Response: Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment. It is assumed that most bargaining unit limitations are enforceable through federal and state labor laws.

1208 — Monitoring Physical Access

(a) Requirements

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall monitor physical access to critical cyber assets 24 hours a day, 7 days a week.

(b) Measures

(1) The responsible entity shall maintain a document identifying its tools and procedures for physical access monitoring. This document shall verify that the tools and procedures are

functioning and being used as planned. *(How can this document verify that the tools and procedures are functional?)*

Response: The document defines tools and procedures. The documented procedures should include processes for periodic verification that the physical access controls and monitoring processes are functioning properly. Without such verification, there is no assurance that the access control system is working and that the controls are not being bypassed.

(2) The responsible entity shall document physical access to critical cyber assets via access records (e.g., logs). Access records shall be verified against the list of access control rights or controlled by video or other physical monitoring. *(Is the intent here that access records (e.g. card key system records) are reviewed on a continuous or periodic basis or is this a suggested audit activity – in either case it seems overly onerous.)*

Response: Access verification does not need to be continuous. It may be manual or automated, and may be routine, frequent snap-shots. The intent is to provide reasonable assurance that access controls continue to function properly, and to retain activity records for a period of time to provide forensic data in the event of an incident.

1209 — Monitoring Electronic Access

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall monitor electronic access to critical cyber assets, 24 hours a day, 7 days a week.

(b) Measures

(1) The responsible entity shall maintain a document identifying electronic access monitoring tools and procedures. This document shall verify that the tools and procedures are functioning and being used as planned. *(How can this document verify that the tools and procedures are functional?)*

Response: The document defines tools and procedures. The documented procedures should include processes for periodic verification that the physical access controls and monitoring processes are functioning properly. Without such verification, there is no assurance that the access control system is working and that the controls are not being bypassed.

(2) The responsible entity shall document electronic access to critical cyber assets via access records (e.g., logs). Access records shall be verified against the list of access control rights. *(Is the intent here that access records (e.g. system logs) are reviewed on a continuous or periodic basis or is this a suggested audit activity – in either case it seems overly onerous.)*

Response: Access verification does not need to be continuous. It may be manual or automated, and may be routine, frequent snap-shots. The intent is to provide reasonable assurance that access controls continue to function properly, and to retain activity records for a period of time to provide forensic data in the event of an incident.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.

(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for six months. The compliance monitor shall keep audit records data for three years.

(3) The responsible entity shall make the following available for inspection by the compliance monitor upon request:

(A) Document as described in 1209(b)(1);

(B) Records of electronic access to critical cyber assets; and *(this is overly onerous as these systems are accessed continuously and access records may be purged periodically due to space limitations/general housekeeping))*

Response: Access records do not have to be maintained in an on-line format. They can be transferred to off-line storage for the 6-month retention period. In addition, the standard does prescribe the level of detail that must be logged.

1210 — Information Protection

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall protect information associated with critical cyber assets and the policies and practices used to keep them secure.

(b) Measures

(1) The responsible entity shall maintain a document identifying the access limitations to sensitive information related to critical cyber assets. At a minimum, this document must address access to procedures, critical asset inventories, maps, floor plans, equipment layouts and configurations. *(This is overly onerous as it involves access to system/records not otherwise covered by this standard (e.g. CAD systems containing building drawings, asset records in SAP, etc.)*

Response: This requirement is limited to the sensitivity of information as it specifically relates to critical cyber assets. General building plans are not meant to be included. However, those plans that identify the perimeter and access points and controls for critical cyber assets are included, for example. A general asset inventory database (SAP, etc.) is not necessarily that sensitive. But a database that clearly identifies the criticality of specific cyber assets is sensitive.

1212 — Systems Management

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall establish systems management policies and procedures for configuring and securing critical cyber assets. At a minimum, these policies and procedures shall address:

(1) The use of effective password management that periodically requires changing of passwords, including default passwords for newly installed equipment;

(2) The authorization and periodic review of computer accounts and access rights;

(3) The disabling of unauthorized, invalidated, expired, or unused computer accounts and physical access rights;
(4) The disabling of unused network services and ports;
(5) Secure dial-up modem connections;
(6) Firewall management;
(7) Intrusion detection processes;
(8) Security patch management;
(9) The installation and update of anti-virus software;
(10) The retention and review of operator logs, application logs, and intrusion detection logs; and
(11) Identification of vulnerabilities and responses.

(b) Measures

(1) The responsible entity shall maintain a document identifying system management policies and procedures.

(2) The responsible entity shall review and update the document referred to in 1212(b)(1) as necessary and at least annually.

(3) The system management policies and procedures document shall address all items in requirement 1212(a).

(4) The responsible entity shall implement system management policies and procedures as described in the system management policies and procedures document.

(c) Regional Differences

None identified.

(d) Compliance Monitoring Process

(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.
(2) The performance-reset period shall be one calendar year. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.
(3) The responsible entity shall make the following available for inspection by the compliance monitor upon request:
(A) Document as described in 1212(b)(1); and
(B) Verification that system management policies and procedures are being followed.

(How? Actual documentation/verification of this is overly onerous)

Response: The document defines tools and procedures. The documented procedures should include processes for periodic verification that the physical access controls and monitoring processes are functioning properly. Without such verification, there is no assurance that the access control system is working and that the controls are not being bypassed.

1213 — Test Procedures

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall establish test procedures and acceptance criteria to ensure that critical cyber assets installed or modified comply with the security requirements in this standard. Test procedures shall require that

testing and acceptance be conducted in an isolated test environment. *(This is ok for new systems or major system modifications however this is not practical for routine type modifications that occur on a daily basis. Also on our EMS and other systems most work is pretested on a development system however this is intentionally not fully isolated from the production system.)*

Response: Electronic isolation is not required by this standard; rather, a controlled non-production system is to be used for testing. The standard does not require that the test environment be outside the electronic security perimeter.

1214 — Electronic Incident Response Actions

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall define electronic incident response actions, including roles and responsibilities assigned by individual or job function.

(b) Measures

(1) The responsible entity shall maintain a document defining the electronic incident response action, including actions, roles and responsibilities.

(1) The document in 1214(b)(1) shall require that incidents involving critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the *NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure*. *(This is a departure from existing NERC policy as such reporting is presently voluntary for both cyber and physical security incidents. Many companies have previously raised objections to the one hour reporting criteria under the existing standards but have been largely ignored. The objections have been based on the fact that the cause of a physical or cyber problem on a transmission system is very often not determined within the one hour reporting window. As a result, this should either remain voluntary or the reporting criteria should be changed to only require reporting in which an incident is known to be malicious in nature or there is reason to believe that it is. Without those qualifications, this requirement will become onerous due to the resulting over reporting. In addition, the result would potentially create such a volume of spurious reports that real incidents will be difficult to identify.)*

Response: The reporting SOP has been in place for several years. NERC is aware of the differing views on the SOP criteria. The only difference between current practice and the requirements of this standard is that reporting will no longer be voluntary.

1215 — Physical Incident Response Actions

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall define physical incident response actions, including roles and responsibilities assigned by individual or job function.

(b) Measures

(1) The responsible entity shall maintain a document defining the physical incident response action, including actions, roles and responsibilities.

(2) The document in 1215(b)(1) shall require that incidents involving physical assets used to protect critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the *NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure. (Same objection as that posed in Section 1214.)*

Response: Please see response to 1214 comment.

1216 — Recovery Plans

(a) Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall create action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident. Each responsible entity shall exercise these plans at least annually. The plans and procedures shall define roles and responsibilities by individual or job function. *(Not a good idea to actually perform many of the procedures that you would follow to re-establish systems as this would entail shutting down the system, etc. for the purpose of a drill which is a not a wise risk (especially with older systems). Faking bringing a system up provides little value. Similar practice/experience can be gained by re-establishing systems following scheduled maintenance, following hardware failures, etc. Also some of our DR plans do not focus on the Cyber system itself but the continuation of the business function)*

Response: NERC understands that a full shutdown and re-initialization of system operations is not practical or desirable. The intent is to validate cyber recovery procedures as much as possible, and to ensure necessary personnel are proficient in those procedures. The use of tabletop exercises and structured walkthroughs may be appropriate in some cases. NERC agrees that utilizing recovery procedures for re-establishing systems following scheduled maintenance, following hardware failures, etc., can satisfy validation and training needs.

PP&L PAPL
Segment: 1
Rep: Ray Mammarella
Affirmative

PPL Generation
Segment: 5
Rep: Mark Heimbach
Affirmative

PPL Corp. agrees with the need and supports the idea of developing a cyber security standard to protect the bulk electric system. The industry thanks the CIPAG for their work and efforts to focus the electric industry on cyber security standards to protect the bulk electric system. PPL Corp. is voting YES because we realize that a standard of this type will eventually be implemented. However, we are also submitting the comments below.

1. The standard does not include enough specific information to determine the applicability of many of the requirements. Many questions have been raised and the answers were either not known, unclear, or contradictory. This uncertainty does not allow entities to truly know what they need to do to be compliant and "self-certify" their performance, or to be able to determine the dollars necessary and budget accurately for any funding that might be needed. It is essential that any standard intended for security of the electric sector be clear and consistent.

Response: Please see the general response to comments regarding ambiguity in this standard. The drafting team believes it adequately addresses this comment.

2. 1201a lists several entities that are affected by this standard. This list is confusing. Specific examples need to be included.

Response: The implementation plan for this standard has been revised to add more clarity in this area. In 2004, only control areas and reliability coordinators will be required to assess their compliance to this standard.

3. Confusion still remains in the definition of "critical cyber assets". Further clarification of statements regarding what systems should be included, such as SCADA, EMS, ICCP, Tagging, IDC, Oasis is needed. Does this include upstream systems that may electronically feed source data to these control systems? Further written clarification is required to determine whether entities dealing in areas such as market function would be required to comply with this standard.

Response: Please see the general response to comments regarding the definition of critical cyber assets. The drafting team believes it adequately addresses this comment.

4. The words "any" and "otherwise" in the definition of "cyber security incident" lead to broad interpretations. Under this definition, any disruptive event albeit non-intentional or malicious, would be classified as an "incident." A simple reboot of a system meets the criteria defined within "any" and also in "otherwise." Consequently, reboots, disk failures, or memory lockups - do - disrupt the "proper operation of a critical cyber asset", yet they are common to production environments. Under this definition any of these common events would constitute an "incident" dealing with a cyber assets. Also, the term "failure" should be clearly defined. As stated above, failures of cyber assets that are caused by non-malicious activities (i.e. software testing, or hardware failure) would be a reportable offense under section 1214.2.2 of this standard. We would recommend the definition be changed to the following: An event of

unknown origin or a significant failure that disrupts the proper operation of a critical cyber asset, causing the reliability of the bulk electric system to be adversely affected.

Response: Please see the general response to comments regarding incident response and reporting. The drafting team believes it adequately addresses this comment.

5. The intent of this standard is "to reduce risk to the reliability of the bulk electric system" from cyber incidents or physical incidents as they relate specifically to the "critical cyber assets." One area of concern however, is the verbiage "from any compromise of critical cyber assets."
This definition lends itself to include non-malicious production glitches, which are often a reality in production environments. The definition also broadens the scope of the standard to include not only the reliability of the overall system itself, but also the reliability of each cyber asset. We would recommend the purpose be changed to the following: To reduce risks to the reliability of the bulk electric systems from intentional and/or malicious acts, which significantly compromise the reliability of the system.

Response: The drafting team does not envision a non-malicious production "glitch" as a compromise of a critical cyber asset. Clearly the failure of a critical asset due to something as common and non-malicious as a hard disk crash is not a security concern, although much if not all of the recovery plans required by Section 1216 would be appropriate for both malicious and non-malicious events.

6. Standards 1208 and 1209 - Monitoring Physical and Electronic Access

Couldn't these two requirements be combined into one? These requirements states that monitoring will take place 24 hours per day, 7 days per week, and that logs on access to critical assets will be collected and verified against lists of authorized users. Access logs are voluminous, and if the standard is to be interpreted literally, it would be impossible to monitor, verify, and report on such logs; other than on a small-random-sample basis without the use of automated correlation tools. What constitutes compliance for monitoring of physical and electronic access? Is existence of logs for forensic purposes and periodic review sufficient? For how long must Video and other Physical data be stored to prove compliance?

Response: The intent of Section 1208, in conjunction with sections 1205 and 1206, is to ensure that only authorized personnel (who have completed the required background check and have an approved need) are granted unescorted access to the critical assets. There are a number of ways that physical access can be monitored and verified per the standard. The most common is an electronic access control system (such as a card reader) with individualized access credentials. The person requesting access presents the credentials (swipes the badge) at which time the access control system validates the credentials, determines whether or not the person is permitted entry, and unlocks the door as appropriate. An electronic log entry of this action, identifying the date, time, person (badge identifier), and which door was accessed is recorded. The electronic system is doing the authentication and the monitoring and thus satisfies the requirements of the standard. Should something unexpected happen, the logs can be quickly reviewed to determine who had access. If there is a concern that the person requesting access is not using their assigned badge, a CCTV monitoring and recording system can also be employed and would serve as an additional "log" source. The minimum data retention requirement is six months, as specified in Section 1208, Paragraph 4.2. Employing both the electronic access control system and the CCTV system exceeds the minimum requirements of this standard. Employing just a CCTV system without pre-entry validation of the credentials (such as by a local or remotely sited security guard) would not meet the standard. As with physical access monitoring, the use of electronic authentication that supports logging is an acceptable method to satisfy the requirements of Section 1209. The person requesting electronic access presents a set of credentials such as username and password (the standard does not mandate multi-

factor authentication). The credentials are validated and the user rights list associated with that identity defines what the user can do. The system will continuously monitor the user's activities in that it will not permit the user to access data or perform functions for which there is no authorization. At a minimum, recording of the log-on and log-off events will satisfy the logging requirement. The use of additional operating system logging, as well as application, database, firewall, and IDS logging is also acceptable and encouraged. To the extent that activity logging is employed, the standard is applicable, particularly with respect to data retention.

7. PPL believes that PJM, not NERC, should be the entity that we interface with for any and all activities related to this Cyber Security Standard.

Response: NERC's Regions are the compliance monitors for this standard.

Regardless of the urgency or the perceived urgency, standards as important to the reliability of the bulk electric system such as these, should be developed with enough time to include the full review and comment of the industry so that proper focus and scope is achieved. In doing so, the industry will have the opportunity to comment and help clarify all of the questions that have been raised. The industry needs a cyber security standard, but it needs to be developed through the full standards setting process so that all of the issues can be addressed.

Response: Please see the general response to comments regarding the use of urgent action for this standard. The drafting team believes it adequately addresses this comment.

Public Service Electric and Gas Company
Segment: 3
Rep: Murty Bhavaraju
Negative

It appears the proposal requires lots of documentation but its effectiveness to improve cyber security was not adequately shown.

Response: This is intended as a base-line standard, with the goal of achieving consistent cyber security implementation across the bulk electric systems of North America to ensure reliability.

Public Service Electric and Gas Company
Segment: 1
Rep: Arthur Giardino
Negative

The need for a Cyber Security Standard is evident, however, in the haste to proceed as an urgent action, the proposed standard is not adequate to meet the goal to reduce risk of compromise of critical cyber assets.

PSE&G endorses and supports the comments offered by the FRCC.

In addition, we are concerned that this standard is documentation based, not results or performance based. For example, we must certify that all critical cyber assets are within the electronic security perimeter. Unfortunately, there is no requirement to assess the effectiveness of the electronic security perimeter. The levels of non-compliance apply only to missing or incomplete paper. The same omission is also found in the physical security provisions and the monitoring of physical and electronic access. Shouldn't a breech of security be a non-compliance? What about requiring corrective action for implementation deficiencies. The systems management section (1212) suffers from the same omission. Nicely worded policies and procedures may not be effective. The documentation should address the results obtained, not just the paper with words on it as specified in the measures for this requirement.

The requirement for background screening of individuals is extremely vague as to applicability and the depth of investigation. The criteria for disallowing an individual access must be established and be consistent. As pointed out by FRCC, the 24-hour reporting requirement will be nearly impossible to meet in hundreds of cases. What are we trying to accomplish with this requirement?

Our last concern is the incorporation of the Compliance Enforcement Matrix as part of the standard. This matrix will be used for all NERC as well as many Regional compliance efforts for all the NERC Standards. As such, it will evolve over time. By making it part of a single standard, that Standard must be revised every time the matrix is modified. Delete the matrix from the standard and provide reference to the NERC Compliance Enforcement Program, which will include the current version of the matrix.

Overall, while a good start, this document is not ready for approval as a mandatory Standard, especially when it is being rushed through as an 'urgent action'.

Response: The drafting team believes these comments are adequately addressed in the general responses to comments regarding the use of urgent action for this standard, compliance to this standard, and background checks. The drafting team has responded to FRCC's comments separately.

Reedy Creek Improvement District RC
Segment: 3
Rep: John Leland Giddens
Negative

Reedy Creek Improvement District RC
Segment: 4
Rep: Jeff Nicely
Negative

Reedy Creek Improvement District RC
Segment: 5
Rep: Bernie Budnik
Negative

Reedy Creek Improvement District agrees with the need and supports the development of a cyber security standard to protect the bulk electric system. However, we do not support the document as drafted or the approval of this within the urgent action standard process.

As members of the Florida Reliability Coordinating Council we generally endorse the comments submitted by our regional representatives with specific emphasis on the following items.

1. The standard lacks clarity in defining the applicability of requirements. Specifically, who must comply with this standard? The term bulk electric system is insufficient to define the compliance boundaries of this standard.
   Response: The implementation plan for this standard has been revised to add more clarity. In 2004, only control areas and reliability coordinators will be required to assess their compliance to this standard.

2. As stated in regional *(FRCC)* comments we do not feel this standard should be developed/implemented in the urgent standard process. Adequate time and industry input is needed to develop a standard that is complete enough to ensure the security of critical cyber assets as well as clear enough to provide direction to industry participants.

   Response: Please see the general response to comments regarding the use of urgent action for this standard. The drafting team believes it adequately addresses this comment.

Reedy Creek Improvement District would be in favor of adopting this proposed standard as a reference document while the full standards process is utilized to develop the final standard.

Reliant Resources Inc RRI
Segment: 5
Rep: Charles H Yeung
Affirmative

Reliant casts an affirmative vote with the understanding that a full process SAR request to replace this Urgent Action Standard will begin soon. Reliant wishes to state for the record that affirmation of this Urgent Action Standard should not hold Reliant to any terms and conditions embodied therein in future comments on a Cyber Security SAR.

Response: The NERC Standards Authorization Committee approved the development of a permanent replacement for the urgent action cyber security standard (that will undergo the entire ANSI accredited NERC standards development process) on May 21, 2003.

Seminole Electric Cooperative SEC
Segment: 4
Rep: Steven Wallace
Negative

FRCC Comment Endorsement — Please see FRCC comments. Additionally:

We support the concept of cyber security standards but believe the standard as proposed requires more development (for examples see endorsed FRCC comments in the uploaded file). As an interim measure during the normal NERC Standards Development Process, we support the us of the draft standard as a "guide".

Another area of concern is applicability to entities not clearly impacting bulk system reliability such as LSE's like distribution cooperatives, and the reliance on regional interpretation of applicability.

Response: Please see responses to FRCC. The implementation plan for this standard has been revised to add more clarity. In 2004, only control areas and reliability coordinators will be required to assess their compliance to this standard.

Snohomish County PUD SNPD
Segment: 3
Rep: David Sam Behar
Affirmative

I am supporting the Standard with some reservations. While I support the principal of the standard and believe that it covers the essential elements of a cyber security program to protect the nation's electrical grid, as written the standard appears to use a "one size fits all" approach and doesn't appear to differentiate between small load serving entities and large bulk transmission entities. In our own case, despite numerous requests for clarification as to whether the standard would apply to us, I could not get a definitive response. That said, I am going to cast my vote in favor of the standard in the belief that despite this flaw, it's potential benefits outweigh it's faults, and because this Urgent Action SAR is designed as a temporary measure while a permanent (and hopefully better written) standard is developed and approved.

I urgently request that the CIPAG committee members who are responsible for developing the permanent standard to develop some clear applicability language and an appropriate graduation in requirements that recognizes the differences in degree of interaction with the bulk power system between smaller distribution utilities and larger generating utilities or other entities that have significant bulk transmission resources.

Thanks for your consideration,

David Behar
Snohomish County Public Utility District
dsbehar@snopud.com
425-783-8770

Response: The implementation plan for this standard has been revised to add more clarity. In 2004, only control areas and reliability coordinators will be required to assess their compliance to this standard.

Southeastern Power Administration SEPA
Segment: 4
Rep: Carter Edge
Affirmative

Southeastern Power Administration SEPB
Segment: 5
Rep: Donnie Cordell
Affirmative

Southeastern believes the standardization of cyber security in the electric industry is necessary.

Southeastern believes the current NERC Cyber Security Urgent Standard is vague in several areas and will require duplicative reporting by Federal entities.

Southeastern believes the duty of the additional reporting requirements will be offset by benefits of cyber security standardization in the electric industry.

Southeastern recommends that NERC make compliance with the Cyber Security Urgent Standard consistent with the National Institute of Standards and Technology (NIST) where practical and strive to eliminate duplicative reporting.

Response: Please see the general response to comments regarding ambiguity in this standard and the general response regarding coordination with other reporting entities. The drafting team believes these responses adequately address the comments above.

Southern California Edison SCET
Segment: 1
Rep: Dana Cabbell
Negative

Southern California Edison SCET
Segment: 5
Rep: Neil Eugene Shockey
Negative

Southern California Edison Comments

Proposed Urgent Action Standard 1200 — Cyber Security

While the Draft Urgent Request Standard 1200 — Cyber Security is flexible in many regards, providing latitude for its implementation, many sections are vague and non-specific, and require additional clarification or specificity.

Response: Please see the general responses to comments regarding ambiguity in this standard. The drafting team believes these responses adequately address these comments.

For example, on the NERC Webcast on May 5, 2003, there was considerable discussion regarding the definition of "Critical Cyber Assets" and what is in-scope and out-of-scope in the standard. After explanation by the Webcast moderators, it is still unclear exactly what is intended to be in-scope, and subject to the standard. Additionally, the draft should specifically exclude nuclear facilities, as that segment of the industry is governed by NRC regulations/standards.

Response: Please refer to the general response to comments regarding the definition of critical cyber assets in this standard. The NRC has regulatory authority over their jurisdictional entities and is in the process of developing its own cyber security requirements. Nuclear plants are not subject to this standard. The drafting team believes this response adequately addresses the comment.

Many of the other sections do not "set the bar" regarding expectations, leaving the compliance measurements subjective. An example would be the area of background investigations in Section 1207, where no criteria for time-frame, rejection criteria or grandfathering are mentioned. Since this is an area that is driven to some degree by legal doctrine and the Fair Credit Reporting Act (FCRA), some specificity should be applied.

Response: Please see the general response to comments regarding compliance and background checks. The drafting team believes it adequately addresses this comment.

The same is true of many of the logging, list maintenance, and updating requirements listed throughout the document, which appear to be somewhat capricious and in conflict with generally accepted records retention policy or legal requirements, and ultimately add unnecessary administrative costs.

Sections 1214 and 1215 require mandatory reporting to the ES-ISAC, in addition to other reporting requirements (e.g., DOE Form EIA-417), which was previously voluntary. This duplicitous reporting is unproductive, and the Standard should seek to identify a single reporting entity to alleviate multiple reports during emergencies.

Response: Please see the general response to comments regarding incident response and reporting. The drafting team believes it adequately addresses this comment. The current version of Form 417 does not address all necessary reporting information required in this standard.

A final element that is missing is any guidance around the handling of information produced under the compliance review process. While there was discussion on the Webcast about the work product remaining with the individual companies, this item should be specifically addressed, with the work product either being classified as Critical Energy Infrastructure Information (CEII) or at a minimum, subject to a non-disclosure agreement (NDA) with the information and identity of the providing entity protected from public disclosure.

Response: Please see the general response to comments regarding compliance with this standard. The drafting team believes this response adequately addresses these comments. The CEII (FERC Order 630) applies only to documents filed with FERC.

Southern California Edison agrees with the development of a standard to set minimum expectations in the increasingly critical cyber security area, as applicable to the bulk power system. However, the proposed Urgent Action Standard has a number of flaws, as identified above, and by other industry members, that should be corrected before it is issued to the industry.

Response: NERC appreciates the time taken for you to provide your comments. It must be noted, however, that while changes have been made to the compliance plan, the ballot process for an Urgent Action SAR does not allow for changes to the text of the standard document itself. We believe that our collective responses will address your concerns and allow you to support the standard during re-balloting.

Southern Company Services SOCO
Segment: 1
Rep: Horace Stephen Williamson
Affirmative

Southern Company Services SOCO
Segment: 5
Rep: Roger Green
Affirmative

Southern Company Services SWE
Segment: 6
Rep: Tony A Reed
Affirmative

Savannah Electric and Power
Segment: 3
Rep: Thomas Harris
Affirmative

Georgia Power Company
Segment: 3
Rep: Leslie Sibert
Affirmative

Gulf Power Company
Segment: 3
Rep: William Pope
Affirmative

Definitions Section:

1. Critical Cyber Assets should include that these standards do NOT apply to Nuclear Power Plants or energy management system RTUs.

Response: This standard does not apply to nuclear power plants. Please see the response to comments on the critical cyber asset definition for clarification.

2. Compliance Monitor could be clarified by indicating that this is the "regional" organization responsible for monitoring compliance with the NERC compliance program.

Response: As indicated by the commenters, the compliance monitors for this standard are the appropriate NERC Regions.

3. The definition of Cyber Security Incident is unnecessarily broad since it states 'malicious or otherwise' and therefore covers anything which affects the operation of the system. As written, it covers such non-security related events as hardware failures or planned outages. This definition, when taken in concert with the reporting requirements stated later in the standard, would require that each of these incidents be reported to the ES-ISAC. This would

increase the 'noise level' of the ES-ISAC and thereby reduce its effectiveness considerably. The 'malicious or otherwise' language in the definition to should be changed to 'malicious or unknown' at the very least. If the incident had a known malicious cause (example: SQL Slammer worm) or after a reasonable amount of time (1 hr) a malicious cause can not be ruled out, then reporting the incident may be prudent.

Response: Please see the general response to comments regarding incident response and reporting. The drafting team believes it adequately addresses this comment.

Section 1207 — Personnel

1. Measure 2.2 which requires document updates within 24 hours is unrealistic. This should be a two step process. Security clearance should be removed within 24 hours under terminations for cause. Security clearance for terminations due to normal attrition should be removed within 5 working days. Any updates to documentation due to terminations should be updated within 5 working days.

Response: Please see the general response to comments regarding background checks. The drafting team believes it adequately addresses this comment.

2. Measure 2.3 is clarified so that individuals, such as control room operators, who have only the capability to use such assets, are not required by this standard to undergo background checks. Southern Company agrees with and supports this clarification.

Response: The clarification will be addressed in the development of the permanent cyber security standard. Thank you for the comment.

Southwestern Power Administration SWPA
Segment: 1
Rep: Stan Mason
Affirmative

Southwestern Power Administration is concerned about the apparent duplication of this Standard with requirements/guidelines it is already required to meet. We urge NERC to provide clarification for dealing with compliance with this Standard when a member is in compliance with an equal or more stringent requirement. This clarification should also provide for reduced reporting burden.

Response: Please see the general response to comments regarding ambiguity in this standard and the general response regarding coordination with other reporting entities. The drafting team believes these responses adequately address the comments above.

Tampa Electric Company TEC
Segment: 5
Rep: JOHN CURRIER
Negative

Tampa Electric Company TEC
Segment: 6
Rep: Jose Benjamin Quintas
Negative

Gainsville Regional Utilities GVL
Segment: 3
Rep: Roger Allen Westphal
Negative

TECO Tampa Electric Company Response to NERC Cyber-Security Urgent Action SAR

We support the implementation of cyber security standards for the electric industry and appreciate the effort and progress of the NERC CIPAG in developing these standards. It is crucial that these new industry standards addressing Cyber security be implemented. These standards are an important component of our industry's effort to support DHS efforts to ensure the security of the national critical infrastructure. However, we feel that the urgent nature of this process has not allowed for adequate industry review and feedback to ensure that the scope and definitions within the standards are sufficiently defined.

While CIPAG has recently done a good job in answering questions and providing some clarity in understanding the scope of the standards, the current standards' language does not reflect the CIPAG's verbal explanation of the scope of the standards. In our opinion, this "lack of clarity" in the standards will lead to inconsistent interpretation and application from company to company and region to region. This may put the infrastructure at risk from those companies and regions that may loosely interpret and apply these standards, while conversely resulting in higher and perhaps unnecessary costs to those companies and regions that may "go-beyond" the intent of these standards.

It is crucial that the standards to protect our industry and the critical infrastructure should be clear and consistently applied across the industry.

We feel that it would be prudent to allow a formal industry feed back period on these proposed standards, even if in an accelerated fashion, prior to the issuance of this urgent action request. This will allow the industry to assist the NERC CIPAG in ensuring that the scope and definitions are clearer to each entity and lead to standards that will be consistently applied across the industry.

We request that NERC consider this as a possible alternative to the current course of action.

Response: The NERC SAR process is an ANSI Certified process. The procedures relevant to an Urgent Action SAR are outside the control of the drafting team. However in the preamble to this document is a collection of general responses addressing a number of common concerns, including the re-stated plan for compliance. It is felt that these general responses, and the following point responses, will address your concerns.

Additionally, we have identified the following points that we would like to have clarified in our own efforts to ensure compliance, as well as for others in the industry.

Item 1
The scope of these standards remains unclear. The SAR request form indicates that the standard applies to generators, as do the requirements sections of each standard. However, the definition section excludes process control systems and distributed control systems in generating stations. With this exclusion, to what extent do these standards apply to generation?

Response: In general it is likely that most generator facilities will not have any critical cyber assets by definition. However, depending on the organizational structure of the generating entity, and the potential for a multi-functional IT environment, the drafting team feels it to be appropriate to include generating entities.

Item 2
The standards do not mention marketing systems. Are marketing operations included in any way within the scope of these standards?

Response (to items 1 and 2 and 4, below): The implementation plan associated with this standard has been revised to add clarity. In 2004, only control areas and reliability coordinators will be required to assess their compliance to this standard.

Item 3
The compliance schedule indicates that compliance is required as soon as the Board of Trustees adopts the standard. Information provided in the May 5 web cast indicated that substantial compliance is required in 2004 and full compliance in 2005. These dates should be formally communicated to the industry with the release of the standards.

Response: Please see the general response to comments regarding compliance to this standard. The drafting team believes it adequately addresses this comment.

Item 4
Are qualified scheduling entities covered under the scope of these standards?

Response: Please see response above.

Item 5
Standard 1208 states that monitoring will take place 24 hours per day, 7 days per week, and that logs on physical access to critical assets will be collected and verified against lists of authorized users. Access logs are voluminous, and if the standard is to be interpreted literally, it would be impossible to monitor, verify, and report on such logs; other than on a small-random-sample basis without the use of automated correlation tools. What constitutes compliance for monitoring of physical access? Is existence of logs for forensic purposes and periodic review sufficient? For how long must Video and other Physical data be stored to prove compliance?

Response: The intent of this section, in conjunction with sections 1205 and 1206, is to ensure that only authorized personnel (who have completed the required background check and have an approved need) are granted unescorted access to the critical assets. There are a number of ways that physical access can be monitored and verified per the standard. The most common is an electronic access control system (such as a card reader) with individualized access credentials. The person requesting access presents the credentials (swipes the badge) at which time the access control system validates the credentials, determines whether or not the person is permitted entry, and unlocks the door as appropriate. An electronic log entry of this action, identifying the date, time, person (badge identifier), and which door was accessed is recorded. The electronic system is doing the authentication and the monitoring and thus satisfies the requirements of the standard. Should something unexpected happen, the logs can be quickly reviewed to determine who had access. If there is a concern that the person requesting access is not using their assigned badge, a CCTV monitoring and recording system can also be employed and would serve as an additional "log" source. The minimum data retention requirement is six months, as specified in Section 1208, Paragraph 4.2. Employing both the electronic access control system and the CCTV system exceeds the minimum requirements of this standard. Employing just a CCTV system without pre-entry validation of the credentials (such as by a local or remotely sited security guard) would not meet the standard.

Item 6
Standard 1209 states that monitoring will take place 24 hours per day, 7 days per week, and that access logs will be verified against lists of authorized users. Access logs are voluminous, and if the standard is to be interpreted literally, it would be impossible to monitor, verify, and report on such logs; other than on a small-random-sample basis without the use of automated correlation tools. What constitutes compliance for monitoring of electronic access? Is existence of active logging for forensic purposes and periodic review sufficient? Additionally, logging can be done on multiple levels including operating system, application, database, firewall, and IDS systems, are the standards applicable to these logs as well?

Response: As with physical access monitoring, the use of electronic authentication that supports logging is an acceptable method. The person requesting electronic access presents a set of credentials such as username and password (the standard does not mandate multi-factor authentication). The credentials are validated and the user rights list associated with that identity defines what the user can do. The system will continuously monitor the user's activities in that it will not permit the user to access data or perform functions for which there is no authorization. At a minimum, recording of the log-on and log-off events will satisfy the logging requirement. The use of additional operating system logging, as well as application, database, firewall, and IDS logging is also acceptable and encouraged. To the extent that activity logging is employed, the standard is applicable, particularly with respect to data retention.

Item 7
Standard 1212 calls for intrusion detection processes, but to what extent is not defined in the document. Generally accepted industry standards would indicate the use of commercial network or host based intrusion detection. While these tools will detect standard IP protocol based attacks, they are not designed to detect attacks that might be based upon older or proprietary protocols used in many utility control systems. The electronic monitoring required in standard 1209 could also be perceived as a form of intrusion detection; however, manual review of system logs is not an effective IDS control due to the volume of data in such logs, and lack of timely response to events. Please clarify what is required for compliance to intrusion detection processes.

Response: The standard specifically does not define intrusion detection technology for the very reasons cited in the comment. It is up to the utility company to evaluate its electronic security perimeter and critical assets therein, determine the risk and nature of an attack against those assets, and devise a reasonable intrusion detection process where technically feasible that will enable the company to detect

and deter an attack before damage can be done. The approach should be commensurate with the risk and resulting consequences of an attack.

Item 8
For standard 1214, the definition of what qualifies as an incident is unclear. In the definitions sections, Incidents are defined as a failure (malicious or otherwise) that interrupts proper operation of a critical asset (computer) which implies that any outage (switch, hard drive, etc.) would then need to be reported. However, standard 1214 references NIPC IAW, which defines an incident as only a malicious event.

Response: Please see the general response to comments regarding incident response and reporting. The drafting team believes it adequately addresses this comment.

Tennessee Valley Authority
Segment: 5
Rep: Dennis Chastain
Affirmative

Tennessee Valley Authority Bulk Power Trading TVAM
Segment: 6
Rep: Gary L. Jackson
Affirmative

TVA supports the development of cyber security standards. We believe it is important that the cyber security standards under development by various organizations and agencies be coordinated to avoid conflicting standards and duplication of effort for the electric industry. For example, coordination with the National Institute of Standards and Technology (NIST) should be a part of the overall NERC cyber security standard development effort in order to develop a consistent and effective standard that avoids duplication.

Response: Please see the general response to comments regarding ambiguity in this standard and the general response regarding coordination with other reporting entities. The drafting team believes these responses adequately address the comments above.

Tennessee Valley Authority — Transmission/Power Supply
Segment: 1
Rep: Mitchell Needham
Affirmative

TVA believes the standardization of security practices across the electric industry is needed. NERC is correct in proposing such a standard. TVA would suggest a careful study be made regarding a very similar security 'guideline' as published by the National Institute of Standards and Technology (NIST). The NIST standard will become a de facto requirement for federal agencies such as the Tennessee Valley Authority. Where practical, we request NERC make every effort to ensure the NERC standard is consistent with the NIST standard and address utilities opting to adopt the NIST standards in place of the NERC standards. We believe that any complication in NERC cyber security compliance assurance is more than offset by the elimination of additional or duplicative reporting by federal entities. TVA will participate actively in the development of the NERC standard over the coming year, as set forth in the Urgent Action criteria. We will assist NERC in the development of language, either for the Scope statement or elsewhere in the standard, which will allow entities which must adopt the NIST standards to ensure compliance as appropriate.

Response: Please see the general response to comments regarding ambiguity in this standard and the general response regarding coordination with other reporting entities. The drafting team believes these responses adequately address the comments above.

United States Bureau of Reclamation
Segment: 5
Rep: Deborah M. Linke
Affirmative

The draft cyber security standard has excellent intent and covers all the basic categories of IT security. All "Measures" are based around the creation and maintenance of documentation. While this is certainly a step forward and an excellent framework, security is more than a paper exercise. As an example, a Technical Vulnerability Assessment (TVA) or Independent Validation and Verification (IV&V) process could easily be considered for incorporation into NERC's process. The costs of such reviews should be covered by the individual member organizations (as a cost of doing business). NERC could establish a baseline of third-party assessment contractors familiar with this process. This would be more consistent with guidance from other national standards organizations such as NIST, who include testing and validation requirements in their materials.

We understand that this is a limited-duration vehicle and would encourage the final version reconsider the self-assessment posture and include independent testing guidelines and validation/verification criteria.

Response: Please see the general response to comments regarding ambiguity in this standard and the general response regarding coordination with other reporting entities. The drafting team believes these responses adequately address the comments above.

US Army Corp of Engineers Northwestern Division
Segment: 5
Rep: Karl Bryan
Affirmative

The standard should recognize NIST, DITSCAP (Dept of Defense IT Security protocol) and others more stringent security protocols and allow a reduced level of reporting. The present standard appears to require a large amount of reporting that is already required by the more stringent security protocols. The intent of the standard is to assure outside parties that a minimum level of IT security is being followed. The intent of the standard is not to require redundant reporting.

Response: Please see the general response to comments regarding ambiguity in this standard and the general response regarding coordination with other reporting entities. The drafting team believes these responses adequately address the comments above.

Western Area Power Administration — CM WACM
Segment: 1
Rep: Mark Fidrych
Affirmative

Western's Comments:

- The proposed Standard is vague and has many loopholes.

Response: Please see the general response to comments regarding ambiguity in this standard. The drafting team believes it adequately addresses this comment.

- NIST 800-26, Security Self-Assessment Guide for Information Technology Systems, is the de facto standard for Federal Government systems and has been developed and refined by cyber security experts at the National Institute of Standards and Technology (NIST) and collaboration with industry, Government and academia during open comment periods. A NERC Standard that requires NIST 800-26 effectiveness of control measures at Level 2 would be a good start, with Level 3 effectiveness of control measures in the second or third year.

Response: Please see the general response to comments regarding ambiguity in this standard and the general response regarding coordination with other reporting entities. The drafting team believes these responses adequately address the comments above.

- The proposed standard is written more as a guideline, leaving interpretation open to the company performing the self-assessment. The measures and requirements are so vague that a company may determine through self-assessment that they fully comply, but an auditor may argue that the company has misinterpreted the requirement and does not comply. This is contrary to the goal of the compliance program that has developed concrete measures and sanctions.
- The weak nature of the proposed Standard will lead to wide differences in the implementation of security measures in the electrical industry, and possibly weak security in some areas.
- The final Standard will presumably be stronger and more detailed than the Urgent Action Standard. Implementation of a weak Standard now will make it more difficult and costly to comply with a stronger standard in the near future.

- While an affirmative vote does not require response to comments prior to a re-circulation ballot, if a ballot is required, we encourage the drafting team to address as many comments/issues as possible and not limit their responses to only the negative votes.
- We request that the all comments received be referred to the Standards Drafting Team for use in the development of a permanent Standard.

Response: Consistent with NERC requirements, all comments received during the balloting of this standard (whether associated with affirmative or negative votes) have been addressed. All comments received during the balloting of this standard will be forwarded to the referenced drafting team.

Wisconsin Energy Corporation — PM WEC
Segment: 4
Rep: Anthony Jankowski
Negative

NERC Cyber Security Standard 1200 Comments by We Energies

Page 1, Definitions
Cyber Security Incident needs clarification. It currently states " Any event or failure (malicious or otherwise) that disrupts the proper operation of a critical cyber asset." This implies that all outages, including forced and planned where there is no malicious activity needs to be reported as well. We assume only cyber security events (known or suspected) need to be reported. This definition should be modified.

Response: Please see the general response to comments regarding incident response and reporting.

All standard sections, item 1, Compliance Monitoring Process
The last sentence states the compliance monitor may investigate upon complaint. How will nuisance complaints be handled? Are they categorized and handled as a single or consolidated complaint? Can complaints be accepted from anyone? Frequency?

Each section refers to a "compliance monitor" conducting audits. There is a lack of specificity with respect to the compliance monitor process. Since the company can be fined as a result of a non-compliance issue, I think that piece of has to be more carefully crafted to ensure that the inspection standards around the ten regions are uniformly established and measured. Who will do the inspections? The company itself? Peer members? Vendors? Government?

All standard sections, Sanctions Table
The sanctions table establishes financial penalties for non-compliance. This is inappropriate and unnecessary. The imposition of fines will be a big media event. We don't need the scrutiny from the regulators. A better and adequate solution is a simple letter of non-compliance to the CEO. With normal management processes and oversight, subordinate responsible organizations will respond.

Response: Please see the general response to questions regarding compliance to this standard. The drafting team believes it adequately addresses these comments. No audits will be conducted in 2004. The compliance monitors for this standard are the appropriate NERC Regions.

Section 1201, Cyber Security Policy
Under requirements, item 2, reword or clarify what the designated cyber security senior manager can authorize with respect to deviations or exceptions to these standards. Some members may feel they can "exempt" themselves from compliance to certain standards that may otherwise be applicable. I would propose that all deviations and or exceptions be reviewed and approved by the NERC compliance monitor prior to certification.

Response: Please see general responses to comments regarding compliance with this standard. The intent of the exception process is to allow continuity of business using alternative mitigating and compensating controls. Clarification will be added during the drafting of the permanent cyber security standard.

Section 1204, Electronic Access Controls

To implement electronic access controls for our system operators who provide grid control (and are located inside our security perimeter) would be a violation of our operating safety rules. EMS control consoles need to be visible at all times and are not electronically locked down. This environment is strictly monitored using physical access control systems.

Response: Strict physical access controls and supervision may be appropriate compensating controls for electronic access in situations where critical cyber assets are being accessed via the console from within both the physical and cyber security perimeters. This presumed to be the case for most control room environments.

Section 1207, Personnel
Updating an access control list for users added within a 24-hour period may not be feasible during non business hours or over a holiday period. The requirement to have background checks performed for employees, service vendors and contractors during an emergency outage or after hours emergency support would negatively impact our service level agreements and extend EMS outage times.

Section 1207 sets a difficult standard when it requires access be canceled within 24 hours. Currently, company processes do not reliable notify Corporate Security when each individual goes out of service. Significant process improvement and training would be required.

Section 1207 establishes a requirement for background investigations with no guidance on what to do with the information and with no authority upon which the company can rely in implementation of the requirement. For instance, a background investigation process presumes that upon developing significant derogatory information, the company will make a determination whether the individual is deemed trustworthy and reliable enough to retain access to critical cyber systems. If not, then the individual must be removed. This will create huge labor and HR issues. Without the force of law (which we have through the DOT and NRC in other arenas) it will be challenging to implement this. The elements of the background investigation, the retrospective periods and those who should be subject to the investigation were all ill defined.

Under compliance, item 3B, how do you plan to measure or verify compliance to the 24hr. modification?

Response: Please see the general response to comments regarding personnel and background checks.

Section 1208, Monitoring Physical Access
Under “Compliance Monitoring Process”, item 3C needs clarification. We use an electronic card key entry system. Our access control list resides on a server. Do we still need to perform video or other physical monitoring?

Response: No. The reference to video monitoring is by example. “… or other physical monitoring” implies, without specifying, that some form of physical security monitoring is required.

Section 1208 requires monitoring physical access to the critical cyber systems but gives no guidance on where the perimeter should be established. At the gate? The front door to the building? Entry to the room? Access to the work station? Access to the server?

Response: It is expected that the physical security perimeter will often be defined by the nearest “four wall boundary” surrounding the critical cyber asset(s). It is suggested that several small, well-defined perimeters, with potentially fewer, easily controlled access points for each perimeter, are easier to manage. A single large perimeter, with a variety of access points, may provide greater risk, and may require more sophisticated monitoring solutions.

Section 1209, Monitoring Electronic Access
See our comments on section 1204. Due to safety reasons, electronic access monitoring and logging could only be performed for our IT system administrators who support the EMS application.

Response: See previous response to 1204. IT personnel with access inside the computer room are less likely to be continuously supervised, therefore requiring that a solution for electronic monitoring be implemented.

Section 1213, Test Procedures
The requirement to use an isolated test environment for acceptance testing needs clarification. We Energies currently has a test network/domain that is used for testing application changes and revisions as well as service patches and OS upgrades. This environment is logically isolated from our production servers, but is physically connected to the production network to allow data transfer. Administrators do not have grid control access from the test domain. Is this considered an isolated test environment?

Response: Yes. Electronic isolation is not required by this standard; rather, a controlled non-production system is to be used for testing. The standard does not require that the test environment be outside the electronic security perimeter.

Section 1214, Incident Response Actions
It appears as if we will be required to report on incidents that includes equipment not inside the security perimeter. This includes but is not limited to: process control systems, distributed control systems, relay and controls located at substations and power plants.

Section 1215, Physical Incident Response Actions
See 1214 comments.

Response: Please see the general response to comments regarding incident response and reporting.

Standard Authorization Request Form

Title of Proposed Standard	Cyber Security
Request Date	May 2, 2003

SAR Requestor Information

Name	Charles Noble (on behalf of CIPAG)	**SAR Type** (Check box for one of these selections.)	
Company		☒	New Standard
Telephone		☐	Revision to Existing Standard
Fax		☐	Withdrawal of Existing Standard [1]
E-mail		☐	Urgent Action

Purpose/Industry Need (Provide one or two sentences.)

To reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets (computers, software and communication networks) that support those systems.

Brief Description

This standard will require that critical cyber assets related to the reliable operation of the bulk electric systems are identified and protected. Requirements will be included in the standard to identify the responsible person(s), create and implement programs and procedures, perform a thorough assessment of cyber security, and implement appropriate and technically feasible security improvements.

Reliability Functions

The Standard will Apply to the Following Functions *(Check box for each one that applies.)*		
☒	Reliability Authority	Ensures the reliability of the bulk transmission system within its Reliability Authority area. This is the highest reliability authority.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within its metered boundary and supports system frequency in real time
☒	Interchange Authority	Authorizes valid and balanced Interchange Schedules
☐	Planning Authority	Plans the bulk electric system
☒	Transmission Service Provider	Provides transmission services to qualified market participants under applicable transmission service agreements
☐	Transmission Owner	Owns transmission facilities
☒	Transmission Operator	Operates and maintains the transmission facilities, and executes switching orders
☐	Distribution Provider	Provides and operates the “wires” between the transmission system and the customer
☒	Generator	Owns and operates generation unit(s) or runs a market for generation products that performs the functions of supplying energy and Interconnected Operations Services
☐	Purchasing-Selling Entity	The function of purchasing or selling energy, capacity and all necessary Interconnected Operations Services as required
☒	Load-Serving Entity	Secures energy and transmission (and related generation services) to serve the end user

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check box for all that apply.)*	
☐	1. Interconnected bulk electric systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk electric systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk electric systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk electric systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk electric systems.
☒	6. Personnel responsible for planning and operating interconnected bulk electric systems shall be trained, qualified and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk electric systems shall be assessed, monitored and maintained on a wide area basis.
Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*	
1. The planning and operation of bulk electric systems shall recognize that reliability is an essential requirement of a robust North American economy. Yes	
2. An Organization Standard shall not give any market participant an unfair competitive advantage.Yes	
3. An Organization Standard shall neither mandate nor prohibit any specific market structure. Yes	
4. An Organization Standard shall not preclude market solutions to achieving compliance with that Standard. Yes	
5. An Organization Standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes	

Detailed Description

1. Recent security incidents have impacted cyber systems that are critical to electric system reliability.

2. The frequency and severity of cyber attacks are increasing.

3. Ongoing world events may lead to further cyber attacks that impact bulk electric system reliability.

4. The standard is based upon guidelines established by the NERC Critical Infrastructure Protection Advisory Group (CIPAG) and approved by the NERC Board of Trustees. These guidelines were submitted to the industry for review and comment. Comments received were reviewed and included in the guidelines, as appropriate.

5. The standard is also based upon the proposed cyber security standard drafted by a NERC-sponsored industry group, approved by CIPAG and the NERC Board of Trustees, and submitted to FERC at its request. Two industry comment periods were included in the development of this proposed cyber security standard.

6. According to the FERC's April 28, 2003 "White Paper, Wholesale Power Market Platform" (FERC Docket No. RM01-12) FERC plans to adopt NERC's Cyber Security Standard.

Reliable electric system 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 bulk electric system operations by establishing standards to assure that a lack of cyber security for one critical asset does not compromise security and risk grid or market failure.

This standard requires that responsible entities understand the role of cyber security in electric infrastructure reliability, have identified their critical cyber assets related to bulk electric system operations, and have a security program in place. This program should mitigate the impact to bulk electric system operations from acts, either accidental or malicious, that could cause wide-ranging, harmful impacts. A basic cyber security program for bulk electric system operations shall cover governance, planning, prevention, operations, incident response, and business continuity. This standard is intended to ensure that appropriate mitigating plans and actions are in place, recognizing the differing roles of each responsible entity and the differing risks being managed.

This cyber security standard shall primarily focus on electronic systems, which include hardware, software, data, related communications networks, control systems as they impact electric system operations, and personnel. In addition, physical security shall be addressed to the extent that it is necessary to assure a secure physical environment for cyber resources.

This standard will apply to entities performing the Reliability Authority, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Operator, Generator, and Load Serving Entity and functions.

This standard provides definition of terms and the minimum requirements to implement and maintain a

cyber security program to protect cyber assets critical to reliable electric system operations.

Definitions

Critical Cyber Assets: Those computers, including installed software and electronic data, and communication networks that support, operate, or otherwise interact with the bulk electric system operations. This definition currently does not include process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations.

Electronic Security Perimeter: The border surrounding the network or group of sub-networks (the "secure network") to which the critical cyber assets are connected.

Physical Security Perimeter: The border surrounding computer rooms, telecommunications rooms, operations centers, and other clearly defined locations in which critical cyber assets are housed and access is controlled.

Cyber Security Incident: Any event or failure (malicious or otherwise) that disrupts the proper operation of a Critical Cyber Asset.

Incident Response: Responding to, and reporting a cyber security incident.

Compliance Monitor: The organization responsible for monitoring compliance with this standard in accordance with the NERC compliance enforcement program.

Related SARs

SAR ID	Explanation
None	

Regional Differences

Region	Explanation
None	

Related NERC Planning Standards/Operating Policies

Standard No.	Explanation
None	

Industry Representatives who participated in developing this SAR	Charles Noble – ISO New England Jerry Freese – American Electric Power Larry Brown – Edison Electric Institute Ken Hall – Edison Electric Institute Larry Bugh – ECAR Regional Council Scott Mix – Electric Power Research Institute Jim Orcheson – Independent Market Operator (Ontario) Roger Lampila – New York ISO James Strange –American Public Power Association Sergio Guzman – Florida Power & Light Lyman Shaffer – Pacific Gas & Electric John Fridye – Reliant Resources Kurt Muehlbauer – Exelon Jay Cribb – Southern Company Seiki Harada – BC Hydro Greg Fraser – Manitoba Hydro Lewis Griffith – Centerpoint Energy Kevin Perry – Southwest Power Pool