COMMISSION BRIEFING SLIDES/EXHIBITS

BRIEFING ON GRID STABILITY

AND OFFSITE POWER ISSUES

MAY 10, 2004

ELECTRIC GRID STABILITY AND NUCLEAR POWER PLANTS

Alison Silverstein
Federal Energy Regulatory Commission

May 10, 2004

Blackout Report Findings

- On August 14, 2004, the grid – and 62,000 MW of generation, including 9 US nuclear plants, went down across 8 states and provinces with almost no warning.
- The problems started hours before, but inadequate situational awareness by the local grid operator and reliability coordinators prevented effective action.

NPPs and the Grid

- **NPPs need a consistent, reliable grid**
  - **To feed power into**
  - **To rely on for safe shut-down**
- **The grid needs NPPs**
  - **For real power, energy and capacity**
  - **For reactive power and voltage support**

Is the grid reliable?

- Very reliable most of the time
- 8/14 (and prior blackouts) teaches us that the best way to assure reliability and prevent big blackouts is to handle the basics and prevent small problems and local blackouts
- Ask NERC, FERC and DOE to work with NRC on probability and risk of local and regional blackouts

Recommendations for NPPs

Make sure the Control Area and Reliability Coordinator operating the grid understand your plant's unique voltage needs.

- **Ask RC and CA for updated voltage studies to determine grid capabilities, potential threats**
- **Create specific grid operating limits designed around each NPP's voltage needs**

Situational Awareness

Improve NPP situational awareness about potential grid problems

- **Access key real-time grid data**
- **Better sharing of grid condition data and state estimator or contingency analysis results**
- **Effective communications protocols between control rooms**

Assure cooperation

How?

- Contracts between NPP, CA, transmission operator and/or RC for clear accountability
- Possible FERC tariff for CA or RC if NPP's needs and the relationship impose additional costs or activities

Protecting the NPP

Voltage at the NPP-to-grid interface must meet range of NPP needs – does it have to come from the whole grid?

- **Reexamine the requirements – how much, how long, how fast is protection needed?**
- **Does it need full grid operability or can local voltage support near the interface help meet the need?**

Cyber-security

Mutual vulnerability between grid operators and the plants on cyber-security

- **Require NPPs to adopt and implement NERC standard 1200 for plant and EMS protections**
- **This will reduce NPP cyber vulnerability and protect grid better**

Nuclear Regulatory Commission Meeting on
Grid Stability and Offsite Power Issues
May 10, 2004

Prepared Remarks of

David R. Nevius
Senior Vice President
North American Electric Reliability Council

Good afternoon Mr. Chairman and members of the Commission. My name is David R. Nevius and I am Senor Vice President of the North American Electric Reliability Council (NERC).[1] Thank you for this opportunity to share NERC's views and activities relative to grid reliability and priority consideration for restoration of offsite power to nuclear power plants.

Before doing so, however, I must say that Congress can take one very important step to ensure we do not have a repeat of August 14. That step is to pass reliability legislation to make reliability rules mandatory and enforceable for all owners, operators, and users of the bulk power system. Right now compliance with NERC rules is voluntary. Legislation to make NERC rules mandatory and enforceable is included in H.R. 6, the comprehensive energy bill that has already passed the House. Senator Domenici included that same language in S. 2095, the slimmed-down version of a comprehensive energy bill. That language enjoys widespread support from all parts of the industry, as well as customers and regulators. I believe that if the reliability legislation had been passed two years ago, we would not have had a blackout last August.

The August 14 blackout that affected eight states and two Canadian provinces was a seminal event for the entire electric industry, including the operators of nuclear power plants. Immediately following the blackout, NERC assembled a team of technical experts to investigate exactly what happened and why. To lead this effort, NERC established a steering group of executive-level experts from systems not directly involved in the cascading grid failure. Every human and data resource we requested of the industry was provided, and hundreds of electric system experts were volunteered from across the United States and Canada to participate in the investigation. Members of the team have worked hard to correlate and analyze the massive amounts of data that we received.

NERC has also been an integral part of the joint fact-finding investigation into the August 14 blackout conducted by the U.S.-Canada Power System Outage Task Force.

---

[1] NERC is a not-for-profit organization formed after the Northeast blackout in 1965 to promote the reliability of the bulk electric systems that serve North America. NERC's mission is to ensure that the bulk electric system in North America is reliable, adequate, and secure. NERC works with all segments of the electric industry as well as electricity consumers and regulators to set and encourage compliance with rules for the planning and operation of reliable electric systems. NERC comprises ten regional reliability councils that account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

NERC fully supports the task force's findings and conclusions, which were laid out in the November 19 interim report, and confirmed in the April 5 final report. With respect to what happened on August 14, the key findings and conclusions of the task force were as follows: "inadequate situational awareness at FirstEnergy Corporation," "FirstEnergy failed to manage adequately tree growth in its transmission rights-of-way," and "failure of the interconnected grid's reliability organizations to provide effective diagnostic support." NERC concurs with those findings.

On October 10, 2003, NERC directed all control areas and reliability coordinators to review certain reliability practices and to verify in writing that their organizations are within NERC and regional reliability council standards and established good utility practices, and to identify areas where corrective actions were needed. The letter addressed:

- Voltage and Reactive Management
- Reliability Communications
- Failures of System Monitoring and Control Functions
- Emergency Action Plans
- Training for Emergencies, and
- Vegetation Management

On February 10, 2004, NERC took significant steps to prevent and mitigate the impacts of future cascading blackouts and increase public confidence in the reliability of the bulk electric system. NERC will use all means available to obtain full compliance with its reliability standards. We will make available detailed information on the nature and potential impacts of significant compliance violations, and will provide greater public and regulatory transparency to compliance violations. NERC has developed disclosure guidelines to guide the release of this data while respecting market sensitive and critical infrastructure information. We will also work closely with the Federal Energy Regulatory Commission (FERC) and other regulators in the United States, Canada, and Mexico to improve bulk electric system reliability.

NERC is implementing 14 recommendations to address reliability shortcomings identified by the blackout investigation. The first recommendation addresses the direct causes of the blackout. First Energy, the Midwest ISO, and PJM were directed to implement specific improvements to rectify deficiencies identified by NERC and the US-Canada Power System Outage Task Force blackout investigations. FE, MISO, and PJM have already made some of these improvements; others are under way.

NERC initiated a series of strategic initiatives that strengthen NERC's Compliance Enforcement Program, including requiring all control areas and reliability coordinators to undergo readiness audits, evaluating vegetation management procedures and results, and tracking the implementation of blackout recommendations. NERC is also undertaking a series of technical initiatives to improve overall electric system

reliability and operations throughout North America. A full copy of NERC's actions is contained in Attachment B.

NERC has implemented a number of key initiatives to ensure reliability going into the summer 2004 season. Most importantly, NERC is targeting the direct causes of the blackout identified by both NERC and the US-Canada task force and ensuring that they are corrected prior to this summer. NERC has reviewed and approved detailed remediation plans from FirstEnergy, the Midwest ISO, and PJM. Each company must demonstrate to NERC that it has successfully implemented those plans prior to June 30.

NERC is conducting reliability readiness audits for all control areas and reliability coordinators in North America. Audits of twenty of the largest control areas will be completed by June 30. Of particular significance to nuclear operators and the Commission, NERC is including in its readiness audits an evaluation of the system operator's awareness of nuclear plant voltage and power requirements in both normal and abnormal operating conditions, including restoration. NERC also approved revisions to NERC operating policies to clarify reliability coordinator and control area functions, responsibilities, and authorities.

NERC adopted a set of 38 compliance templates for immediate use by its Compliance Enforcement Program. These templates, which have been revised to more clearly define their measurement and compliance criteria, will be used to measure compliance with NERC reliability rules. The templates will be incorporated into a set of new reliability standards that will translate existing NERC operating policies and planning standards into an integrated and comprehensive set of measurable standards by the end of 2004.

NERC approved a Vegetation Management Compliance Template in that requires each transmission owner to document its transmission vegetation management program. Each program must have inspection requirements, trimming clearances, and an annual work plan. Transmission owners will report annually on compliance with their program as well as be audited every three years. Transmission owners are also required to report vegetation-related outages to their Region. NERC is also developing an enforceable standard for transmission system vegetation management in concert with experts in this field.

NERC's blackout investigation will continue for some time. Although we believe that we understand what happened and why for most aspects of the outage, we are conducting more detailed analyses in several areas, notably dynamic simulations of the transient or high speed phases of the cascade, and a final verification of the full scope of all violations of NERC and regional reliability standards that led to the outage.

To complete the technical investigation of what happened, regional modeling teams working with NERC have constructed electrical models to simulate the exact conditions of August 14 and are in the process of subjecting those models to the events

that occurred during the time preceding the outage to understand better its causes. These simulations will examine the electrical stability of the grid—that is, how strongly the generators were synchronized to one another—and whether there was a voltage collapse of the transmission system. We will also focus on why operating procedures that should have detected problems that developed on the grid and kept them from spreading did not prevent the cascading outage across such a wide area. We expect to issue a detailed technical report on these issues later in the year.

NERC strongly endorses recent FERC actions to improve electric system reliability taken in response to recommendations made in the final U.S.-Canada blackout report. While enacting legislation that authorizes binding and enforceable reliability standards is the best way to ensure reliability, but neither NERC nor FERC can sit idle waiting for Congress to act.

FERC's policy statement on reliability does a very important thing: it defines compliance with reliability standards as "Good Utility Practice" and requires all jurisdictional entities to comply with NERC reliability standards. This is an extremely positive development, even if it only applies to NERC-jurisdictional entities. But understand, that still leaves a lot of entities out of the picture. FERC also issued an order requiring transmitting entities to report vegetation management plans to FERC and NERC. This is completely in line with the recommendation we are already implementing. FERC's recent actions and their willingness to work closely with NERC on reliability matters will go a long way to enhance the reliability of the bulk power system in the absence reliability legislation.

NERC is fully committed to working with all sectors of the electricity industry, the Nuclear Regulatory Commission, FERC, other regulatory agencies, and with customers to ensure the ongoing reliability of the bulk electric system in North America. Our principal focus in the next several months will be to implement the recommendations that NERC has adopted, along with the recommendations in the final report of the U.S. – Canada Power System Outage Task Force.

I will conclude my testimony where I began, with the urgent message that Congress needs to enact reliability legislation this year. The set of recommendations the NERC has adopted is an aggressive one. Right now we are able to accomplish much because we have the strong support of the chief executives from all parts of the industry, as well as the attention of all industry participants. But everyone is focused on reliability because we are still very close to the events of August 14. With the passage of time, priorities will shift, people will move on, and other issues will compete for our attention. Having the reliability legislation in place will make sure that we can maintain the proper focus on reliability on an ongoing, sustainable basis, and that mandatory and enforceable rules will apply to all system owners, operators, and users.

Thank you.

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

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

August 14, 2003 Blackout: NERC Actions to Prevent and Mitigate the Impacts of Future Cascading Blackouts February 10, 2004

Preamble

The Board of Trustees recognizes the paramount importance of a reliable bulk electric system in North America. In consideration of the findings of the investigation into the August 14, 2003 blackout, NERC must take firm and immediate actions to increase public confidence that the reliability of the North American bulk electric system is being protected.

A key finding of the blackout investigators is that violations of existing NERC reliability standards contributed directly to the blackout. Pending enactment of federal reliability legislation creating a framework for enforcement of mandatory reliability standards, and with the encouragement of the Stakeholders Committee, the board is determined to obtain full compliance with all existing and future reliability standards and intends to use all legitimate means available to achieve that end. The board therefore resolves to:

- *Receive specific information on all violations of NERC standards, including the identities of the parties involved;*
- *Take firm actions to improve compliance with NERC reliability standards;*
- *Provide greater transparency to violations of standards, while respecting the confidential nature of some information and the need for a fair and deliberate due process; and*
- *Inform and work closely with the Federal Energy Regulatory Commission and other applicable federal, state, and provincial regulatory authorities in the United States, Canada, and Mexico as needed to ensure public interests are met with respect to compliance with reliability standards.*

The board expresses its appreciation to the blackout investigators and the Steering Group for their objective and thorough work in preparing a report of recommended NERC actions. With a few clarifications, the board approves the report and directs implementation of the recommended actions. The board holds the assigned committees and organizations accountable to report to the board the progress in completing the recommended actions, and intends itself to publicly report those results. The board recognizes the possibility that this action plan may have to be adapted as additional analysis is completed, but stresses the need to move forward immediately with the actions as stated.

Furthermore, the board directs management to immediately advise the board of any significant violations of NERC reliability standards, including details regarding the nature and potential reliability impacts of the alleged violations and the identity of parties involved. Management shall supply to the board in advance of board meetings a detailed report of all violations of reliability standards.

Finally, the board resolves to form a task force to develop guidelines for the board to consider with regard to the confidentiality of compliance information and disclosure of such information to regulatory authorities and the public.

Overview of Investigation Conclusions

The North American Electric Reliability Council (NERC) has conducted a comprehensive investigation of the August 14, 2003 blackout. The results of NERC's investigation contributed significantly to the U.S./Canada Power System Outage Task Force's November 19, 2003 Interim Report identifying the root causes of the outage and the sequence of events leading to and during the cascading failure. NERC fully concurs with the conclusions of the Interim Report and continues to provide its support to the Task Force through ongoing technical analysis of the outage. Although an understanding of what happened and why has been resolved for most aspects of the outage, detailed analysis continues in several areas, notably dynamic simulations of the transient phases of the cascade and a final verification of the full scope of all violations of NERC and regional reliability standards that occurred leading to the outage.

From its investigation of the August 14 blackout, NERC concludes that:

- Several entities violated NERC operating policies and planning standards, and those violations contributed directly to the start of the cascading blackout.
- The existing process for monitoring and assuring compliance with NERC and regional reliability standards was shown to be inadequate to identify and resolve specific compliance violations before those violations led to a cascading blackout.
- Reliability coordinators and control areas have adopted differing interpretations of the functions, responsibilities, authorities, and capabilities needed to operate a reliable power system.
- Problems identified in studies of prior large-scale blackouts were repeated, including deficiencies in vegetation management, operator training, and tools to help operators better visualize system conditions.
- In some regions, data used to model loads and generators were inaccurate due to a lack of verification through benchmarking with actual system data and field testing.
- Planning studies, design assumptions, and facilities ratings were not consistently shared and were not subject to adequate peer review among operating entities and regions.
- Available system protection technologies were not consistently applied to optimize the ability to slow or stop an uncontrolled cascading failure of the power system.

Overview of Recommendations

The Board of Trustees approves the NERC Steering Group recommendations to address these shortcomings. The recommendations fall into three categories.

Actions to Remedy Specific Deficiencies: Specific actions directed to First Energy (FE), the Midwest Independent System Operator (MISO), and the PJM Interconnection, LLC (PJM) to correct the deficiencies that led to the blackout.

1. Correct the Direct Causes of the August 14, 2003 Blackout.

Strategic Initiatives: Strategic initiatives by NERC and the regional reliability councils to strengthen compliance with existing standards and to formally track completion of recommended actions from August 14, and other significant power system events.

2. Strengthen the NERC Compliance Enforcement Program.
3. Initiate Control Area and Reliability Coordinator Reliability Readiness Audits.
4. Evaluate Vegetation Management Procedures and Results.
5. Establish a Program to Track Implementation of Recommendations.

Technical Initiatives: Technical initiatives to prevent or mitigate the impacts of future cascading blackouts.

6. Improve Operator and Reliability Coordinator Training
7. Evaluate Reactive Power and Voltage Control Practices.
8. Improve System Protection to Slow or Limit the Spread of Future Cascading Outages.
9. Clarify Reliability Coordinator and Control Area Functions, Responsibilities, Capabilities and Authorities.
10. Establish Guidelines for Real-Time Operating Tools.
11. Evaluate Lessons Learned During System Restoration.
12. Install Additional Time-Synchronized Recording Devices as Needed.
13. Reevaluate System Design, Planning and Operating Criteria.
14. Improve System Modeling Data and Data Exchange Practices.

Market Impacts

Many of the recommendations in this report have implications for electricity markets and market participants, particularly those requiring reevaluation or clarification of NERC and regional standards, policies and criteria. Implicit in these recommendations is that the NERC board charges the Market Committee with assisting in the implementation of the recommendations and interfacing with the North American Energy Standards Board with respect to any necessary business practices.

Recommendation to Remedy Specific Deficiencies

Recommendation 1. Correct the Direct Causes of the August 14, 2003 Blackout.

NERC's technical analysis of the August 14 blackout leads it to fully concur with the Task Force Interim Report regarding the direct causes of the blackout. The report stated that the principal causes of the blackout were that FE did not maintain situational awareness of conditions on its power system and did not adequately manage tree growth in its transmission rights-of-way. Contributing factors included ineffective diagnostic support provided by MISO as the reliability coordinator for FE and ineffective communications between MISO and PJM.

NERC will take immediate and firm actions to ensure that the same deficiencies that were directly causal to the August 14 blackout are corrected. These steps are necessary to assure electricity customers, regulators and others with an interest in the reliable delivery of electricity that the power system is being operated in a manner that is safe and reliable, and that the specific causes of the August 14 blackout have been identified and fixed.

Recommendation 1a: FE, MISO, and PJM shall each complete the remedial actions designated in Attachment A for their respective organizations and certify to the NERC board no later than June 30, 2004, that these specified actions have been completed. Furthermore, each organization shall present its detailed plan for completing these actions to the NERC committees for technical review on March 23-24, 2004, and to the NERC board for approval no later than April 2, 2004.

Recommendation 1b: The NERC Technical Steering Committee shall immediately assign a team of experts to assist FE, MISO, and PJM in developing plans that adequately address the issues listed in Attachment A, and other remedial actions for which each entity may seek technical assistance.

Strategic Initiatives to Assure Compliance with Reliability Standards and to Track Recommendations

Recommendation 2. Strengthen the NERC Compliance Enforcement Program.

NERC's analysis of the actions and events leading to the August 14 blackout leads it to conclude that several violations of NERC operating policies contributed directly to an uncontrolled, cascading outage on the Eastern Interconnection. NERC continues to investigate additional violations of NERC and regional reliability standards and expects to issue a final report of those violations in March 2004.

In the absence of enabling legislation in the United States and complementary actions in Canada and Mexico to authorize the creation of an electric reliability organization, NERC lacks legally sanctioned authority to enforce compliance with its reliability rules. However, the August 14 blackout is a clear signal that voluntary compliance with reliability rules is no longer adequate. NERC and the regional reliability councils must assume firm authority to measure compliance, to more transparently report significant violations that could risk the integrity of the interconnected power system, and to take immediate and effective actions to ensure that such violations are corrected.

Violations of NERC standards identified in the November 19, 2003 Interim Report:

1. Following the outage of the Chamberlin-Harding 345 kV line, FE did not take the necessary actions to return the system to a safe operating state within 30 minutes (violation of NERC Operating Policy 2).
2. FE did not notify other systems of an impending system emergency (violation of NERC Operating Policy 5).
3. FE's analysis tools were not used to effectively assess system conditions (violation of NERC Operating Policy 5).
4. FE operator training was inadequate for maintaining reliable conditions (violation of NERC Operating Policy 8).
5. MISO did not notify other reliability coordinators of potential problems (violation of NERC Operating Policy 9).

Recommendation 2a: Each regional reliability council shall report to the NERC Compliance Enforcement Program within one month of occurrence all significant[1] violations of NERC operating policies and planning standards and regional standards, whether verified or still under investigation. Such reports shall confidentially note details regarding the nature and potential reliability impacts of the alleged violations and the identity of parties involved. Additionally, each regional reliability council shall report quarterly to NERC, in a format prescribed by NERC, all violations of NERC and regional reliability council standards.

Recommendation 2b: Being presented with the results of the investigation of any significant violation, and with due consideration of the surrounding facts and circumstances, the NERC board shall require an offending organization to correct the violation within a specified time. If the board determines that an offending organization is non-responsive and continues to cause a risk to the reliability of the interconnected power systems, the board will seek to remedy the violation by requesting assistance of the appropriate regulatory authorities in the United States, Canada, and Mexico.

[1] Although all violations are important, a significant violation is one that could directly reduce the integrity of the interconnected power systems or otherwise cause unfavorable risk to the interconnected power systems. By contrast, a violation of a reporting or administrative requirement would not by itself generally be considered a significant violation.

Recommendation 2c: The Planning and Operating Committees, working in conjunction with the Compliance Enforcement Program, shall review and update existing approved and draft compliance templates applicable to current NERC operating policies and planning standards; and submit any revisions or new templates to the board for approval no later than March 31, 2004. To expedite this task, the NERC President shall immediately form a Compliance Template Task Force comprised of representatives of each committee. The Compliance Enforcement Program shall issue the board-approved compliance templates to the regional reliability councils for adoption into their compliance monitoring programs.

This effort will make maximum use of existing approved and draft compliance templates in order to meet the aggressive schedule. The templates are intended to include all existing NERC operating policies and planning standards but can be adapted going forward to incorporate new reliability standards as they are adopted by the NERC board for implementation in the future.

When the investigation team's final report on the August 14 violations of NERC and regional standards is available in March, it will be important to assess and understand the lapses that allowed violations to go unreported until a large-scale blackout occurred.

Recommendation 2d: The NERC Compliance Enforcement Program and ECAR shall, within three months of the issuance of the final report from the Compliance and Standards investigation team, evaluate the identified violations of NERC and regional standards, as compared to previous compliance reviews and audits for the applicable entities, and develop recommendations to improve the compliance process.

Recommendation 3. Initiate Control Area and Reliability Coordinator Reliability Readiness Audits.

In conducting its investigation, NERC found that deficiencies in control area and reliability coordinator capabilities to perform assigned reliability functions contributed to the August 14 blackout. In addition to specific violations of NERC and regional standards, some reliability coordinators and control areas were deficient in the performance of their reliability functions and did not achieve a level of performance that would be considered acceptable practice in areas such as operating tools, communications, and training. In a number of cases there was a lack of clarity in the NERC policies with regard to what is expected of a reliability coordinator or control area. Although the deficiencies in the NERC policies must be addressed (see Recommendation 9), it is equally important to recognize that standards cannot prescribe all aspects of reliable operation and that minimum standards present a threshold, not a target for performance. Reliability coordinators and control areas must perform well, particularly under emergency conditions, and at all times strive for excellence in their assigned reliability functions and responsibilities.

Recommendation 3a: The NERC Compliance Enforcement Program and the regional reliability councils shall jointly establish a program to audit the reliability readiness of all reliability coordinators and control areas, with immediate attention given to addressing the deficiencies identified in the August 14 blackout investigation. Audits of all control areas and reliability coordinators shall be completed within three years and continue in a three-year cycle. The 20 highest priority audits, as determined by the Compliance Enforcement Program, will be completed by June 30, 2004.

Recommendation 3b: NERC will establish a set of baseline audit criteria to which regional criteria may be added. The control area requirements will be based on the existing NERC Control Area Certification Procedure. Reliability coordinator audits will include evaluation of reliability plans, procedures, processes, tools, personnel qualifications, and training. In addition to reviewing written documents, the audits will carefully examine the actual practices and preparedness of control areas and reliability coordinators.

Recommendation 3c: The reliability regions, with the oversight and direct participation of NERC, will audit each control area's and reliability coordinator's readiness to meet these audit criteria. FERC and other relevant regulatory agencies will be invited to participate in the audits, subject to the same confidentiality conditions as the other members of the audit teams.

Recommendation 4. Evaluate Vegetation Management Procedures and Results.

Ineffective vegetation management was a major cause of the August 14 blackout and also contributed to other historical large-scale blackouts, such on July 2-3, 1996 in the west. Maintaining transmission line rights-of-way (ROW), including maintaining safe clearances of energized lines from vegetation, under-build, and other obstructions[2] incurs a substantial ongoing cost in many areas of North America. However, it is an important investment for assuring a reliable electric system.

NERC does not presently have standards for ROW maintenance. Standards on vegetation management are particularly challenging given the great diversity of vegetation and growth patterns across North America. However, NERC's standards do require that line ratings are calculated so as to maintain safe clearances from all obstructions. Furthermore, in the United States, the National Electrical Safety Code (NESC) Rules 232, 233, and 234 detail the minimum vertical and horizontal safety clearances of overhead conductors from grounded objects and various types of obstructions. NESC Rule 218 addresses tree clearances by simply stating, "Trees that may interfere with ungrounded supply conductors should be trimmed or removed." Several states have adopted their own electrical safety codes and similar codes apply in Canada.

Recognizing that ROW maintenance requirements vary substantially depending on local conditions, NERC will focus attention initially on measuring performance as indicated by the number of high voltage line trips caused by vegetation rather than immediately move toward developing standards for

[2] Vegetation, such as the trees that caused the initial line trips in FE that led to the August 14, 2003 outage is not the only type of obstruction that can breach the safe clearance distances from energized lines. Other examples include under-build of telephone and cable TV lines, train crossings, and even nests of certain large bird species.

ROW maintenance. This approach has worked well in the Western Electricity Coordinating Council (WECC) since being instituted after the 1996 outages.

Recommendation 4a: NERC and the regional reliability councils shall jointly initiate a program to report all bulk electric system[3] transmission line trips resulting from vegetation contact[4]. The program will use the successful WECC vegetation monitoring program as a model.

Recommendation 4b: Beginning with an effective date of January 1, 2004, each transmission operator will submit an annual report of all vegetation-related high voltage line trips to its respective reliability region. Each region shall assemble a detailed annual report of vegetation-related line trips in the region to NERC no later than March 31 for the preceding year, with the first reporting to be completed by March 2005 for calendar year 2004.

Vegetation management practices, including inspection and trimming requirements, can vary significantly with geography. Additionally, some entities use advanced techniques such as planting beneficial species or applying growth retardants. Nonetheless, the events of August 14 and prior outages point to the need for independent verification that viable programs exist for ROW maintenance and that the programs are being followed.

Recommendation 4c: Each bulk electric transmission owner shall make its vegetation management procedure, and documentation of work completed, available for review and verification upon request by the applicable regional reliability council, NERC, or applicable federal, state or provincial regulatory agency.

Should this approach of monitoring vegetation-related line outages and procedures prove ineffective in reducing the number of vegetation-related line outages, NERC will consider the development of minimum line clearance standards to assure reliability.

Recommendation 5. Establish a Program to Track Implementation of Recommendations.

The August 14 blackout shared a number of contributing factors with prior large-scale blackouts, including:

- Conductors contacting trees
- Ineffective visualization of power system conditions and lack of situational awareness
- Ineffective communications
- Lack of training in recognizing and responding to emergencies
- Insufficient static and dynamic reactive power supply
- Need to improve relay protection schemes and coordination

[3] All transmission lines operating at 230 kV and higher voltage, and any other lower voltage lines designated by the regional reliability council to be critical to the reliability of the bulk electric system, shall be included in the program.
[4] A line trip includes a momentary opening and reclosing of the line, a lock out, or a combination. For reporting purposes, all vegetation-related openings of a line occurring within one 24-hour period should be considered one event. Trips known to be caused by severe weather or other natural disaster such as earthquake are excluded. Contact with vegetation includes both physical contact and arcing due to insufficient clearance.

It is important that recommendations resulting from system outages be adopted consistently by all regions and operating entities, not just those directly affected by a particular outage. Several lessons learned prior to August 14, if heeded, could have prevented the outage. WECC and NPCC, for example, have programs that could be used as models for tracking completion of recommendations. NERC and some regions have not adequately tracked completion of recommendations from prior events to ensure they were consistently implemented.

Recommendation 5a: NERC and each regional reliability council shall establish a program for documenting completion of recommendations resulting from the August 14 blackout and other historical outages, as well as NERC and regional reports on violations of reliability standards, results of compliance audits, and lessons learned from system disturbances. Regions shall report quarterly to NERC on the status of follow-up actions to address recommendations, lessons learned, and areas noted for improvement. NERC staff shall report both NERC activities and a summary of regional activities to the board.

Assuring compliance with reliability standards, evaluating the reliability readiness of reliability coordinators and control areas, and assuring recommended actions are achieved will be effective steps in reducing the chances of future large-scale outages. However, it is important for NERC to also adopt a process for continuous learning and improvement by seeking continuous feedback on reliability performance trends, not rely mainly on learning from and reacting to catastrophic failures.

Recommendation 5b: NERC shall by January 1, 2005 establish a reliability performance monitoring function to evaluate and report bulk electric system reliability performance.

Such a function would assess large-scale outages and near misses to determine root causes and lessons learned, similar to the August 14 blackout investigation. This function would incorporate the current Disturbance Analysis Working Group and expand that work to provide more proactive feedback to the NERC board regarding reliability performance. This program would also gather and analyze reliability performance statistics to inform the board of reliability trends. This function could develop procedures and capabilities to initiate investigations in the event of future large-scale outages or disturbances. Such procedures and capabilities would be shared between NERC and the regional reliability councils for use as needed, with NERC and regional investigation roles clearly defined in advance.

Recommendation 6. Improve Operator and Reliability Coordinator Training.

NERC found during its investigation that some reliability coordinators and control area operators had not received adequate training in recognizing and responding to system emergencies. Most notable was the lack of realistic simulations and drills for training and verifying the capabilities of operating personnel. This training deficiency contributed to the lack of situational awareness and failure to declare an emergency when operator intervention was still possible prior to the high speed portion of the sequence of events.

Recommendation 6: All reliability coordinators, control areas, and transmission operators shall provide at least five days per year of training and drills in system emergencies, using realistic simulations[5], for each staff person with responsibility for the real-time operation or reliability monitoring of the bulk electric system. This system emergency training is in addition to other training requirements. Five days of system emergency training and drills are to be completed prior to June 30, 2004, with credit given for documented training already completed since July 1, 2003. Training documents, including curriculum, training methods, and individual training records, are to be available for verification during reliability readiness audits.

NERC has published Continuing Education Criteria specifying appropriate qualifications for continuing education providers and training activities.

In the longer term, the NERC Personnel Certification Governance Committee (PCGC), which is independent of the NERC board, should explore expanding the certification requirements of system operating personnel to include additional measures of competency in recognizing and responding to system emergencies. The current NERC certification examination is a written test of the NERC Operating Manual and other references relating to operator job duties, and is not by itself intended to be a complete demonstration of competency to handle system emergencies.

Recommendation 7. Evaluate Reactive Power and Voltage Control Practices.

The August 14 blackout investigation identified inconsistent practices in northeastern Ohio with regard to the setting and coordination of voltage limits and insufficient reactive power supply. Although the deficiency of reactive power supply in northeastern Ohio did not directly cause the blackout, it was a contributing factor and was a significant violation of existing reliability standards.

In particular, there appear to have been violations of NERC Planning Standard I.D.S1 requiring static and dynamic reactive power resources to meet the performance criteria specified in Table I of

[5] The term "realistic simulations" includes a variety of tools and methods that present operating personnel with situations to improve and test diagnostic and decision-making skills in an environment that resembles expected conditions during a particular type of system emergency. Although a full replica training simulator is one approach, lower cost alternatives such as PC-based simulators, tabletop drills, and simulated communications can be effective training aids if used properly.

Planning Standard I.A on Transmission Systems. Planning Standard II.B.S1 requires each regional reliability council to establish procedures for generating equipment data verification and testing, including reactive power capability. Planning Standard III.C.S1 requires that all synchronous generators connected to the interconnected transmission systems shall be operated with their excitation system in the automatic voltage control mode unless approved otherwise by the transmission system operator. S2 of this standard also requires that generators shall maintain a network voltage or reactive power output as required by the transmission system operator within the reactive capability of the units.

On one hand, the unsafe conditions on August 14 with respect to voltage in northeastern Ohio can be said to have resulted from violations of NERC planning criteria for reactive power and voltage control, and those violations should have been identified through the NERC and ECAR compliance monitoring programs (addressed by Recommendation 2). On the other hand, investigators believe these deficiencies are also symptomatic of a systematic breakdown of the reliability studies and practices in FE and the ECAR region that allowed unsafe voltage criteria to be set and used in study models and operations. There were also issues identified with reactive characteristics of loads, as addressed in Recommendation 14.

Recommendation 7a: The Planning Committee shall reevaluate within one year the effectiveness of the existing reactive power and voltage control standards and how they are being implemented in practice in the ten NERC regions. Based on this evaluation, the Planning Committee shall recommend revisions to standards or process improvements to ensure voltage control and stability issues are adequately addressed.

Recommendation 7b: ECAR shall no later than June 30, 2004 review its reactive power and voltage criteria and procedures, verify that its criteria and procedures are being fully implemented in regional and member studies and operations, and report the results to the NERC board.

Recommendation 8. Improve System Protection to Slow or Limit the Spread of Future Cascading Outages.

The importance of automatic control and protection systems in preventing, slowing, or mitigating the impact of a large-scale outage cannot be stressed enough. To underscore this point, following the trip of the Sammis-Star line at 4:06, the cascading failure into parts of eight states and two provinces, including the trip of over 531 generating units and over 400 transmission lines, was completed in the next eight minutes. Most of the event sequence, in fact, occurred in the final 12 seconds of the cascade. Likewise, the July 2, 1996 failure took less than 30 seconds and the August 10, 1996 failure took only 5 minutes. It is not practical to expect operators will always be able to analyze a massive, complex system failure and to take the appropriate corrective actions in a matter of a few minutes. The NERC investigators believe that two measures would have been crucial in slowing or stopping the uncontrolled cascade on August 14:

- Better application of zone 3 impedance relays on high voltage transmission lines
- Selective use of under-voltage load shedding.

First, beginning with the Sammis-Star line trip, most of the remaining line trips during the cascade phase were the result of the operation of a zone 3 relay for a perceived overload (a combination of high amperes and low voltage) on the protected line. If used, zone 3 relays typically act as an overreaching backup to the zone 1 and 2 relays, and are not intentionally set to operate on a line overload. However, under extreme conditions of low voltages and large power swings as seen on August 14, zone 3 relays can operate for overload conditions and propagate the outage to a wider area by essentially causing the system to "break up". Many of the zone 3 relays that operated during the August 14 cascading outage were not set with adequate margins above their emergency thermal ratings. For the short times involved, thermal heating is not a problem and the lines should not be tripped for overloads. Instead, power system protection devices should be set to address the specific condition of concern, such as a fault, out-of-step condition, etc., and should not compromise a power system's inherent physical capability to slow down or stop a cascading event.

Recommendation 8a: All transmission owners shall, no later than September 30, 2004, evaluate the zone 3 relay settings on all transmission lines operating at 230 kV and above for the purpose of verifying that each zone 3 relay is not set to trip on load under extreme emergency conditions[6]. In each case that a zone 3 relay is set so as to trip on load under extreme conditions, the transmission operator shall reset, upgrade, replace, or otherwise mitigate the overreach of those relays as soon as possible and on a priority basis, but no later than December 31, 2005. Upon completing analysis of its application of zone 3 relays, each transmission owner may no later than December 31, 2004 submit justification to NERC for applying zone 3 relays outside of these recommended parameters. The Planning Committee shall review such exceptions to ensure they do not increase the risk of widening a cascading failure of the power system.

A second key finding with regard to system protection was that if an automatic under-voltage load shedding scheme had been in place in the Cleveland-Akron area on August 14, there is a high probability the outage could have been limited to that area.

Recommendation 8b: Each regional reliability council shall complete an evaluation of the feasibility and benefits of installing under-voltage load shedding capability in load centers within the region that could become unstable as a result of being deficient in reactive power following credible multiple-contingency events. The regions are to complete the initial studies and report the results to NERC within one year. The regions are requested to promote the installation of under-voltage load shedding capabilities within critical areas, as determined by the studies to be effective in preventing an uncontrolled cascade of the power system.

The NERC investigation of the August 14 blackout has identified additional transmission and generation control and protection issues requiring further analysis. One concern is that generating unit control and protection schemes need to consider the full range of possible extreme system conditions, such as the low voltages and low and high frequencies experienced on August 14. The team also noted that improvements may be needed in under-frequency load shedding and its coordination with generator under-and over-frequency protection and controls.

[6] The NERC investigation team recommends that the zone 3 relay, if used, should not operate at or below 150% of the emergency ampere rating of a line, assuming a .85 per unit voltage and a line phase angle of 30 degrees.

Recommendation 8c: The Planning Committee shall evaluate Planning Standard III – System Protection and Control and propose within one year specific revisions to the criteria to adequately address the issue of slowing or limiting the propagation of a cascading failure. The board directs the Planning Committee to evaluate the lessons from August 14 regarding relay protection design and application and offer additional recommendations for improvement.

Recommendation 9. Clarify Reliability Coordinator and Control Area Functions, Responsibilities, Capabilities and Authorities.

Ambiguities in the NERC operating policies may have allowed entities involved in the August 14 blackout to make different interpretations regarding the functions, responsibilities, capabilities, and authorities of reliability coordinators and control areas. Characteristics and capabilities necessary to enable prompt recognition and effective response to system emergencies must be specified.

The lack of timely and accurate outage information resulted in degraded performance of state estimator and reliability assessment functions on August 14. There is a need to review options for sharing of outage information in the operating time horizon (e.g. 15 minutes or less), so as to ensure the accurate and timely sharing of outage data necessary to support real-time operating tools such as state estimators, real-time contingency analysis, and other system monitoring tools.

On August 14, reliability coordinator and control area communications regarding conditions in northeastern Ohio were ineffective, and in some cases confusing. Ineffective communications contributed to a lack of situational awareness and precluded effective actions to prevent the cascade. Consistent application of effective communications protocols, particularly during emergencies, is essential to reliability. Alternatives should be considered to one-on-one phone calls during an emergency to ensure all parties are getting timely and accurate information with a minimum number of calls.

NERC operating policies do not adequately specify critical facilities, leaving ambiguity regarding which facilities must be monitored by reliability coordinators. Nor do the policies adequately define criteria for declaring transmission system emergencies. Operating policies should also clearly specify that curtailing interchange transactions through the NERC Transmission Loading Relief (TLR) Procedure is not intended as a method for restoring the system from an actual Operating Security Limit violation to a secure operating state.

Recommendation 9: The Operating Committee shall complete the following by June 30, 2004:

- **Evaluate and revise the operating policies and procedures, or provide interpretations, to ensure reliability coordinator and control area functions, responsibilities, and authorities are completely and unambiguously defined.**
- **Evaluate and improve the tools and procedures for operator and reliability coordinator communications during emergencies.**
- **Evaluate and improve the tools and procedures for the timely exchange of outage information among control areas and reliability coordinators.**

Recommendation 10. Establish Guidelines for Real-Time Operating Tools.

The August 14 blackout was caused by a lack of situational awareness that was in turn the result of inadequate reliability tools and backup capabilities. Additionally, the failure of FE's control computers and alarm system contributed directly to the lack of situational awareness. Likewise, MISO's incomplete tool set and the failure of its state estimator to work effectively on August 14 contributed to the lack of situational awareness.

Recommendation 10: The Operating Committee shall within one year evaluate the real-time operating tools necessary for reliable operation and reliability coordination, including backup capabilities. The Operating Committee is directed to report both minimum acceptable capabilities for critical reliability functions and a guide of best practices.

This evaluation should include consideration of the following:

- Modeling requirements, such as model size and fidelity, real and reactive load modeling, sensitivity analyses, accuracy analyses, validation, measurement, observability, update procedures, and procedures for the timely exchange of modeling data.
- State estimation requirements, such as periodicity of execution, monitoring external facilities, solution quality, topology error and measurement error detection, failure rates including times between failures, presentation of solution results including alarms, and troubleshooting procedures.
- Real-time contingency analysis requirements, such as contingency definition, periodicity of execution, monitoring external facilities, solution quality, post-contingency automatic actions, failure rates including mean/maximum times between failures, reporting of results, presentation of solution results including alarms, and troubleshooting procedures including procedures for investigating unsolvable contingencies.

Recommendation 11. Evaluate Lessons Learned During System Restoration.

The efforts to restore the power system and customer service following the outage were effective, considering the massive amount of load lost and the large number of generators and transmission lines that tripped. Fortunately, the restoration was aided by the ability to energize transmission from neighboring systems, thereby speeding the recovery. Despite the apparent success of the restoration effort, it is important to evaluate the results in more detail to determine opportunities for improvement. Blackstart and restoration plans are often developed through study of simulated conditions. Robust testing of live systems is difficult because of the risk of disturbing the system or interrupting customers. The August 14 blackout provides a valuable opportunity to apply actual events and experiences to learn to better prepare for system blackstart and restoration in the future. That opportunity should not be lost, despite the relative success of the restoration phase of the outage.

Recommendation 11a: The Planning Committee, working in conjunction with the Operating Committee, NPCC, ECAR, and PJM, shall evaluate the black start and system restoration performance following the outage of August 14, and within one year report to the NERC board the results of that evaluation with recommendations for improvement.

Recommendation 11b: All regional reliability councils shall, within six months of the Planning Committee report to the NERC board, reevaluate their procedures and plans to assure an effective blackstart and restoration capability within their region.

Recommendation 12. Install Additional Time-Synchronized Recording Devices as Needed.

A valuable lesson from the August 14 blackout is the importance of having time-synchronized system data recorders. NERC investigators labored over thousands of data items to synchronize the sequence of events, much like putting together small pieces of a very large puzzle. That process would have been significantly improved and sped up if there had been a sufficient number of synchronized data recording devices.

NERC Planning Standard I.F – Disturbance Monitoring does require location of recording devices for disturbance analysis. Often time, recorders are available, but they are not synchronized to a time standard. All digital fault recorders, digital event recorders, and power system disturbance recorders should be time stamped at the point of observation with a precise Global Positioning Satellite (GPS) synchronizing signal. Recording and time-synchronization equipment should be monitored and calibrated to assure accuracy and reliability.

Time-synchronized devices, such as phasor measurement units, can also be beneficial for monitoring a wide-area view of power system conditions in real-time, such as demonstrated in WECC with their Wide-Area Monitoring System (WAMS).

Recommendation 12a: The reliability regions, coordinated through the NERC Planning Committee, shall within one year define regional criteria for the application of synchronized recording devices in power plants and substations. Regions are requested to facilitate the installation of an appropriate number, type and location of devices within the region as soon as practical to allow accurate recording of future system disturbances and to facilitate benchmarking of simulation studies by comparison to actual disturbances.

Recommendation 12b: Facilities owners shall, in accordance with regional criteria, upgrade existing dynamic recorders to include GPS time synchronization and, as necessary, install additional dynamic recorders.

Recommendation 13. Reevaluate System Design, Planning and Operating Criteria.

The investigation report noted that FE entered the day on August 14 with insufficient resources to stay within operating limits following a credible set of contingencies, such as the loss of the East Lake 5 unit and the Chamberlin-Harding line. NERC will conduct an evaluation of operations planning practices and criteria to ensure expected practices are sufficient and well understood. The review will reexamine fundamental operating criteria, such as n-1 and the 30-minute limit in preparing the system for a next contingency, and Table I Category C.3 of the NERC planning standards. Operations planning and operating criteria will be identified that are sufficient to ensure the system is in a known and reliable condition at all times, and that positive controls, whether

manual or automatic, are available and appropriately located at all times to return the Interconnection to a secure condition. Daily operations planning, and subsequent real time operations planning will identify available system reserves to meet operating criteria.

Recommendation 13a: The Operating Committee shall evaluate operations planning and operating criteria and recommend revisions in a report to the board within one year.

Prior studies in the ECAR region did not adequately define the system conditions that were observed on August 14. Severe contingency criteria were not adequate to address the events of August 14 that led to the uncontrolled cascade. Also, northeastern Ohio was found to have insufficient reactive support to serve its loads and meet import criteria. Instances were also noted in the FE system and ECAR area of different ratings being used for the same facility by planners and operators and among entities, making the models used for system planning and operation suspect. NERC and the regional reliability councils must take steps to assure facility ratings are being determined using consistent criteria and being effectively shared and reviewed among entities and among planners and operators.

Recommendation 13b: ECAR shall no later than June 30, 2004 reevaluate its planning and study procedures and practices to ensure they are in compliance with NERC standards, ECAR Document No. 1, and other relevant criteria; and that ECAR and its members' studies are being implemented as required.

Recommendation 13c: The Planning Committee, working in conjunction with the regional reliability councils, shall within two years reevaluate the criteria, methods and practices used for system design, planning and analysis; and shall report the results and recommendations to the NERC board. This review shall include an evaluation of transmission facility ratings methods and practices, and the sharing of consistent ratings information.

Regional reliability councils may consider assembling a regional database that includes the ratings of all bulk electric system (100 kV and higher voltage) transmission lines, transformers, phase angle regulators, and phase shifters. This database should be shared with neighboring regions as needed for system planning and analysis.

NERC and the regional reliability councils should review the scope, frequency, and coordination of interregional studies, to include the possible need for simultaneous transfer studies. Study criteria will be reviewed, particularly the maximum credible contingency criteria used for system analysis. Each control area will be required to identify, for both the planning and operating time horizons, the planned emergency import capabilities for each major load area.

Recommendation 14. Improve System Modeling Data and Data Exchange Practices.

The after-the-fact models developed to simulate August 14 conditions and events indicate that dynamic modeling assumptions, including generator and load power factors, used in planning and operating models were inaccurate. Of particular note, the assumptions of load power factor were overly optimistic (loads were absorbing much more reactive power than pre-August 14 models indicated). Another suspected problem is modeling of shunt capacitors under depressed voltage

conditions. Regional reliability councils should establish regional power system models that enable the sharing of consistent, validated data among entities in the region. Power flow and transient stability simulations should be periodically compared (benchmarked) with actual system events to validate model data. Viable load (including load power factor) and generator testing programs are necessary to improve agreement between power flows and dynamic simulations and the actual system performance.

Recommendation 14: The regional reliability councils shall within one year establish and begin implementing criteria and procedures for validating data used in power flow models and dynamic simulations by benchmarking model data with actual system performance. Validated modeling data shall be exchanged on an inter-regional basis as needed for reliable system planning and operation.

During the data collection phase of the blackout investigation, when control areas were asked for information pertaining to merchant generation within their area, data was frequently not supplied. The reason often given was that the control area did not know the status or output of the generator at a given point in time. Another reason was the commercial sensitivity or confidentiality of such data.

Attachment A to Recommendation 1

Corrective Actions to Be Taken by FirstEnergy, Midwest Independent System Operator and PJM Draft – January 26, 2004

This attachment identifies corrective actions to be completed by FE, MISO, and PJM no later than June 30, 2004, as referenced in NERC Recommendation 1. These actions are intended to assure peer operating systems and reliability coordinators, regulators, electricity customers, and the public that the specific deficiencies leading to the August 14, 2003 cascading outage have been resolved and will not be the cause of a similar outage in the near future.

A. Corrective Actions to Be Completed by FirstEnergy

FirstEnergy shall complete the following corrective actions by June 30, 2004. Unless otherwise stated, the requirements apply to FE's northern Ohio system and connected generators.

1. Voltage Criteria and Reactive Resources

a. **Interim Voltage Criteria.** The investigation team found that FE was not operating on August 14 within NERC planning and operating criteria with respect to its voltage profile and reactive power supply margin in the Cleveland-Akron area. FE was also operating in apparent violation of its own historical planning and operating criteria that were developed and used by Centerior Energy Corporation (The Cleveland Electric Illuminating Company and the Toledo Edison Company) prior to 1998 to meet the relevant NERC and ECAR standards and criteria. FE's stated acceptable ranges for voltage are not compatible with neighboring systems or interconnected systems in general.

   Until such time that the study of the northern Ohio system ordered by the Federal Energy Regulatory Commission (FERC) on December 23 is completed, and until FE is able to determine (in b. below) a current set of voltage and reactive requirements verified to be within NERC and ECAR criteria, FE shall immediately operate such that voltages at all 345 kV buses in the Cleveland-Akron area shall have a minimum voltage of .95 per unit following the simultaneous loss of the two largest generating units in that area.

b. **Calculation of Minimum Bus Voltages and Reactive Reserves.** FE shall, consistent with or as part of the FERC-ordered study, determine the minimum location-specific voltages at all 345 kV and 138 kV buses and all generating stations within their control area (including merchant plants). FE shall determine the minimum dynamic reactive reserves that must be maintained in local areas to ensure that these minimum voltages are met following contingencies studied in accordance with ECAR Document 1. Criteria and minimum voltage requirements

must comply with NERC planning criteria, including Table 1A, Category C3, and Operating Policy 2.

c. **Voltage Procedures.** FE shall determine voltage and reactive criteria and procedures to enable operators to understand and operate to these criteria.

d. **Study Results.** When the FERC-ordered study is completed, FE is to adopt the planning and operating criteria determined as a result of that study and update the operating criteria and procedures for its system operators. If the study indicates a need for system reinforcements, FE shall develop a plan for developing such reinforcements as soon as practical, and shall develop operational procedures or other mitigating programs to maintain safe operating conditions until such time that the necessary system reinforcements can be made.

e. **Reactive Resources.** FE shall inspect all reactive resources, including generators, and assure that all are fully operational. FE shall verify that all installed capacitors have no blown fuses and that at least 98% of installed capacitors at 69 kV and higher are available and in service during the summer 2004.

f. **Communications.** FE shall communicate its voltage criteria and procedures, as described in the items above to MISO and FE's neighboring systems.

2. Operational Preparedness and Action Plan

FE's 2003 Summer Assessment was not considered to be sufficiently comprehensive to cover a wide range of known and expected system conditions, nor effective for the August 14 conditions based on the following:

- No voltage stability assessment was included to assess the Cleveland-Akron area which has a long-known history of potential voltage collapse, as indicated CEI studies prior to 1997, by non-convergence of powerflow studies in the 1998 analysis, and advice from AEP of potential voltage collapse prior to the onset of 2003 summer load period.
- Only single contingencies were tested for basically one set of 2003 study conditions. This does not comply with the study requirements of ECAR Document 1.
- Study conditions should have assumed a wider range of generation dispatch and import/export and inter-regional transfers. For example, imports from MECS (north-to-south transfers) are likely to be less stressful to the FE system than imports from AEP (south-to-north transfers). Sensitivity studies should have been conducted to assess the impact of each key parameter and derive the system operating limits accordingly based on the most limiting of transient stability, voltage stability and thermal capability.

- The 2003 study conditions are considered to be more onerous than those assumed in the 1998 study, since the former has Davis Besse (830 MW) as a scheduled outage. However, the 2003 study does not show any voltage instability problems as shown by the 1998 study.
- The 2003 study conditions are far less onerous than the actual August 14 conditions from the generation and transmission availability viewpoint. This is another indication that n-1 contingency assessment, based on one assumed system condition, is not sufficient to cover the variability of changing system conditions due to forced outages.

FE shall prepare and submit to ECAR, with a copy to NERC, an Operational Preparedness and Action Plan to ensure system security and full compliance with NERC and planning and operating criteria, including ECAR Document 1. The action plan shall include, but not be limited to the following:

a. **2004 Summer Studies.** Complete a 2004 summer study to identify a comprehensive set of System Operating Limits (SOL) and Interconnection Reliability Limits (IRLs) based on the NERC Operating Limit Definition Task Force Report. Any inter-dependency between FE's SOL and those of its neighboring entities, known and forecasted regional and interregional transfers shall be included in the derivation of SOL and IRL.

b. **Extreme Contingencies.** Identify high risk contingencies that are beyond normal studied criteria and determine the performance of the system for these contingencies. Where these extreme contingencies result in cascading outages, determine means to reduce their probability of occurrence or impact. These contingencies and mitigation plans must be communicated to FE operators, ECAR, MISO, and neighboring systems.

c. **Maximum Import Capability.** Determine the maximum import capability into the Cleveland-Akron area for the summer of 2004, consistent with the criteria stated in (1) above and all applicable NERC and ECAR criteria. The maximum import capability shall take into account historical and forecasted transactions and outage conditions expected with due regard to maintaining adequate operating and local dynamic reactive reserves.

d. **Vegetation Management.** FE was found to not be complying with its own procedures for right-of-way maintenance and was not adequately resolving inspection and forced outage reports indicating persistent problems with vegetation contacts prior to August 14, 2003. FE shall complete rights-of-way trimming for all 345 kV and 138 kV transmission lines, so as to be in compliance with the National Electrical Safety Code criteria for safe clearances for overhead conductors, other applicable federal, state and local laws, and FE's right-of-way maintenance procedures. Priority should be placed on completing work for all 345 kV lines as soon as possible. FE will report monthly progress to NERC and ECAR.

e. **Line Ratings.** FE shall reevaluate its criteria for calculating line ratings, survey the 345 kV and 138 kV rights-of-way by visual inspection to ensure line ratings are appropriate for the clearances observed, and calculate updated ratings for each line. FE shall ensure that system operators, MISO, ECAR, NERC (MMWG), and neighboring systems are informed of and able to use the updated line ratings.

3. **Emergency Response Capabilities and Preparedness**

a. **Emergency Response Resources.** FE shall develop a capability no later than June 30, 2004 to reduce load in the Cleveland-Akron area by 1,500 MW within ten minutes of a directive to do so by MISO or the FE system operator. Such a capability may be provided by automatic or manual load shedding, voltage reduction, direct-controlled commercial or residential load management, or any other method or combination of methods capable of achieving the 1,500 MW of reduction in ten minutes without adversely affecting other interconnected systems. The amount of required load reduction capability may be reduced to an amount shown by the FERC-ordered study to be sufficient for response to severe contingencies and if approved by ECAR and NERC.

b. **Emergency Response Plan.** FE shall develop emergency response plans, including plans to deploy the load reduction capabilities noted above. The plan shall include criteria for declaring an emergency and various states of emergency. The plan shall include detailed description of authorities, operating procedures, and communication protocols with all the relevant entities including MISO, FE operators, and market participants within the FE area that have ability move generation or shed load upon orders from FE operators. The plan shall include procedures for load restoration after the declaration that the FE system is no longer in the emergency operating state.

4. **Operating Center and Training**

a. **Operator Communications.** FE shall develop communications procedures for FE operating personnel to use within FE, with MISO and neighboring systems, and others. The procedure and the operating environment within the FE system control center shall allow focus on reliable system operation and avoid distractions such as calls from customers and others who are not responsible for operation of a portion of the transmission system.

b. **Reliability Monitoring Tools.** FE shall ensure its state estimation and real-time contingency analysis functions are being used to reliably execute full contingency analysis automatically every ten minutes, or on demand, and to alarm operators of potential first contingency violations.

c. **System Visualization Tools.** FE shall provide its operating personnel with the capability to visualize the status of the power system from an overview

perspective and to determine critical system failures or unsafe conditions quickly without multiple-step searches for failures. A dynamic map board or equivalent capability is encouraged.

d. **Backup Functions and Center.** FE shall develop and prepare to implement a plan for the loss of its system operating center or any portion of its critical operating functions. FE shall comport with the criteria of the NERC Reference Document – Back Up Control Centers, and ensure that FE is able to continue meeting all NERC and ECAR criteria in the event the operating center becomes unavailable. Consideration should be given to using capabilities at MISO or neighboring systems as a backup capability, at least for summer 2004 until alternative backup functionality can be provided.

e. **GE XA21 System Updates.** Until the current energy management system is replaced, FE shall incorporate all fixes for the GE XA21 system known to be necessary to assure reliable and stable operation of critical reliability functions, and particularly to correct the alarm processor failure that occurred on August 14, 2003.

f. **Operator Training.** Prior to June 30, 2004 FE shall meet the operator training requirements detailed in NERC Recommendation 6.

g. **Technical Support.** FE shall develop and implement a written procedure describing the interactions between control center technical support personnel and system operators. The procedure shall address notification of loss of critical functionality and testing procedures.

B. Corrective Actions to Be Completed by MISO

MISO shall complete the following corrective actions no later than June 30, 2004.

1. **Reliability Tools.** MISO shall fully implement and test its topology processor to provide its operating personnel real-time view of the system status for all transmission lines operating and all generating units within its system, and all critical transmission lines and generating units in neighboring systems. Alarms should be provided for operators for all critical transmission line outages. MISO shall establish a means of exchanging outage information with its members and neighboring systems such that the MISO state estimation has accurate and timely information to perform as designed. MISO shall fully implement and test its state estimation and real-time contingency analysis tools to ensure they can operate reliably no less than every ten minutes. MISO shall provide backup capability for all functions critical to reliability.

2. **Visualization Tools.** MISO shall provide its operating personnel tools to quickly visualize system status and failures of key lines, generators or equipment. The visualization shall include a high level voltage profile of the systems at least within the MISO footprint.

3. **Training.** Prior to June 30, 2004 MISO shall meet the operator training criteria stated in NERC Recommendation 6.

4. **Communications.** MISO shall reevaluate and improve its communications protocols and procedures with operational support personnel within MISO, its operating members, and its neighboring control areas and reliability coordinators.

5. **Operating Agreements.** MISO shall reevaluate its operating agreements with member entities to verify its authority to address operating issues, including voltage and reactive management, voltage scheduling, the deployment and redispatch of real and reactive reserves for emergency response, and the authority to direct actions during system emergencies, including shedding load.

C. Corrective Actions to Be Completed by PJM

PJM shall complete the following corrective actions no later than June 30, 2004.

1. **Communications.** PJM shall reevaluate and improve its communications protocols and procedures between PJM and its neighboring reliability coordinators and control areas.

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

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

June 11, 2003

Implementation Plan — Urgent Action Cyber Security Standard

The intent of the proposed NERC cyber security standard is to ensure that all entities responsible for the reliability of the bulk electric systems of North America identify and protect critical cyber assets that control or could impact the reliability of the bulk electric systems.

Although the urgent action cyber security standard is written using NERC's functional model, entities performing these functions have not yet been certified. NERC has historically developed its standards on a control area basis. Because all North American bulk electric systems are monitored by NERC certified control areas and reliability coordinators, the NERC Compliance and Enforcement Program (CEP) will evaluate only control areas and reliability coordinators for compliance with this standard in 2004. Other entities identified in the standard are expected to work to meet the requirements of the standard; however, self-certification forms will not be required.

To provide time for responsible entities to examine their policies and procedures and to assemble the necessary documentation to meet the requirements of the standard, compliance with this standard will not be evaluated until the first quarter of 2004.

Urgent action standards are valid for one year unless the industry votes to approve a one-year extension. Development of a permanent replacement for the urgent action cyber security standard has been approved by the NERC Standards Authorization Committee (SAC). A separate, formal compliance review and audit procedure will be included in the implementation plan developed for the permanent standard.

Implementation Schedule

2003 — (Assumes Ballot Pool approves Urgent Action Cyber Security Standard)

The NERC Board of Trustees adopts the urgent action cyber security standard in the summer of 2003. The standard becomes mandatory for NERC and NERC Regional Reliability Council members subject to the schedule outlined in this implementation plan. Control areas and reliability coordinators must initiate internal reviews and examine their policies and procedures to ensure that they meet the standard on or before these scheduled dates.

NERC and its Regions will develop self-certification forms as part of their compliance and enforcement programs. The Regions will distribute these forms to the control areas and reliability coordinators within their respective Regions.

Regions may ask other entities to provide self-certification forms if the Region believes that these entities are performing one of the functions identified in the standard. In such cases, the completion of a self-certification form by those other than control areas and reliability coordinators will be at the entity's discretion.

2004

All control areas and reliability coordinators will complete and submit the appropriate Regional self-certification form, indicating their compliance or degree of non-compliance with the requirements of the cyber security standard during the first quarter of 2004. These self-certification forms will be submitted to the appropriate NERC Regional Reliability Council, which will hold the individual responses in confidence.

Compliance with the standard will be used to determine the overall level of cyber security preparedness in the industry. Self-certification results will be aggregated by the NERC Regions and reported to NERC. This data will illustrate whether the industry is substantially compliant with the standard in the beginning of 2004.

Neither the Regions nor NERC will issue letters of non-compliance to those who indicate, via self-certification, that they do not fully comply with the requirements of this standard.

Neither the Regions nor NERC will conduct audits to verify the self-certifications.

No monetary sanctions will be levied for violations of this standard.

2005 and Beyond

Should a permanent standard be developed to replace the urgent action cyber security standard, a new implementation plan will be developed in conjunction with that standard.

In the event that a permanent standard is not yet developed and a one-year extension is requested for the urgent action cyber security standard, the industry will be given an opportunity to vote on the extension of the standard and any implementation plan associated with it. It is likely that another self-certification may be required in the first quarter of 2005, if the standard is extended.

Similar to 2004, only aggregated data would be submitted to NERC. The NERC Regions would hold company-specific data in confidence. From the aggregated data, an overall assessment of the state of the industry participants in meeting the standard can be developed. For 2005, the intent would be that all industry participants would be fully compliant with the standard.

1200 — CYBER SECURITY

1. **Purpose:** To reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets.
2. **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.
3. **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.

1201 — Cyber Security Policy

1. Requirement

1.1. 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.

1.2. 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.

2. Measures

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

2.2. The responsible entity shall review the cyber security policy at least annually.

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

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

3. Regional Differences

None identified.

4. Compliance Monitoring Process

4.1. 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.

4.2. 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.

4.3. The responsible entity shall make the following available for inspection by the compliance monitor upon request:

4.3.1. Written cyber security policy;

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

4.3.3. Documentation of justification for any deviations or exemptions.

5. Levels of Noncompliance

5.1. Level one:

5.1.1. A current senior management official was not designated for less than 30 days during a calendar year; or

5.1.2. A written cyber security policy exists but has not been reviewed in the last calendar year.

5.2. Level two: A current senior management official was not designated for 30 or more days, but less than 60 days during a calendar year.

5.3. Level three: A current senior management official was not designated for 60 or more days, but less than 90 days during a calendar year

5.4. Level four:

5.4.1. A current senior management official was not designated for more than 90 days during a calendar year; or

5.4.2. No cyber security policy exists.

6. Sanctions

6.1. 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.

1202 — Critical Cyber Assets

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 its critical cyber assets.

2. Measures

   2.1. The responsible entity shall maintain a document identifying critical cyber assets.

   2.2. The responsible entity shall review and update its critical cyber asset identification document at least annually or within 90 days of the addition or removal of any critical cyber assets.

3. **Regional Differences**

   None identified.

4. **Compliance Monitoring Process**

   4.1. 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.

   4.2. 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.

   4.3. The responsible entity shall make the following available for inspection by the compliance monitor upon request:

      4.3.1. List of critical cyber assets; and

      4.3.2. Verification that necessary updates were made at least annually or within 90 days of the addition or removal of critical cyber assets.

5. **Levels of Noncompliance**

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

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

   5.3. Level three: (None specified.)

   5.4. Level four: No document exists.

6. Sanctions

   6.1. 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.

1203 — Electronic Security Perimeter

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 its electronic security perimeter(s).

2. **Measures**

   2.1. 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).

   2.2. The responsible entity shall review and update its document referenced in 1203.2.1 at least annually or within 90 days of the modification of the network.

3. **Regional Differences**

   None identified.

4. **Compliance Monitoring Process**

   4.1. 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.

   4.2. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

   4.3. The responsible entity shall make the following available for inspection by the compliance monitor upon request:

      4.3.1. Document as described in 1203.2.1; and

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

5. **Levels of Noncompliance**

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

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

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

   5.4. Level four: No document exists.

6. **Sanctions**

   6.1. 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.

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.

2. Measures

   2.1. The responsible entity shall maintain a document identifying the access controls and their implementation for each electronic access point to the electronic security perimeter(s).

   2.2. The responsible entity shall review and update the documentation referenced in 1204.2.1 at least annually or within 90 days of the modification of the electronic security perimeter or the electronic access controls.

3. **Regional Differences**

   None identified.

4. **Compliance Monitoring Process**

   4.1. 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.

   4.2. 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.

   4.3. The responsible entity shall make the following available for inspection by the compliance monitor upon request:

      4.3.1. Document as described in 1204.2.1; and

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

5. **Levels of Noncompliance**

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

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

   5.3. Level three: Document exists, but the document does not identify the electronic access controls for one or more access points.

   5.4. Level four: No document exists.

6. Sanctions

   6.1. 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.

1205 — Physical Security Perimeter

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 its physical security perimeter(s) for the protection of critical cyber assets.

2. Measures

2.1. The responsible entity shall maintain a document depicting the physical security perimeter(s) and all physical access points to every such perimeter. The document shall verify that all critical cyber assets are within the physical security perimeter(s).

2.2. The responsible entity shall review and update the document referenced in 1205.2.1 at least annually or within 90 days of the modification of the network.

3. Regional Differences

None identified.

4. Compliance Monitoring Process

4.1. 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.

4.2. 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.

4.3. The responsible entity shall make the following available for inspection by the compliance monitor upon request:

4.3.1. Document as described in 1205.2.1; and

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

5. Levels of Noncompliance

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

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

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

5.4. Level four: No document exists.

6. Sanctions

6.1. 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.

1206 — Physical 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 physical access controls for access to critical cyber assets within the physical security perimeter(s).

2. Measures

2.1. The responsible entity shall maintain a document identifying the access controls and their implementation for each physical access point to the physical security perimeter(s).

2.2. The responsible entity shall review and update the documentation referenced in 1206.2.1 at least annually or within 90 days of the modification of the physical security perimeter(s) or the physical access controls.

3. Regional Differences

None identified.

4. Compliance Monitoring Process

4.1. 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.

4.2. The responsible entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years.

4.3. The responsible entity shall make the following available for inspection by the compliance monitor upon request:

4.3.1. Document as described in 1206.2.1; and

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

5. Levels of Noncompliance

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

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

5.3. Level three: Document exists, but the document does not identify the physical access controls for one or more access points.

5.4. Level four: No document exists.

6. Sanctions

6.1. 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

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).

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.

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.

3. Regional Differences

None identified.

4. Compliance Monitoring Process

4.1. 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.

4.2. 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.

4.3. The responsible entity shall make the following available for inspection by the compliance monitor upon request:

4.3.1. Document as described in 1207.2.1;

4.3.2. Verification that necessary updates were made at least quarterly or within 24 hours of a modification; and

4.3.3. Verification that personnel background checks are being conducted consistent with access granted to them.

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.

5.2. Level two:

5.2.1. Access control rights list is available, but has not been updated or reviewed for more than 6 months but less than 12 months; or

5.2.2. More than one but not more than five instances of personnel termination (employee, contractor or service vendor) in which the access control list was not updated within 24 hours.

5.3. Level three:

5.3.1. Access control rights list is available, but does not include service vendors;

5.3.2. More than five instances of personnel termination (employee, contractor or service vendor) in which the access control list was not updated within 24 hours; or

5.3.3. No personnel background screening conducted.

5.4. Level four: Access control rights list does not exist.

6. Sanctions

6.1. 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.

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.

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.

3. **Regional Differences**

   None identified.

4. **Compliance Monitoring Process**

   4.1. 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.

   4.2. 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 for three years.

   4.3. The responsible entity shall make the following available for inspection by the compliance monitor upon request:

      4.3.1. Document as described in 1208.2.1;

      4.3.2. Records of physical access to critical cyber assets; and

      4.3.3. Demonstration that the list of access control rights is controlled by video or other physical monitoring.

5. **Levels of Noncompliance**

   5.1. Level one: Monitoring is in place, but a gap in the logs or other measures exists for less than seven days.

   5.2. Level two: Access not monitored to any critical cyber asset for less than one day.

   5.3. Level three:

      5.3.1. Access not monitored to any critical cyber asset for more than one day but less than one week; or

      5.3.2. Log or other monitoring reveals access by personnel not approved on the access control list.

   5.4. Level four: No monitoring of access exists.

6. Sanctions

   6.1. 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.

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.

3. **Regional Differences**

   None identified.

4. **Compliance Monitoring Process**

   4.1. 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.

   4.2. 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.

   4.3. The responsible entity shall make the following available for inspection by the compliance monitor upon request:

      4.3.1. Document as described in 1209.2.1;

      4.3.2. Records of electronic access to critical cyber assets; and

      4.3.3. Demonstration that the list of access control rights is verified.

5. **Levels of Noncompliance**

   5.1. Level one: Monitoring is in place, but a gap in the access records exists for less than seven days.

   5.2. Level two: Access not monitored to any critical cyber asset for less than one day.

   5.3. Level three:

      5.3.1. Access not monitored to any critical cyber asset for more than one day but less than one week; or

      5.3.2. Access records reveal access by personnel not approved on the access control list.

   5.4. Level four: No monitoring of access exists.

6. Sanctions

   6.1. 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.

1210 — Information Protection

1. **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.

2. **Measures**

   2.1. 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.

   2.2. The responsible entity shall review and update the document referred to in 1210.2.1 as necessary and at least annually.

3. **Regional Differences**

   None identified.

4. **Compliance Monitoring Process**

   4.1. 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.

   4.2. 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.

   4.3. The responsible entity shall make the document as described in 1210.2.1 available for inspection by the compliance monitor upon request.

5. **Levels of Noncompliance**

   5.1. Level one: Document exists, but document has not been reviewed or updated in the last 12 months.

   5.2. Level two: Document exists, but does not cover one of the specific items identified.

   5.3. Level three: Document exists, but does not cover three of the specific items identified.

   5.4. Level four: No document exists.

6. **Sanctions**

   6.1. 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.

1211 — Training

1. Requirement

The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall train personnel commensurate with their access to critical cyber assets. The training shall address, at a minimum: the cyber security policy, physical and electronic access controls to critical cyber assets, the release of critical cyber asset information, potential threat incident reporting, and action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident. Training shall be conducted upon initial employment and reviewed annually.

2. Measures

2.1. The responsible entity shall develop and maintain a company-specific cyber security training program that includes, at a minimum, the following required items:

2.1.1. The cyber security policy;

2.1.2. Physical and electronic access controls to critical cyber assets;

2.1.3. The release of critical cyber asset information;

2.1.4. Potential threat incident reporting; and

2.1.5. Action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident.

2.2. The responsible entity shall maintain a document identifying all personnel who have access to critical cyber assets and the date of the successful completion of their training.

2.3. The responsible entity shall document that it has reviewed its training program at least annually.

3. Regional Differences

None identified.

4. Compliance Monitoring Process

4.1. 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.

4.2. 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.

4.3. The responsible entity shall make the training documents described in 1211.2.1, -2.2, and -2.3 available for inspection by the compliance monitor upon request.

5. Levels of Noncompliance

5.1. Level one: Training program exists, but records of training either do not exist or reveal some key personnel not trained as required.

5.2. Level two: Training program exists, but does not cover one of the specific items identified.

5.3. Level three: Document exists, but does not cover two of the specific items identified.

5.4. Level four: No training program exists addressing critical cyber assets.

6. Sanctions

6.1. 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.

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.

2. Measures

2.1. The responsible entity shall maintain a document identifying system management policies and procedures.

2.2. The responsible entity shall review and update the document referred to in 1212.2.1 as necessary and at least annually.

2.3. The system management policies and procedures document shall address all items in requirement 1212.1.

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

3. Regional Differences

None identified.

4. Compliance Monitoring Process

4.1. 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.

4.2. 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.

4.3. The responsible entity shall make the following available for inspection by the compliance monitor upon request:

4.3.1. Document as described in 1212.2.1; and

4.3.2. Verification that system management policies and procedures are being followed.

5. Levels of Noncompliance

5.1. Level one:

5.1.1. Document exists, but does not cover one of the specific items identified; or

5.1.2. The document has not been reviewed or updated in the last 12 months.

5.2. Level two: Document exists, but does not cover three of the specific items identified.

5.3. Level three: Document exists, but does not cover five of the specific items identified.

5.4. Level four: No document exists.

6. Sanctions

6.1. 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.

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.

2. Measures

2.1. The responsible entity shall maintain a document identifying test and acceptance criteria for the installation or modification of critical cyber assets.

2.2. The responsible entity shall maintain a document verifying that it has implemented the test and acceptance criteria.

3. Regional Differences

None identified.

4. Compliance Monitoring Process

4.1. 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.

4.2. 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.

4.3. The responsible entity shall make the documents described in 1213.2.1 and -2.2 available for inspection by the compliance monitor upon request.

5. Levels of Noncompliance

5.1. Level one: Test procedures and acceptance criteria document exists, but has not been reviewed or updated within the last 12 months.

5.2. Level two: (None specified.)

5.3. Level three: (None specified.)

5.4. Level four: Test procedures and acceptance criteria document does not exist.

6. Sanctions

6.1. 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.

1214 — Electronic Incident Response Actions

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 Procedure.*

3. **Regional Differences**

   None identified.

4. **Compliance Monitoring Process**

   4.1. 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.

   4.2. 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.

   4.3. The responsible entity shall make the document described in 1214.2.1 available for inspection by the compliance monitor upon request.

5. **Levels of Noncompliance**

   5.1. Level one: Electronic incident response plan exists, but has not been reviewed or updated in the last 12 months.

   5.2. Level two: (None specified.)

   5.3. Level three:

      5.3.1. Document exists, but does not assign responsibilities; or

      5.3.2. Document exists, but does not 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.*

   5.4. Level four: No document exists.

6. Sanctions

   6.1. 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 this urgent action standard.

1215 — Physical Incident Response Actions

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 physical 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 physical incident response action, including actions, roles and responsibilities.

   2.2. The document in 1215.2.1 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.*

3. **Regional Differences**

   None identified.

4. **Compliance Monitoring Process**

   4.1. 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.

   4.2. 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.

   4.3. The responsible entity shall make the document described in 1215.2.1 available for inspection by the compliance monitor upon request.

5. **Levels of Noncompliance**

   5.1. Level one: Physical incident response plan exists, but has not been reviewed or updated in the last 12 months.

   5.2. Level two: (None specified.)

   5.3. Level three:

      5.3.1. Document exists, but does not assign responsibilities; or

      5.3.2. Document exists, but does not 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.*

   5.4. Level four: No document exists.

6. **Sanctions**

   6.1. 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.

1216 — Recovery Plans

1. **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.

2. Measures

   2.1. The responsible entity shall maintain a document defining the action plan and procedures used to recover or re-establish critical cyber assets following a cyber security event, including actions, roles and responsibilities.

   2.2. The responsible entity shall maintain a document verifying that the action plan is exercised via drill at least annually.

3. **Regional Differences**

   None identified.

4. **Compliance Monitoring Process**

   4.1. 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.

   4.2. 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.

   4.3. The responsible entity shall make the documents described in 1216.2.1 and -2.2 available for inspection by the compliance monitor upon request.

5. **Levels of Noncompliance**

   5.1. Level one: Action plans and procedures exist, but have not been reviewed or updated in the last 12 months.

   5.2. Level two: Action plans and procedures have not been exercised through a drill in the last 12 months.

   5.3. Level three: Action plans and procedures do not define specific roles and responsibilities.

   5.4. Level four: No action plans of procedures exist.

6. Sanctions

   6.1. 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.

Sanctions Table

The following is an approved matrix of compliance sanctions developed by the Compliance Subcommittee as part of the NERC Compliance Enforcement Program and was approved by the NERC Board of Trustees.

Levels of noncompliance are tied to this matrix. The matrix is divided into four levels of increasing noncompliance vertically and the number of violations in a defined period at a given level horizontally.

In the enforcement matrix, note that there are three sanctions that can be used: a letter, a fixed fine, and a $$ per MW fine.

Letter

The letter is a sanction used to notify company executives, Regional officers, and regulators when an entity is non-compliant. The distribution of the letter varies depending on the severity of the noncompliance. It is used first to bring noncompliance to light to people who can influence the operation to become compliant.

- Letter (A) — Letter to the entity's vice president level or equivalent informing the entity of noncompliance, with copies to the data reporting contact, and the entity's highest ranking Regional Council representative.
- Letter (B) — Letter to the entity's chief executive officer or equivalent, with copies to the data reporting contact, the entity's highest ranking Regional Council representative, and the vice president over the area in which noncompliance occurred.
- Letter (C) — Letter to the entity's chief executive officer and chairman of the board, with copies to the NERC president, regulatory authorities having jurisdiction over the non-compliant entity (if requested by such regulatory authorities), the data reporting contact, the entity's highest ranking Regional Council representative, and the vice president over the area in which non-compliance occurred.

Fixed Dollars

This sanction is used when a letter is not enough and a stronger message is desired. Fixed dollars are typically assigned as a one-time fine that is ideal for measures involving planning-related standards. Many planning actions use forward-looking assumptions. If those assumptions prove wrong in the future, yet they are made in good faith using good practices, entities should not be harshly penalized for the outcome.

Dollars per MW

Dollars per MW sanctions are oriented toward operationally based standards. The MW can be load, generation, or flow on a line. Reasonableness of a sanction needs to be figured into assessing $/MW penalties. Assessing large financial penalties is not the goal, but sending a message with proper emphasis on $$$ can be controlled with the multiplier.

Occurrence Period Category	Number of Violations in Occurrence Period at a Given Level			
1st Period of Violations (Fully Compliant Last Period)	1	2	3	4 or more
2nd Consecutive Period of Violations		1	2	3 or more
		$ Sanction from Table; Letter (C) only if Letter (B) previously sent		
3rd Consecutive Period of Violations			1	2 or more
			$ Sanction from Table; Letter (C) only if Letter (B) previously sent	
4th or greater Consecutive Period of Violations				1
				$ Sanction from Table; Letter (C)

Level of Non-Compliance	Sanctions Associated with Non-compliance			
Level 1	Letter (A)	Letter (A)	Letter (B) and $1,000 or $1 Per MW	Letter (B) and $2,000 or $2 Per MW
Level 2	Letter (A)	Letter (B) and $1,000 or $1 Per MW	Letter (B) and $2,000 or $2 Per MW	Letter (B) and $4,000 or $4 Per MW
Level 3	Letter (B) and $1,000 or $1 Per MW	Letter (B) and $2,000 or $2 Per MW	Letter (B) and $4,000 or $4 Per MW	Letter (B) and $6,000 or $6 Per MW
Level 4	Letter (B) and $2,000 or $2 Per MW	Letter (B) and $4,000 or $4 Per MW	Letter (B) and $6,000 or $6 Per MW	Letter (B) and $10,000 or $10 Per MW

Interpreting the Tables:

- These tables address penalties for violations of the same measure occurring in consecutive compliance reporting periods.
- If a participant has non-compliant performance in consecutive compliance reporting periods, the sanctions applied are more punitive.

These definitions have been 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.

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.

U.S.-Canada Power System Outage Investigation

August 14, 2003 Blackout in the United States and Canada:

20 Key Recommendations

Overview

- Single most important recommendation: Congress should enact reliability provisions in H.R. 6/ S. 2095
- Overall, recommendations package is a roadmap to a reliable future
- 46 recommendations, in 4 groups:
  - Address institutional problems (14)
  - Strengthen NERC initiatives of Feb. 10, 2004 (17)
  - Improve physical and cyber security (13)
  - Address issues in Canadian nuclear power sector (2)

20 Key Recommendations

1. Make compliance mandatory and enforceable.
2. Establish regulator-approved funding for NERC and regional councils.
3. Strengthen reliability framework – e.g., metrics for reliability performance, criteria for selection of NERC Board, reassess role of regional reliability councils, set minimum functional requirements for reliability coordinators and control areas.

20 Key Recommendations - 2

4. Clarify that prudent reliability investments will be recoverable through transmission rates.
5. Track implementation of recommendations.
6. Correct the direct causes of the August 2003 blackout.
7. Establish enforceable standards for maintenance of electrical clearances in right-of-way areas.
8. Strengthen NERC Compliance Enforcement Program.
9. Strengthen NERC Reliability Readiness Audit Program.

20 Key Recommendations - 3

10. Improve training and certification requirements.
11. Define *normal, alert*, and *emergency* operating conditions. Clarify roles, responsibilities, and authorities of reliability coordinators and control areas for each condition.
12. Make wider use of system protection measures.
13. Strengthen reactive power and voltage control practices.
14. Improve quality of system modeling data and data exchange practices.

20 Key Recommendations - 4

15. Accelerate NERC's development and adoption of enforceable standards.
16. NERC and regional councils should tighten communications protocols, especially for communications during alerts and emergencies.
17. Implement NERC IT standards.
18. Develop and deploy IT management procedures.
19. Develop corporate-level IT security strategies.
20. Implement controls to manage IT system health, network monitoring, incident management.

Will More Blackouts Occur?

- System is highly reliable – but residual risks of design error, mechanical failure, and operator error are unavoidable.
- NERC's readiness audits are a key preventive measure.
- The U.S – Canada Task Force has been extended for a year to provide oversight for implementation of recommendations.

David.Meyer@hq.doe.gov

Exelon

Exelon Actions to Address Grid Reliability and Ensure Reactor Safety

Chris Crane
Chief Nuclear Officer
Exelon Corporation

Exelon Electrical Distribution Focus Areas

- Grid Reliability Self Assessment based on the U.S. – Canada Power System Outage Task Force Report (Nuclear Participated)
- Five Focus Areas
  - Vegetation Management
  - Real Time System Tool and Communication Systems
  - System Operation Processes and Procedures
  - Transmission System Restoration
  - Training
- Short & Long Term actions in each area

Nuclear Focus Areas

- Summer Readiness
- SOER 99-01 Actions
- Communications/Interface between Electrical Distribution and Nuclear

Summer Readiness

- Lessons learned from 2003 blackout
  - Operator training on grid instability response
  - Practice fast plant trip turnaround
  - Verify communications under loss of power
- All Site Vice-Presidents to supply Summer Readiness Certification letters
  - System readiness
  - Switchyard readiness
  - Outage plans
  - Contingency review
- Transmission Providers certify summer readiness
  - Upgrades to switchyard material condition and relaying

Exelon

SOER 99-01

All actions verified complete by INPO

- Interfaces established with grid operators
- Electrical grid degradation procedures reviewed for adequacy
- Equipment PMs under site responsibility reviewed
- Validity of assumptions for grid reliability and stability validated
- Operator training on degraded grid conditions

Communications/Interface with Electrical Distribution

- Monthly Executive Meeting between Electrical Distribution and Nuclear
- Improved communications between Electrical Distribution, Nuclear Duty Officer, and the Nuclear sites
- State Estimator for continuous monitoring and voltage event predicting
- Compensatory actions developed for switchyard voltage conditions
- Project plan developed for units without load tap changing transformers

Grid Reliability

Chuck Dugger
Vice President, Operations

NEI

Purpose

- Discuss industry activities

Industry Activities

- **SOER 99-01, Loss of Grid**
  - **Grid operator interfaces**
  - **Loss or degradation of the grid procedures**
  - **Grid reliability and stability design assumptions**
  - **Operator training**

Industry Activities (cont'd)

- **SOER 03-01, Emergency Power Reliability**
  - **Design vulnerabilities**
  - **Operating & Maintenance practices**
  - **Modification processes**
  - **Performance monitoring**
  - **Testing practices**

Industry Activities (cont'd)

- Review of losses of all offsite power events
- Configuration risk management practices
- Collaboration with NRC RES

Industry Activities (cont'd)

- Formed Industry Task Force
  - Survey of recent LOOP events & impact on plant licensing basis
  - Engage NRC staff
  - Monitor NERC Activities

NEI

Summary

- Awareness
  - Grid conditions
  - Impact on NPP
- Compliance
  - 50.63, 50.65(a)(4), GDC-17
  - Technical Specifications

Commission Briefing Grid Stability and Offsite Power Issues

Office of Nuclear Reactor Regulation

May 10, 2004

Briefing Topics

- Joint Task Force Report on August 14, 2003 Blackout
- Applicable Regulatory Requirements
- Staff Actions – Prior to Blackout Event
- Staff Actions – Short Term (Summer 2004)
- Staff Actions – Long Term

Joint Task Force Report on August 14, 2003 Blackout

- 9 plants tripped according to design
- No Nuclear Power Plant (NPP) Recommendations
- Significant Electric Working Group Recommendations

Regulatory Requirements

- 10 CFR Part 50 Appendix A, General Design Criteria (GDC) 17
- 10 CFR 50.63, Station Blackout Rule
- 10 CFR 50.65, Maintenance Rule
- Plant Technical Specifications

Staff Actions – Prior to 2003 Blackout Event

- In response to the 1996 Western Grid Disturbance, the staff conducted a number of activities to assess the risk and to make contact with the Federal Energy Regulatory Commission and the North American Electric Reliability Council

- No additional regulatory action recommended

Staff Actions – Prior to 2003 Blackout Event [Cont'd]

- In response to the Callaway Degraded Voltage Condition on August 11, 1999, the staff engaged the industry on loss of offsite power (LOOP) issues

- Regulatory Information Summary (RIS) 2000-24 documented staff concerns that high power flows due to grid operation can lead to voltage inadequacies

Staff Actions – Short Term (Summer 2004)

- Deterministic evaluation of issues (~50)
- Risk insights provided the following:
  - Long duration LOOPs are safety significant
  - Risk increases as the plant's ability to cope with event is decreased (e.g., Emergency Diesel Generator Allowable Outage Time)
  - Grid is less reliable during the Summer period

Staff Actions – Short Term (Summer 2004)[Cont'd]

- Objective: Ensure that nuclear power plants are ready in the event of an offsite power outage
  - Raise awareness among licensees

    => RIS 2004-05
  - Verify readiness of licensees

    => Temporary Instruction (TI)
  - Maintain cognizance of grid conditions during Summer 2004

Staff Actions – Long Term

- Future staff actions will be based upon
  - **TI and other operating experience feedback during the Summer of 2004**
  - **Office of Research Station Blackout Rule Study results to be completed in March 2005**
  - **Review of SBO considerations and determine regulatory actions June 2005**
- Activities will focus on the adequacy of existing regulatory requirements

Commission Briefing NPP/Grid's Report Issues Resolution Status

---

José Calvo

Office of Nuclear Reactor Regulation

May 10, 2004

Briefing Topics

- **Recommendations**
- **EEIB's grid-related activities**
- **NPP/Grid's report issues resolution status**
- **Electrical operating requirements**
- **NPP/Grid Needs**
- **Goals and objectives**

Recommendations

- **The staff should remain cognizant of the current status of grid issues, and assess future electric power grid reliability and its potential impact on NPPs' offsite power systems through its continued contacts with FERC, NERC and others.**

Recommendations (cont.)

- **In order to predict the likelihood of future blackout events and mitigating the impact of such events on the safe operation of NPPs, it would necessitate the collection of grid data available to FERC/ NERC. NRC staff should prepare a memorandum of understanding between NRC and FERC/NERC in this regard.**

Recommendations (cont.)

- The issuance of a generic letter or bulletin to verify that the licensing bases for the electric power systems for each NPP continue to be met and is documented in the UFSAR.

- To continue addressing the grid issues identified in the NPP/Grid's report.

- To establish an agency ombudsperson on technical matters.

EEIB grid-related activities
following 2003 power blackout event

- **Preliminary ASP analysis of NPPs affected by the 2003 blackout in October 2003—showed potential high risks.**
- **NPP/Grid's report issued in December 2003.**
- **EEIB assigned to resolve the issues identified in the NPP/Grid's report in January 2004.**
- **Action Plan issued in February 2004.**

NPP/Grid's report issues resolution status summary

- **10 issues on grid reliability**

→ **4- Compliance w/regulations--importance: high; resolution before summer of 2004: pending.**

→ **2- Engaging NRC staff w/external stakeholders–importance: high; resolution before summer of 2004: partially completed.**

NPP/Grid's report issues (cont.) resolution status summary

- **10 issues on grid reliability (cont.)**

→ **2- Depletion of MVARs resulting by power uprates—importance: medium; resolution before the summer of 2004: partially completed.**

→ **2- Work w/electric industry on cascading containment and cyber- attacks—importance: medium; resolution start in January 2004: partially started.**

NPP/Grid's report issues (cont.) resolution status summary

- 2 issues on risk assessment

→ CCDPs—importance: high; resolution before the summer of 2004: completed.

→ Collective risk—importance: low; resolution before the summer of 2004: incomplete.

NPP/Grid's report issues (cont.) resolution status summary

- 1 issue on the adequacy of SBO- importance: medium; resolution before the summer of 2004: pending.

- 3 issues on studies of underfrequency settings, grid operational data, and onsite power system improvements—importance: medium/low; resolution start in January 2004: effort has not started.

Electrical operating requirements General design criterion 17

- **Minimize the probability of losing electrical power from the remaining supplies.**

- **Underlying assumptions and licensing basis.**

→ **Before deregulation easily established.**

→ **After deregulation difficult to be established.**

- **First contingency.**

NPP/Grid Needs

- **NPP needs from the electric grid**

→ **Reliable grid ensures the availability of OSP.**

→ **Notification from grid operator of grid degradation.**

→ **Prompt restoration of OSP.**

→ **Collection of grid operational data to predict potential future risks.**

NPP/Grid Needs (cont.)

- **Grid needs from the NPP**

→ **Contribute to the reliability of the grid (without compromising safe NPP operation).**

→ **Reassessment of degraded voltage sensing.**

→ **Reassessment of NPP underfrequency trips.**

→ **Compensation for MVAR depletion attributed to power uprates.**

→ **Support by the NPP in the restoration of the grid following a major loop event.**

Goals and objectives

- **Boosting the NRC's capability to assess grid reliability into the 21st century.**
- **Update regulations for electric power systems of NPPs to address realistic operations of the grid in the 21st century.**
- **Significantly increase interactions between EEIB and external grid-related organizations.**

Goals and objectives (cont.)

- **Foster a work environment that values differing opinions and rewards safety-conscious thinking (NRC Performance Goal 3-Strategy 4).**

- **Persuading the Commission to establish an agency ombudsperson on technical matters.**