7. The August 14 Blackout Compared With Previous Major North American Outages

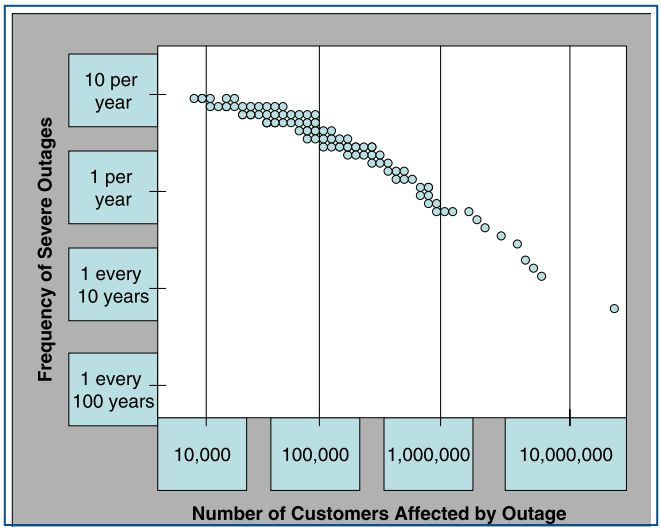
Incidence and Characteristics of Power System Outages

Short, localized outages occur on power systems fairly frequently. System-wide disturbances that affect many customers across a broad geographic area are rare, but they occur more frequently than a normal distribution of probabilities would predict. North American power system outages between 1984 and 1997 are shown in Figure 7.1 by the number of customers affected and the rate of occurrence. While some of these were widespread weather-related events, some were cascading events that, in retrospect, were preventable. Electric power systems are fairly robust and are capable of withstanding one or two contingency events, but they are fragile with respect to multiple contingency events unless the systems are readjusted between contingencies. With the shrinking margin in the current transmission system, it is likely to be more vulnerable to cascading outages than it was in the past, unless effective countermeasures are taken.

As evidenced by the absence of major transmission projects undertaken in North America over the past 10 to 15 years, utilities have found ways to increase the utilization of their existing facilities to meet increasing demands without adding significant high-voltage equipment. Without intervention, this trend is likely to continue. Pushing the system harder will undoubtedly increase reliability challenges. Special protection schemes may be relied on more to deal with particular challenges, but the system still will be less able to withstand unexpected contingencies.

A smaller transmission margin for reliability makes the preservation of system reliability a harder job than it used to be. The system is being operated closer to the edge of reliability than it was just a few years ago. Table 7.1 represents some of the changed conditions that make the preservation of reliability more challenging.

Figure 7.1. North American Power System Outages, 1984-1997



Note: The circles represent individual outages in North America between 1984 and 1997, plotted against the frequency of outages of equal or greater size over that period.

Source: Adapted from John Doyle, California Institute of Technology, "Complexity and Robustness," 1999. Data from NERC.

If nothing else changed, one could expect an increased frequency of large-scale events as compared to historical experience. The last and most extreme event shown in Figure 7.1 is the August 10, 1996, outage. August 14, 2003, surpassed that event in terms of severity. In addition, two significant outages in the month of September 2003 occurred abroad: one in England and one, initiated in Switzerland, that cascaded over much of Italy.

In the following sections, seven previous outages are reviewed and compared with the blackout of August 14, 2003: (1) Northeast blackout on November 9, 1965; (2) New York City blackout on July 13, 1977; (3) West Coast blackout on December 22, 1982; (4) West Coast blackout on July 2-3, 1996; (5) West Coast blackout on August 10, 1996; (6) Ontario and U.S. North Central blackout on June 25, 1998; and (7) Northeast outages and non-outage disturbances in the summer of 1999.

Outage Descriptions and Major Causal Factors

November 9, 1965: Northeast Blackout

This disturbance resulted in the loss of over 20,000 MW of load and affected 30 million people. Virtually all of New York, Connecticut, Massachusetts, Rhode Island, small segments of northern Pennsylvania and northeastern New Jersey, and substantial areas of Ontario, Canada, were affected. Outages lasted for up to 13 hours. This event resulted in the formation of the North American Electric Reliability Council in 1968.

A backup protective relay operated to open one of five 230-kV lines taking power north from a generating plant in Ontario to the Toronto area. When the flows redistributed instantaneously on the remaining four lines, they tripped out successively in a total of 2.5 seconds. The resultant power swings resulted in a cascading outage that blacked out much of the Northeast.

The major causal factors were as follows:

- Operation of a backup protective relay took a 230-kV line out of service when the loading on the line exceeded the 375-MW relay setting.
- Operating personnel were not aware of the operating set point of this relay.
- Another 230-kV line opened by an overcurrent relay action, and several 115- and 230-kV lines opened by protective relay action.
- Two key 345-kV east-west (Rochester-Syracuse) lines opened due to instability, and several lower voltage lines tripped open.
- Five of 16 generators at the St. Lawrence (Massena) plant tripped automatically in accordance with predetermined operating procedures.
- Following additional line tripouts, 10 generating units at Beck were automatically shut down by low governor oil pressure, and 5 pumping generators were tripped off by overspeed governor control.
- Several other lines then tripped out on under-frequency relay action.

July 13, 1977: New York City Blackout

This disturbance resulted in the loss of 6,000 MW of load and affected 9 million people in New York City. Outages lasted for up to 26 hours. A series of events triggering the separation of the Consolidated Edison system from neighboring systems and its subsequent collapse began when two 345-kV lines on a common tower in Northern Westchester were struck by lightning and tripped out. Over the next hour, despite Consolidated Edison dispatcher actions, the system electrically separated from surrounding systems and collapsed. With the loss of imports, generation in New York City was not sufficient to serve the load in the city.

Major causal factors were:

Table 7.1. Changing Conditions That Affect System Reliability

Previous Conditions	Emerging Conditions
Fewer, relatively large resources	Smaller, more numerous resources
Long-term, firm contracts	Contracts shorter in duration More non-firm transactions, fewer long-term firm transactions
Bulk power transactions relatively stable and predictable	Bulk power transactions relatively variable and less predictable
Assessment of system reliability made from stable base (narrower, more predictable range of potential operating states)	Assessment of system reliability made from variable base (wider, less predictable range of potential operating states)
Limited and knowledgable set of utility players	More players making more transactions, some with less interconnected operation experience; increasing with retail access
Unused transmission capacity and high security margins	High transmission utilization and operation closer to security limits
Limited competition, little incentive for reducing reliability investments	Utilities less willing to make investments in transmission reliability that do not increase revenues
Market rules and reliability rules developed together	Market rules undergoing transition, reliability rules developed separately
Limited wheeling	More system throughput

- Two 345-kV lines connecting Buchanan South to Millwood West experienced a phase B to ground fault caused by a lightning strike.
- Circuit breaker operations at the Buchanan South ring bus isolated the Indian Point No. 3 generating unit from any load, and the unit tripped for a rejection of 883 MW of load.
- Loss of the ring bus isolated the 345-kV tie to Ladentown, which had been importing 427 MW, making the cumulative resources lost 1,310 MW.
- 18.5 minutes after the first incident, an additional lightning strike caused the loss of two 345-kV lines, which connect Sprain Brook to Buchanan North and Sprain Brook to Millwood West. These two 345-kV lines share common towers between Millwood West and Sprain Brook. One line (Sprain Brook to Millwood West) automatically reclosed and was restored to service in about 2 seconds. The failure of the other line to reclose isolated the last Consolidated Edison interconnection to the Northwest.
- The resulting surge of power from the Northwest caused the loss of the Pleasant Valley to Millwood West line by relay action (a bent contact on one of the relays at Millwood West caused the improper action).
- 23 minutes later, the Leeds to Pleasant Valley 345-kV line sagged into a tree due to overload and tripped out.
- Within a minute, the 345 kV to 138 kV transformer at Pleasant Valley overloaded and tripped off, leaving Consolidated Edison with only three remaining interconnections.
- Within 3 minutes, the Long Island Lighting Co. system operator, on concurrence of the pool dispatcher, manually opened the Jamaica to Valley Stream tie.
- About 7 minutes later, the tap-changing mechanism failed on the Goethals phase-shifter, resulting in the loss of the Linden-to-Goethals tie to PJM, which was carrying 1,150 MW to Consolidated Edison.
- The two remaining external 138-kV ties to Consolidated Edison tripped on overload, isolating the Consolidated Edison system.
- Insufficient generation in the isolated system caused the Consolidated Edison island to collapse.

December 22, 1982: West Coast Blackout

This disturbance resulted in the loss of 12,350 MW of load and affected over 5 million people in the West. The outage began when high winds caused the failure of a 500-kV transmission tower. The tower fell into a parallel 500-kV line tower, and both lines were lost. The failure of these two lines mechanically cascaded and caused three additional towers to fail on each line. When the line conductors fell they contacted two 230-kV lines crossing under the 500-kV rights-of-way, collapsing the 230-kV lines.

The loss of the 500-kV lines activated a remedial action scheme to control the separation of the interconnection into two pre-engineered islands and trip generation in the Pacific Northwest in order to minimize customer outages and speed restoration. However, delayed operation of the remedial action scheme components occurred for several reasons, and the interconnection separated into four islands.

In addition to the mechanical failure of the transmission lines, analysis of this outage cited problems with coordination of protective schemes, because the generator tripping and separation schemes operated slowly or did not operate as planned. A communication channel component performed sporadically, resulting in delayed transmission of the control signal. The backup separation scheme also failed to operate, because the coordination of relay settings did not anticipate the power flows experienced in this severe disturbance.

In addition, the volume and format in which data were displayed to operators made it difficult to assess the extent of the disturbance and what corrective action should be taken. Time references to events in this disturbance were not tied to a common standard, making real-time evaluation of the situation more difficult.

July 2-3, 1996: West Coast Blackout

This disturbance resulted in the loss of 11,850 MW of load and affected 2 million people in the West. Customers were affected in Arizona, California, Colorado, Idaho, Montana, Nebraska, Nevada, New Mexico, Oregon, South Dakota, Texas, Utah, Washington, and Wyoming in the United States; Alberta and British Columbia in Canada; and Baja California Norte in Mexico. Outages lasted from a few minutes to several hours.

The outage began when a 345-kV transmission line in Idaho sagged into a tree and tripped out. A protective relay on a parallel transmission line also detected the fault and incorrectly tripped a second line. An almost simultaneous loss of these lines greatly reduced the ability of the system to transmit power from the nearby Jim Bridger plant. Other relays tripped two of the four generating units at that plant. With the loss of those two units, frequency in the entire Western Interconnection began to decline, and voltage began to collapse in the Boise, Idaho, area, affecting the California-Oregon AC Intertie transfer limit.

For 23 seconds the system remained in precarious balance, until the Mill Creek to Antelope 230-kV line between Montana and Idaho tripped by zone 3 relay, depressing voltage at Summer Lake Substation and causing the intertie to slip out of synchronism. Remedial action relays separated the system into five pre-engineered islands designed to minimize customer outages and restoration times. Similar conditions and initiating factors were present on July 3; however, as voltage began to collapse in the Boise area, the operator shed load manually and contained the disturbance.

August 10, 1996: West Coast Blackout

This disturbance resulted in the loss of over 28,000 MW of load and affected 7.5 million people in the West. Customers were affected in Arizona, California, Colorado, Idaho, Montana, Nebraska, Nevada, New Mexico, Oregon, South Dakota, Texas, Utah, Washington, and Wyoming in the United States; Alberta and British Columbia in Canada; and Baja California Norte in Mexico. Outages lasted from a few minutes to as long as nine hours.

Triggered by several major transmission line outages, the loss of generation from McNary Dam, and resulting system oscillations, the Western Interconnection separated into four electrical islands, with significant loss of load and generation. Prior to the disturbance, the transmission system from Canada south through the Northwest into California was heavily loaded with north-to-south power transfers. These flows were due to high Southwest demand caused by hot weather, combined with excellent hydroelectric conditions in Canada and the Northwest.

Very high temperatures in the Northwest caused two lightly loaded transmission lines to sag into untrimmed trees and trip out. A third heavily loaded line also sagged into a tree. Its outage led to the overload and loss of additional transmission lines. General voltage decline in the Northwest and the loss of McNary generation due to incorrectly applied relays caused power oscillations on the California to Oregon AC intertie. The intertie's protective relays tripped these facilities out and caused the Western Interconnection to separate into four islands. Following the loss of the first two lightly loaded lines, operators were unaware that the system was in an insecure state over the next hour, because new operating studies had not been performed to identify needed system adjustments.

June 25, 1998: Upper Midwest Blackout

This disturbance resulted in the loss of 950 MW of load and affected 152,000 people in Minnesota, Montana, North Dakota, South Dakota, and Wisconsin in the United States; and Ontario, Manitoba, and Saskatchewan in Canada. Outages lasted up to 19 hours.

A lightning storm in Minnesota initiated a series of events, causing a system disturbance that affected the entire Mid-Continent Area Power Pool (MAPP) Region and the northwestern Ontario Hydro system of the Northeast Power Coordinating Council. A 345-kV line was struck by lightning and tripped out. Underlying lower voltage lines began to overload and trip out, further weakening the system. Soon afterward, lightning struck a second 345-kV line, taking it out of service as well. Following the outage of the second 345-kV line, the remaining lower voltage transmission lines in the area became significantly overloaded, and relays took them out of service. This cascading removal of lines from service continued until the entire northern MAPP Region was separated from the Eastern Interconnection, forming three islands and resulting in the eventual blackout of the northwestern Ontario Hydro system.

Summer of 1999: Northeast U.S. Non-outage Disturbances

Load in the PJM system on July 6, 1999, was 51,600 MW (approximately 5,000 MW above forecast). PJM used all emergency procedures (including a 5% voltage reduction) except manually tripping load, and imported 5,000 MW from external systems to serve the record customer demand. Load on July 19, 1999, exceeded 50,500 MW. PJM loaded all available eastern PJM generation and again implemented emergency operating procedures from approximately 12 noon into the evening on both days.

During these record peak loads, steep voltage declines were experienced on the bulk transmission system. In each case, a voltage collapse was barely averted through the use of emergency procedures. Low voltage occurred because reactive demand exceeded reactive supply. High reactive demand was due to high electricity demand and high losses resulting from high transfers across the system. Reactive supply was inadequate because generators were unavailable or unable to meet rated reactive capability due to ambient conditions, and because some shunt capacitors were out of service.

Common or Similar Factors Among Major Outages

The factors that were common to some of the major outages above and the August 14 blackout include: (1) conductor contact with trees; (2) overestimation of dynamic reactive output of system generators; (3) inability of system operators or coordinators to visualize events on the entire system; (4) failure to ensure that system operation was within safe limits; (5) lack of coordination on system protection; (6) ineffective communication; (7) lack of "safety nets;" and (8) inadequate training of operating personnel. The following sections describe the nature of these factors and list recommendations from previous investigations that are relevant to each.

Conductor Contact With Trees

This factor was an initiating trigger in several of the outages and a contributing factor in the severity of several more. Unlike lightning strikes, for which system operators have fair storm-tracking tools, system operators generally do not have direct knowledge that a line has contacted a tree and faulted. They will sometimes test the line by trying to restore it to service, if that is deemed to be a safe operation. Even if it does go back into service, the line may fault and trip out again as load heats it up. This is most likely to happen when vegetation has not been adequately managed, in combination with hot and windless conditions.

In some of the disturbances, tree contact accounted for the loss of more than one circuit, contributing multiple contingencies to the weakening of the system. Lines usually sag into right-of-way obstructions when the need to retain transmission interconnection is high. High inductive load composition, such as air conditioning or irrigation pumping, accompanies hot weather and places higher burdens on transmission lines. Losing circuits contributes to voltage decline. Inductive load is unforgiving when voltage declines, drawing additional reactive supply from the system and further contributing to voltage problems.

Recommendations from previous investigations include:

- Paying special attention to the condition of rights-of-way following favorable growing seasons. Very wet and warm spring and summer growing conditions preceded the 1996 outages in the West.
- Careful review of any reduction in operations and maintenance expenses that may contribute to decreased frequency of line patrols or trimming. Maintenance in this area should be strongly directed toward preventive rather than remedial maintenance.

Dynamic Reactive Output of Generators

Reactive supply is an important ingredient in maintaining healthy power system voltages and facilitating power transfers. Inadequate reactive supply was a factor in most of the events. Shunt capacitors and generating resources are the most significant suppliers of reactive power. Operators perform contingency analysis based on how power system elements will perform under various power system conditions. They determine and set transfer limits based on these analyses. Shunt capacitors are easy to model because they are static. Modeling the dynamic reactive output of generators under stressed system conditions has proven to be more challenging. If the model is incorrect, estimated transfer limits will also be incorrect.

In most of the events, the assumed contribution of dynamic reactive output of system generators was greater than the generators actually produced, resulting in more significant voltage problems. Some generators were limited in the amount of reactive power they produced by over-excitation limits, or necessarily derated because of high ambient temperatures. Other generators were controlled to a fixed power factor and did not contribute reactive supply in depressed voltage conditions. Under-voltage load shedding is employed as an automatic remedial action in some interconnections to prevent cascading, and could be used more widely.

Recommendations from previous investigations concerning voltage support and reactive power management include:

- Communicate changes to generator reactive capability limits in a timely and accurate manner for both planning and operational modeling purposes.
- Investigate the development of a generator MVAr/voltage monitoring process to determine when generators may not be following reported MVAr limits.
- Establish a common standard for generator steady-state and post-contingency (15-minute) MVAr capability definition; determine methodology, testing, and operational reporting requirements.
- Determine the generator service level agreement that defines generator MVAr obligation to help ensure reliable operations.
- Periodically review and field test the reactive limits of generators to ensure that reported MVAr limits are attainable.
- Provide operators with on-line indications of available reactive capability from each generating unit or groups of generators, other VAr sources, and the reactive margin at all critical buses. This information should assist in the operating practice of maximizing the use of shunt capacitors during heavy transfers and thereby increase the availability of system dynamic reactive reserve.
- For voltage instability problems, consider fast automatic capacitor insertion (both series and shunt), direct shunt reactor and load tripping, and under-voltage load shedding.
- Develop and periodically review a reactive margin against which system performance should be evaluated and used to establish maximum transfer levels.

System Visibility Procedures and Operator Tools

Each control area operates as part of a single synchronous interconnection. However, the parties with various geographic or functional responsibilities for reliable operation of the grid do not have visibility of the entire system. Events in neighboring systems may not be visible to an operator or reliability coordinator, or power system data may be available in a control center but not be presented to operators or coordinators as information they can use in making appropriate operating decisions.

Recommendations from previous investigations concerning visibility and tools include:

- Develop communications systems and displays that give operators immediate information on changes in the status of major components in their own and neighboring systems.
- Supply communications systems with uninterruptible power, so that information on system conditions can be transmitted correctly to control centers during system disturbances.
- In the control center, use a dynamic line loading and outage display board to provide operating personnel with rapid and comprehensive information about the facilities available and the operating condition of each facility in service.
- Give control centers the capability to display to system operators computer-generated alternative actions specific to the immediate situation, together with expected results of each action.
- Establish on-line security analysis capability to identify those next and multiple facility outages that would be critical to system reliability from thermal, stability, and post-contingency voltage points of view.
- Establish time-synchronized disturbance monitoring to help evaluate the performance of the interconnected system under stress, and design appropriate controls to protect it.

System Operation Within Safe Limits

Operators in several of the events were unaware of the vulnerability of the system to the next contingency. The reasons were varied: inaccurate modeling for simulation, no visibility of the loss of key transmission elements, no operator monitoring of stability measures (reactive reserve monitor, power transfer angle), and no reassessment of system conditions following the loss of an element and readjustment of safe limits.

Recommendations from previous investigations include:

- Following a contingency, the system must be returned to a reliable state within the allowed readjustment period. Operating guides must be reviewed to ensure that procedures exist to restore system reliability in the allowable time periods.

- Reduce scheduled transfers to a safe and prudent level until studies have been conducted to determine the maximum simultaneous transfer capability limits.
- Reevaluate processes for identifying unusual operating conditions and potential disturbance scenarios, and make sure they are studied before they are encountered in real-time operating conditions.

Coordination of System Protection (Transmission and Generation Elements)

Protective relays are designed to detect short circuits and act locally to isolate faulted power system equipment from the system—both to protect the equipment from damage and to protect the system from faulty equipment. Relay systems are applied with redundancy in primary and backup modes. If one relay fails, another should detect the fault and trip appropriate circuit breakers. Some backup relays have significant "reach," such that non-faulted line overloads or stable swings may be seen as faults and cause the tripping of a line when it is not advantageous to do so. Proper coordination of the many relay devices in an interconnected system is a significant challenge, requiring continual review and revision. Some relays can prevent resynchronizing, making restoration more difficult.

System-wide controls protect the interconnected operation rather than specific pieces of equipment. Examples include controlled islanding to mitigate the severity of an inevitable disturbance and under-voltage or under-frequency load shedding. Failure to operate (or misoperation of) one or more relays as an event developed was a common factor in several of the disturbances.

Recommendations developed after previous outages include:

- Perform system trip tests of relay schemes periodically. At installation the acceptance test should be performed on the complete relay scheme in addition to each individual component so that the adequacy of the scheme is verified.
- Continually update relay protection to fit changing system development and to incorporate improved relay control devices.
- Install sensing devices on critical transmission lines to shed load or generation automatically if the short-term emergency rating is exceeded for a specified period of time. The time delay should be long enough to allow the system operator to attempt to reduce line loadings promptly by other means.
- Review phase-angle restrictions that can prevent reclosing of major interconnections during system emergencies. Consideration should be given to bypassing synchronism-check relays to permit direct closing of critical interconnections when it is necessary to maintain stability of the grid during an emergency.
- Review the need for controlled islanding. Operating guides should address the potential for significant generation/load imbalance within the islands.

Effectiveness of Communications

Under normal conditions, parties with reliability responsibility need to communicate important and prioritized information to each other in a timely way, to help preserve the integrity of the grid. This is especially important in emergencies. During emergencies, operators should be relieved of duties unrelated to preserving the grid. A common factor in several of the events described above was that information about outages occurring in one system was not provided to neighboring systems.

Need for Safety Nets

A safety net is a protective scheme that activates automatically if a pre-specified, significant contingency occurs. When activated, such schemes involve certain costs and inconvenience, but they can prevent some disturbances from getting out of control. These plans involve actions such as shedding load, dropping generation, or islanding, and in all cases the intent is to have a controlled outcome that is less severe than the likely uncontrolled outcome. If a safety net had not been taken out of service in the West in August 1996, it would have lessened the severity of the disturbance from 28,000 MW of load lost to less than 7,200 MW. (It has since been returned to service.) Safety nets should not be relied upon to establish transfer limits, however.

Previous recommendations concerning safety nets include:

- Establish and maintain coordinated programs of automatic load shedding in areas not so equipped, in order to prevent total loss of power in an area that has been separated from the

main network and is deficient in generation. Load shedding should be regarded as an insurance program, however, and should not be used as a substitute for adequate system design.

- Install load-shedding controls to allow fast single-action activation of large-block load shedding by an operator.

Training of Operating Personnel

Operating procedures were necessary but not sufficient to deal with severe power system disturbances in several of the events. Enhanced procedures and training for operating personnel were recommended. Dispatcher training facility scenarios with disturbance simulation were suggested as well. Operators tended to reduce schedules for transactions but were reluctant to call for increased generation—or especially to shed load—in the face of a disturbance that threatened to bring the whole system down.

Previous recommendations concerning training include:

- Thorough programs and schedules for operator training and retraining should be vigorously administered.
- A full-scale simulator should be made available to provide operating personnel with "hands-on" experience in dealing with possible emergency or other system conditions.
- Procedures and training programs for system operators should include anticipation, recognition, and definition of emergency situations.
- Written procedures and training materials should include criteria that system operators can use to recognize signs of system stress and mitigating measures to be taken before conditions degrade into emergencies.
- Line loading relief procedures should not be relied upon when the system is in an insecure state, as these procedures cannot be implemented effectively within the required time frames in many cases. Other readjustments must be used, and the system operator must take responsibility to restore the system immediately.
- Operators' authority and responsibility to take immediate action if they sense the system is starting to degrade should be emphasized and protected.
- The current processes for assessing the potential for voltage instability and the need to enhance the existing operator training programs, operational tools, and annual technical assessments should be reviewed to improve the ability to predict future voltage stability problems prior to their occurrence, and to mitigate the potential for adverse effects on a regional scale.

Comparisons With the August 14 Blackout

The blackout on August 14, 2003, had several causes or contributory factors in common with the earlier outages, including:

- Inadequate vegetation management
- Failure to ensure operation within secure limits
- Failure to identify emergency conditions and communicate that status to neighboring systems
- Inadequate operator training
- Inadequate regional-scale visibility over the power system
- Inadequate coordination of relays and other protective devices or systems.

New causal features of the August 14 blackout include: inadequate interregional visibility over the power system; dysfunction of a control area's SCADA/EMS system; and lack of adequate backup capability to that system.

8. Performance of Nuclear Power Plants Affected by the Blackout

Introduction

On August 14, 2003, nine U.S. nuclear power plants experienced rapid shutdowns (reactor trips) as a consequence of the power outage. Seven nuclear power plants in Canada operating at high power levels at the time of the event also experienced rapid shutdowns. Four other Canadian nuclear plants automatically disconnected from the grid due to the electrical transient but were able to continue operating at a reduced power level and were available to supply power to the grid as it was restored by the transmission system operators. Six nuclear plants in the United States and one in Canada experienced significant electrical disturbances but were able to continue generating electricity. Many non-nuclear generating plants in both countries also tripped during the event. Numerous other nuclear plants observed disturbances on the electrical grid but continued to generate electrical power without interruption.

The Nuclear Working Group (NWG) was one of three Working Groups created to support the U.S.-Canada Power System Outage Task Force. The NWG was charged with identifying all relevant actions by nuclear generating facilities in connection with the outage. Nils Diaz, Chairman of the U.S. Nuclear Regulatory Commission (NRC) and Linda Keen, President and CEO of the Canadian Nuclear Safety Commission (CNSC) were co-chairs of the Working Group, with other members appointed from industry and various State and federal agencies.

In Phase I, the NWG focused on collecting and analyzing data from each affected nuclear power plant to determine what happened, and whether any activities at the plants caused or contributed to the power outage or involved a significant safety issue. Phase I culminated in the issuance of the Task Force's *Interim Report*, which reported that:

- The affected nuclear power plants did not trigger the power outage or inappropriately contribute to its spread (i.e., to an extent beyond the normal tripping of the plants at expected conditions).
- The severity of the grid transient caused generators, turbines, or reactor systems at the nuclear plants to reach protective feature limits and actuate automatic protective actions.
- The nuclear plants responded to the grid conditions in a manner consistent with the plant designs.
- The nuclear plants were maintained in a safe condition until conditions were met to permit the nuclear plants to resume supplying electrical power to the grid.
- **For nuclear plants in the United States:**
  - Fermi 2, Oyster Creek, and Perry tripped due to main generator trips, which resulted from voltage and frequency fluctuations on the grid. Nine Mile 1 tripped due to a main turbine trip due to frequency fluctuations on the grid.
  - FitzPatrick and Nine Mile 2 tripped due to reactor trips, which resulted from turbine control system low pressure due to frequency fluctuations on the grid. Ginna tripped due to a reactor trip which resulted from a large loss of electrical load due to frequency fluctuations on the grid. Indian Point 2 and Indian Point 3 tripped due to a reactor trip on low flow, which resulted when low grid frequency tripped reactor coolant pumps.
- **For nuclear plants in Canada:**
  - At Bruce B and Pickering B, frequency and/or voltage fluctuations on the grid resulted in the automatic disconnection of generators from the grid. For those units that were successful in maintaining the unit generators operational, reactor power was automatically reduced.

- At Darlington, load swing on the grid led to the automatic reduction in power of the four reactors. The generators were, in turn, automatically disconnected from the grid.
- Three reactors at Bruce B and one at Darlington were returned to 60% power. These reactors were available to deliver power to the grid on the instructions of the transmission system operator.
- Three units at Darlington were placed in a zero-power hot state, and four units at Pickering B and one unit at Bruce B were placed in a Guaranteed Shutdown State.

The licensees' return to power operation followed a deliberate process controlled by plant procedures and regulations. Equipment and process problems, whether existing prior to or caused by the event, would normally be addressed prior to restart. The NWG is satisfied that licensees took an appropriately conservative approach to their restart activities, placing a priority on safety.

- **For U.S. nuclear plants:** Ginna, Indian Point 2, Nine Mile 2, and Oyster Creek resumed electrical generation on August 17. FitzPatrick and Nine Mile 1 resumed electrical generation on August 18. Fermi 2 resumed electrical generation on August 20. Perry resumed electrical generation on August 21. Indian Point 3 resumed electrical generation on August 22. Indian Point 3 had equipment issues (failed splices in the control rod drive mechanism power system) that required repair prior to restart. Ginna submitted a special request for enforcement discretion from the NRC to permit mode changes and restart with an inoperable auxiliary feedwater pump. The NRC granted the request for enforcement discretion.
- **For Canadian nuclear plants:** The restart of the Canadian nuclear plants was carried out in accordance with approved Operating Policies and Principles. Three units at Bruce B and one at Darlington were resynchronized with the grid within 6 hours of the event. The remaining three units at Darlington were reconnected by August 17 and 18. Units 5, 6, and 8 at Pickering B and Unit 6 at Bruce B returned to service between August 22 and August 25.

The NWG has found no evidence that the shutdown of the nuclear power plants triggered the outage or inappropriately contributed to its spread (i.e., to an extent beyond the normal tripping of the plants at expected conditions). All the nuclear plants that shut down or disconnected from the grid responded automatically to grid conditions. All the nuclear plants responded in a manner consistent with the plant designs. Safety functions were effectively accomplished, and the nuclear plants that tripped were maintained in a safe shutdown condition until their restart.

In Phase II, the NWG collected comments and analyzed information related to potential recommendations to help prevent future power outages. Representatives of the NWG, including representatives of the NRC and the CNSC, attended public meetings to solicit feedback and recommendations held in Cleveland, Ohio; New York City, New York; and Toronto, Ontario, on December 4, 5, and 8, 2003, respectively. Representatives of the NWG also participated in the NRC's public meeting to solicit feedback and recommendations on the Northeast blackout held in Rockville, Maryland, on January 6, 2004.

Additional details on both the Phase I and Phase II efforts are available in the following sections. Due to the major design differences between nuclear plants in Canada and the United States, the NWG decided to have separate sections for each country. This also responds to the request by the nuclear regulatory agencies in both countries to have sections of the report that stand alone, so that they can also be used as regulatory documents.

Findings of the U.S. Nuclear Working Group

Summary

The U.S. NWG found no evidence that the shutdown of the nine U.S. nuclear power plants triggered the outage, or inappropriately contributed to its spread (i.e., to an extent beyond the normal tripping of the plants at expected conditions). All nine plants that experienced a reactor trip were responding to grid conditions. The severity of the grid transient caused generators, turbines, or reactor systems at the plants to reach a protective feature limit and actuate a plant shutdown. All nine plants tripped in response to those conditions in a manner consistent with the plant designs. The nine plants automatically shut down in a safe fashion to protect the plants from the grid transient. Safety functions were effectively accomplished with few problems, and the plants were maintained in a safe shutdown condition until their restart.

The nuclear power plant outages that resulted from the August 14, 2003, power outage were triggered by automatic protection systems for the reactors or turbine-generators, not by any manual operator actions. The NWG has received no information that points to operators deliberately shutting down nuclear units to isolate themselves from instabilities on the grid. In short, only automatic separation of nuclear units occurred.

Regarding the 95 other licensed commercial nuclear power plants in the United States: 4 were already shut down at the time of the power outage, one of which experienced a grid disturbance; 70 operating plants observed some level of grid disturbance but accommodated the disturbances and remained on line, supplying power to the grid; and 21 operating plants did not experience any grid disturbance.

Introduction

The NRC, which regulates U.S. commercial nuclear power plants, has regulatory requirements for offsite power systems. These requirements address the number of offsite power sources and the ability to withstand certain transients. Offsite power is the normal source of alternating current (AC) power to the safety systems in the plants when the plant main generator is not in operation. The requirements also are designed to protect safety systems from potentially damaging variations (in voltage and frequency) in the supplied power. For loss of offsite power events, the NRC requires emergency generation (typically emergency diesel generators) to provide AC power to safety systems. In addition, the NRC provides oversight of the safety aspects of offsite power issues through its inspection program, by monitoring operating experience, and by performing technical studies.

Phase I: Fact Finding

Phase I of the NWG effort focused on collecting and analyzing data from each plant to determine what happened, and whether any activities at the plants caused or contributed to the power outage or its spread or involved a significant safety issue. To ensure accuracy, comprehensive coordination was maintained among the working group members and among the NWG, ESWG, and SWG.

The staff developed a set of technical questions to obtain data from the owners or licensees of the nuclear power plants that would enable them to review the response of the nuclear plant systems in detail. Two additional requests for more specific information were made for certain plants. The collection of information from U.S. nuclear power plants was gathered through the NRC regional offices, which had NRC resident inspectors at each plant obtain licensee information to answer the questions. General design information was gathered from plant-specific Updated Final Safety Analysis Reports and other documents.

Plant data were compared against plant designs by the NRC staff to determine whether the plant responses were as expected; whether they appeared to cause the power outage or contributed to the spread of the outage; and whether applicable safety requirements were met. In some cases supplemental questions were developed, and answers were obtained from the licensees to clarify the observed response of the plant. The NWG interfaced with the ESWG to validate some data and to obtain grid information, which contributed to the analysis. The NWG identified relevant actions by nuclear generating facilities in connection with the power outage.

Typical Design, Operational, and Protective Features of U.S. Nuclear Power Plants

Nuclear power plants have a number of design, operational, and protective features to ensure that the plants operate safely and reliably. This section describes these features so as to provide a better understanding of how nuclear power plants interact with the grid and, specifically, how nuclear power plants respond to changing grid conditions. While the features described in this section are typical, there are differences in the design and operation of individual plants which are not discussed.

Design Features of U.S. Nuclear Power Plants

Nuclear power plants use heat from nuclear reactions to generate steam and use a single steam-driven turbine-generator (also known as the main generator) to produce electricity supplied to the grid.

Connection of the plant switchyard to the grid. The plant switchyard normally forms the interface between the plant main generator and the electrical grid. The plant switchyard has multiple transmission lines connected to the grid system to meet offsite power supply requirements for having reliable offsite power for the nuclear station under all operating and shutdown conditions. Each

transmission line connected to the switchyard has dedicated circuit breakers, with fault sensors, to isolate faulted conditions in the switchyard or the connected transmission lines, such as phase-to-phase or phase-to-ground short circuits. The fault sensors are fed into a protection scheme for the plant switchyard that is engineered to localize any faulted conditions with minimum system disturbance.

Connection of the main generator to the switchyard. The plant main generator produces electrical power and transmits that power to the offsite transmission system. Most plants also supply power to the plant auxiliary buses for normal operation of the nuclear generating unit through the unit auxiliary transformer. During normal plant operation, the main generator typically generates electrical power at about 22 kV. The voltage is increased to match the switchyard voltage by the main transformers, and the power flows to the high voltage switchyard through two power circuit breakers.

Power supplies for the plant auxiliary buses. The safety-related and nonsafety auxiliary buses are normally lined up to receive power from the main generator auxiliary transformer, although some plants leave some of their auxiliary buses powered from a startup transformer (that is, from the offsite power distribution system). When plant power generation is interrupted, the power supply automatically transfers to the offsite power source (the startup transformer). If that is not supplying acceptable voltage, the circuit breakers to the safety-related buses open, and the buses are reenergized by the respective fast-starting emergency diesel generators. The nonsafety auxiliary buses will remain deenergized until offsite power is restored.

Operational Features of U.S. Nuclear Power Plants

Response of nuclear power plants to changes in switchyard voltage. With the main generator voltage regulator in the automatic mode, the generator will respond to an increase of switchyard voltage by reducing the generator field excitation current. This will result in a decrease of reactive power, normally measured as mega-volts-amperes-reactive (MVAr) from the generator to the switchyard and out to the surrounding grid, helping to control the grid voltage increase. With the main generator voltage regulator in the automatic mode, the generator will respond to a decrease of switchyard voltage by increasing the generator field excitation current. This will result in an increase of reactive power (MVAr) from the generator to the switchyard and out to the surrounding grid, helping to control the grid voltage decrease. If the switchyard voltage goes low enough, the increased generator field current could result in generator field overheating. Over-excitation protective circuitry is generally employed to prevent this from occurring. This protective circuitry may trip the generator to prevent equipment damage.

Under-voltage protection is provided for the nuclear power plant safety buses, and may be provided on nonsafety buses and at individual pieces of equipment. It is also used in some pressurized water reactor designs on reactor coolant pumps (RCPs) as an anticipatory loss of RCP flow signal.

Protective Features of U.S. Nuclear Power Plants

The main generator and main turbine have protective features, similar to fossil generating stations, which protect against equipment damage. In general, the reactor protective features are designed to protect the reactor fuel from damage and to protect the reactor coolant system from over-pressure or over-temperature transients. Some trip features also produce a corresponding trip in other components; for example, a turbine trip typically results in a reactor trip above a low power setpoint.

Generator protective features typically include over-current, ground detection, differential relays (which monitor for electrical fault conditions within a zone of protection defined by the location of the sensors, typically the main generator and all transformers connected directly to the generator output), electrical faults on the transformers connected to the generator, loss of the generator field, and a turbine trip. Turbine protective features typically include over-speed (usually set at 1980 rpm or 66 Hz), low bearing oil pressure, high bearing vibration, degraded condenser vacuum, thrust bearing failure, or generator trip. Reactor protective features typically include trips for over-power, abnormal pressure in the reactor coolant system, low reactor coolant system flow, low level in the steam generators or the reactor vessel, or a trip of the turbine.

Considerations on Returning a U.S. Nuclear Power Plant to Power Production After Switchyard Voltage Is Restored

The following are examples of the types of activities that must be completed before returning a

nuclear power plant to power production following a loss of switchyard voltage.

- Switchyard voltage must be normal and stable from an offsite supply. Nuclear power plants are not designed for black-start capability (the ability to start up without external power).
- Plant buses must be energized from the switchyard and the emergency diesel generators restored to standby mode.
- Normal plant equipment, such as reactor coolant pumps and circulating water pumps, must be restarted.
- A reactor trip review report must be completed and approved by plant management, and the cause of the trip must be addressed.
- All plant technical specifications must be satisfied. Technical specifications are issued to each nuclear power plant as part of their license by the NRC. They dictate equipment which must be operable and process parameters which must be met to allow operation of the reactor. Examples of actions that were required following the events of August 14 include refilling the diesel fuel oil storage tanks, refilling the condensate storage tanks, establishing reactor coolant system forced flow, and cooling the suppression pool to normal operating limits. Surveillance tests must be completed as required by technical specifications (for example, operability of the low-range neutron detectors must be demonstrated).
- Systems must be aligned to support the startup.
- Pressures and temperatures for reactor startup must be established in the reactor coolant system for pressurized water reactors.
- A reactor criticality calculation must be performed to predict the control rod withdrawals needed to achieve criticality, where the fission chain reaction becomes self-sustaining due to the increased neutron flux. Certain neutron-absorbing fission products increase in concentration following a reactor trip (followed later by a decrease or decay). At pressurized water reactors, the boron concentration in the primary coolant must be adjusted to match the criticality calculation. Near the end of the fuel cycle, the nuclear power plant may not have enough boron adjustment or control rod worth available for restart until the neutron absorbers have decreased significantly (more than 24 hours after the trip).

It may require a day or more before a nuclear power plant can restart following a normal trip. Plant trips are a significant transient on plant equipment, and some maintenance may be necessary before the plant can restart. When combined with the infrequent event of loss of offsite power, additional recovery actions will be required. Safety systems, such as emergency diesel generators and safety-related decay heat removal systems, must be restored to normal lineups. These additional actions would extend the time necessary to restart a nuclear plant from this type of event.

Summary of U.S. Nuclear Power Plant Response to and Safety During the August 14 Outage

The NWG's review did not identify any activity or equipment issues at U.S. nuclear power plants that caused the transient on August 14, 2003. Nine nuclear power plants tripped within about 60 seconds as a result of the grid disturbance. Additionally, many nuclear power plants experienced a transient due to this grid disturbance.

Nuclear Power Plants That Tripped

The trips at nine nuclear power plants resulted from the plant responses to the grid disturbances. Following the initial grid disturbances, voltages in the plant switchyard fluctuated and reactive power flows fluctuated. As the voltage regulators on the main generators attempted to compensate, equipment limits were exceeded and protective trips resulted. This happened at Fermi 2 and Oyster Creek. Fermi 2 tripped on a generator field protection trip. Oyster Creek tripped due to a generator trip on high ratio of voltage relative to the electrical frequency.

Also, as the balance between electrical generation and electrical load on the grid was disturbed, the electrical frequency began to fluctuate. In some cases the electrical frequency dropped low enough to actuate protective features. This happened at Indian Point 2, Indian Point 3, and Perry. Perry tripped due to a generator under-frequency trip signal. Indian Point 2 and Indian Point 3 tripped when the grid frequency dropped low enough to trip reactor coolant pumps, which actuated a reactor protective feature.

In other cases, the electrical frequency fluctuated and went higher than normal. Turbine control systems responded in an attempt to control the frequency. Equipment limits were exceeded as a result of the reaction of the turbine control systems to large frequency changes. This led to trips at FitzPatrick, Nine Mile 1, Nine Mile 2, and Ginna. FitzPatrick and Nine Mile 2 tripped on low pressure in the turbine hydraulic control oil system. Nine Mile 1 tripped on turbine light load protection. Ginna tripped due to conditions in the reactor following rapid closure of the turbine control valves in response to high frequency on the grid.

The Perry, Fermi 2, Oyster Creek, and Nine Mile 1 reactors tripped immediately after the generator tripped, although that is not apparent from the times below, because the clocks were not synchronized to the national time standard. The Indian Point 2 and 3, FitzPatrick, Ginna, and Nine Mile 2 reactors tripped before the generators. When the reactor trips first, there is generally a short time delay before the generator output breakers open. The electrical generation decreases rapidly to zero after the reactor trip. Table 8.1 provides the times from the data collected for the reactor trip times, and the time the generator output breakers opened (generator trip), as reported by the ESWG. Additional details on the plants that tripped are given below, and summarized in Table 8.2 on page 120.

Fermi 2. Fermi 2 is located 25 miles (40 km) northeast of Toledo, Ohio, in southern Michigan on Lake Erie. It was generating about 1,130 megawatts-electric (MWe) before the event. The reactor tripped due to a turbine trip. The turbine trip was likely the result of multiple generator field protection trips (overexcitation and loss of field) as the Fermi 2 generator responded to a series of rapidly changing transients prior to its loss. This is consistent with data that shows large swings of the Fermi 2 generator MVAr prior to its trip.

Offsite power was subsequently lost to the plant auxiliary buses. The safety buses were deenergized and automatically reenergized from the emergency diesel generators. The operators tripped one emergency diesel generator that was paralleled to the grid for testing, after which it automatically loaded. Decay heat removal systems maintained the cooling function for the reactor fuel.

The lowest emergency declaration, an Unusual Event, was declared at about 16:22 EDT due to the loss of offsite power. Offsite power was restored to at least one safety bus at about 01:53 EDT on August 15. The following equipment problems were noted: the Combustion Turbine Generator (the alternate AC power source) failed to start from the control room; however, it was successfully started locally. In addition, the Spent Fuel Pool Cooling System was interrupted for approximately 26 hours and reached a maximum temperature of 130 degrees Fahrenheit (55 degrees Celsius). The main generator was reconnected to the grid at about 01:41 EDT on August 20.

FitzPatrick. FitzPatrick is located about 8 miles (13 km) northeast of Oswego, NY, in northern New York on Lake Ontario. It was generating about 850 MWe before the event. The reactor tripped due to low pressure in the hydraulic system that controls the turbine control valves. Low pressure in this system typically indicates a large load reject, for which a reactor trip is expected. In this case the pressure in the system was low because the control system was rapidly manipulating the turbine control valves to control turbine speed, which was being affected by grid frequency fluctuations.

Immediately preceding the trip, both significant over-voltage and under-voltage grid conditions were experienced. Offsite power was subsequently lost to the plant auxiliary buses. The safety buses were deenergized and automatically reenergized from the emergency diesel generators.

The lowest emergency declaration, an Unusual Event, was declared at about 16:26 EDT due to the loss of offsite power. Decay heat removal systems maintained the cooling function for the reactor fuel. Offsite power was restored to at least one safety bus at about 23:07 EDT on August 14. The main generator was reconnected to the grid at about 06:10 EDT on August 18.

Table 8.1. U.S. Nuclear Plant Trip Times

Nuclear Plant	Reactor Trip[a]	Generator Trip[b]
Perry	16:10:25 EDT	16:10:42 EDT
Fermi 2	16:10:53 EDT	16:10:53 EDT
Oyster Creek . . .	16:10:58 EDT	16:10:57 EDT
Nine Mile 1	16:11 EDT	16:11:04 EDT
Indian Point 2 . .	16:11 EDT	16:11:09 EDT
Indian Point 3 . .	16:11 EDT	16:11:23 EDT
FitzPatrick	16:11:04 EDT	16:11:32 EDT
Ginna.	16:11:36 EDT	16:12:17 EDT
Nine Mile 2	16:11:48 EDT	16:11:52 EDT

[a]As determined from licensee data (which may not be synchronized to the national time standard).
[b]As reported by the Electrical System Working Group (synchronized to the national time standard).

Ginna. Ginna is located 20 miles (32 km) northeast of Rochester, NY, in northern New York on Lake Ontario. It was generating about 487 MWe before the event. The reactor tripped due to Over-Temperature-Delta-Temperature. This trip signal protects the reactor core from exceeding temperature limits. The turbine control valves closed down in response to the changing grid conditions. This caused a temperature and pressure transient in the reactor, resulting in an Over-Temperature-Delta-Temperature trip.

Offsite power was not lost to the plant auxiliary buses. In the operators' judgement, offsite power was not stable, so they conservatively energized the safety buses from the emergency diesel generators. Decay heat removal systems maintained the cooling function for the reactor fuel. Offsite power was not lost, and stabilized about 50 minutes after the reactor trip.

The lowest emergency declaration, an Unusual Event, was declared at about 16:46 EDT due to the degraded offsite power. Offsite power was restored to at least one safety bus at about 21:08 EDT on August 14. The following equipment problems were noted: the digital feedwater control system behaved in an unexpected manner following the trip, resulting in high steam generator levels; there was a loss of RCP seal flow indication, which complicated restarting the pumps; and at least one of the power-operated relief valves experienced minor leakage following proper operation and closure during the transient. Also, one of the motor-driven auxiliary feedwater pumps was damaged after running with low flow conditions due to an improper valve alignment. The redundant pumps supplied the required water flow.

The NRC issued a Notice of Enforcement Discretion to allow Ginna to perform mode changes and restart the reactor with one auxiliary feedwater (AFW) pump inoperable. Ginna has two AFW pumps, one turbine-driven AFW pump, and two standby AFW pumps, all powered from safety-related buses. The main generator was reconnected to the grid at about 20:38 EDT on August 17.

Indian Point 2. Indian Point 2 is located 24 miles (39 km) north of New York City on the Hudson River. It was generating about 990 MWe before the event. The reactor tripped due to loss of a reactor coolant pump that tripped because the auxiliary bus frequency fluctuations actuated the under-frequency relay, which protects against inadequate coolant flow through the reactor core. This reactor protection signal tripped the reactor, which resulted in turbine and generator trips.

The auxiliary bus experienced the under-frequency due to fluctuating grid conditions. Offsite power was lost to all the plant auxiliary buses. The safety buses were reenergized from the emergency diesel generators. Decay heat removal systems maintained the cooling function for the reactor fuel.

The lowest emergency declaration, an Unusual Event, was declared at about 16:25 EDT due to the loss of offsite power for more than 15 minutes. Offsite power was restored to at least one safety bus at about 20:02 EDT on August 14. The following equipment problems were noted: the service water to one of the emergency diesel generators developed a leak; a steam generator atmospheric dump valve did not control steam generator pressure in automatic and had to be shifted to manual; a steam trap associated with the turbine-driven AFW pump failed open, resulting in operators securing the turbine after 2.5 hours; loss of instrument air required operators to take manual control of charging and a letdown isolation occurred; and operators in the field could not use radios; and the diesel generator for the Unit 2 Technical Support Center failed to function. Also, several uninterruptible power supplies in the Emergency Operations Facility failed. This reduced the capability for communications and data collection. Alternate equipment was used to maintain vital communications.[1] The main generator was reconnected to the grid at about 12:58 EDT on August 17.

Indian Point 3. Indian Point 3 is located 24 miles (39 km) north of New York City on the Hudson River. It was generating about 1,010 MWe before the event. The reactor tripped due to loss of a reactor coolant pump that tripped because the auxiliary bus frequency fluctuations actuated the under-frequency relay, which protects against inadequate coolant flow through the reactor core. This reactor protection signal tripped the reactor, which resulted in turbine and generator trips.

The auxiliary bus experienced the under-frequency due to fluctuating grid conditions. Offsite power was lost to all the plant auxiliary buses. The safety buses were reenergized from the emergency diesel generators. Decay heat removal systems maintained the cooling function for the reactor fuel.

The lowest emergency declaration, an Unusual Event, was declared at about 16:23 EDT due to the

loss of offsite power for more than 15 minutes. Offsite power was restored to at least one safety bus at about 20:12 EDT on August 14. The following equipment problems were noted: a steam generator safety valve lifted below its desired setpoint and was gagged; loss of instrument air, including failure of the diesel backup compressor to start and failure of the backup nitrogen system, resulted in manual control of atmospheric dump valves and AFW pumps needing to be secured to prevent overfeeding the steam generators; a blown fuse in a battery charger resulted in a longer battery discharge; a control rod drive mechanism cable splice failed, and there were high resistance readings on 345-kV breaker-1. These equipment problems required correction prior to startup, which delayed the startup. The diesel generator for the Unit 3 Technical Support Center failed to function. Also, several uninterruptible power supplies in the Emergency Operations Facility failed. This reduced the capability for communications and data collection. Alternate equipment was used to maintain vital communications.[2] The main generator was reconnected to the grid at about 05:03 EDT on August 22.

Nine Mile 1. Nine Mile 1 is located 6 miles (10 km) northeast of Oswego, NY, in northern New York on Lake Ontario. It was generating about 600 MWe before the event. The reactor tripped in response to a turbine trip. The turbine tripped on light load protection (which protects the turbine against a loss of electrical load), when responding to fluctuating grid conditions. The turbine trip caused fast closure of the turbine valves, which, through acceleration relays on the control valves, create a signal to trip the reactor. After a time delay of 10 seconds, the generator tripped on reverse power.

The safety buses were automatically deenergized due to low voltage and automatically reenergized from the emergency diesel generators. Decay heat removal systems maintained the cooling function for the reactor fuel.

The lowest emergency declaration, an Unusual Event, was declared at about 16:33 EDT due to the degraded offsite power. Offsite power was restored to at least one safety bus at about 23:39 EDT on August 14. The following additional equipment problems were noted: a feedwater block valve failed "as is" on the loss of voltage, resulting in a high reactor vessel level; fuses blew in fire circuits, causing control room ventilation isolation and fire panel alarms; and operators were delayed in placing shutdown cooling in service for several hours due to lack of procedure guidance to address particular plant conditions encountered during the shutdown. The main generator was reconnected to the grid at about 02:08 EDT on August 18.

Nine Mile 2. Nine Mile 2 is located 6 miles (10 km) northeast of Oswego, NY, in northern New York on Lake Ontario. It was generating about 1,193 MWe before the event. The reactor scrammed due to the actuation of pressure switches which detected low pressure in the hydraulic system that controls the turbine control valves. Low pressure in this system typically indicates a large load reject, for which a reactor trip is expected. In this case the pressure in the system was low because the control system was rapidly manipulating the turbine control valves to control turbine speed, which was being affected by grid frequency fluctuations.

After the reactor tripped, several reactor level control valves did not reposition, and with the main feedwater system continuing to operate, a high water level in the reactor caused a turbine trip, which caused a generator trip. Offsite power was degraded but available to the plant auxiliary buses. The offsite power dropped below the normal voltage levels, which resulted in the safety buses being automatically energized from the emergency diesel generators. Decay heat removal systems maintained the cooling function for the reactor fuel.

The lowest emergency declaration, an Unusual Event, was declared at about 17:00 EDT due to the loss of offsite power to the safety buses for more than 15 minutes. Offsite power was restored to at least one safety bus at about 01:33 EDT on August 15. The following additional equipment problem was noted: a tap changer on one of the offsite power transformers failed, complicating the restoration of one division of offsite power. The main generator was reconnected to the grid at about 19:34 EDT on August 17.

Oyster Creek. Oyster Creek is located 9 miles (14 km) south of Toms River, NJ, near the Atlantic Ocean. It was generating about 629 MWe before the event. The reactor tripped due to a turbine trip. The turbine trip was the result of a generator trip due to actuation of a high Volts/Hz protective trip. The Volts/Hz trip is a generator/transformer protective feature. The plant safety and auxiliary buses transferred from the main generator supply to the offsite power supply following the plant trip. Other than the plant transient, no equipment

or performance problems were determined to be directly related to the grid problems.

Post-trip the operators did not get the mode switch to shutdown before main steam header pressure reached its isolation setpoint. The resulting MSIV closure complicated the operator's response because the normal steam path to the main condenser was lost. The operators used the isolation condensers for decay heat removal. The plant safety and auxiliary buses remained energized from offsite power for the duration of the event, and the emergency diesel generators were not started. Decay heat removal systems maintained the cooling function for the reactor fuel. The main generator was reconnected to the grid at about 05:02 EDT on August 17.

Perry. Perry is located 7 miles (11 km) northeast of Painesville, OH, in northern Ohio on Lake Erie. It was generating about 1,275 MWe before the event. The reactor tripped due to a turbine control valve fast closure trip signal. The turbine control valve fast closure trip signal was due to a generator under-frequency trip signal that tripped the generator and the turbine and was triggered by grid frequency fluctuations. Plant operators noted voltage fluctuations and spikes on the main transformer, and the Generator Out-of-Step Supervisory relay actuated approximately 30 minutes before the trip. This supervisory relay senses a ground fault on the grid. The purpose is to prevent a remote fault on the grid from causing a generator out-of-step relay to activate, which would result in a generator trip. Approximately 30 seconds prior to the trip operators noted a number of spikes on the generator field volt meter, which subsequently went offscale high. The MVAr and MW meters likewise went offscale high.

The safety buses were deenergized and automatically reenergized from the emergency diesel generators. Decay heat removal systems maintained the cooling function for the reactor fuel. The following equipment problems were noted: a steam bypass valve opened; a reactor water clean-up system pump tripped; the off-gas system isolated, and a keep-fill pump was found to be air-bound, requiring venting and filling before the residual heat removal system loop A and the low pressure core spray system could be restored to service.

The lowest emergency declaration, an Unusual Event, was declared at about 16:20 EDT due to the loss of offsite power. Offsite power was restored to at least one safety bus at about 18:13 EDT on August 14. The main generator was reconnected to the grid at about 23:15 EDT on August 21. After the plant restarted, a surveillance test indicated a problem with one emergency diesel generator.[3]

Nuclear Power Plants With a Significant Transient

The electrical disturbance on August 14 had a significant impact on seven plants that continued to remain connected to the grid. For this review, significant impact means that these plants had significant load adjustments that resulted in bypassing steam from the turbine generator, opening of relief valves, or requiring the onsite emergency diesel generators to automatically start due to low voltage.

Nuclear Power Plants With a Non-Significant Transient

Sixty-four nuclear power plants experienced non-significant transients caused by minor disturbances on the electrical grid. These plants were able to respond to the disturbances through normal control systems. Examples of these transients included changes in load of a few megawatts or changes in frequency of a few-tenths Hz.

Nuclear Power Plants With No Transient

Twenty-four nuclear power plants experienced no transient and saw essentially no disturbances on the grid, or were shut down at the time of the transient.

General Observations Based on the Facts Found During Phase One

The NWG found no evidence that the shutdown of U.S. nuclear power plants triggered the outage or inappropriately contributed to its spread (i.e., to an extent beyond the normal tripping of the plants at expected conditions). This review did not identify any activity or equipment issues that appeared to start the transient on August 14, 2003. All nine plants that experienced a reactor trip were responding to grid conditions. The severity of the transient caused generators, turbines, or reactor systems to reach a protective feature limit and actuate a plant shutdown.

All nine plants tripped in response to those conditions in a manner consistent with the plant designs. All nine plants safely shut down. All safety functions were effectively accomplished, with few problems, and the plants were maintained in a safe shutdown condition until their restart. Fermi 2, Nine Mile 1, Oyster Creek, and Perry tripped on turbine and generator protective

features. FitzPatrick, Ginna, Indian Point 2 and 3, and Nine Mile 2 tripped on reactor protective features.

Nine plants used their emergency diesel generators to power their safety-related buses during the power outage. Offsite power was restored to the safety buses after the grid was energized and the plant operators, in consultation with the transmission system operators, decided the grid was stable. Although the Oyster Creek plant tripped, offsite power was never lost to their safety buses and the emergency diesel generators did not start and were not required. Another plant, Davis-Besse, was already shut down but lost power to the safety buses. The emergency diesel generators started and provided power to the safety buses as designed.

For the eight remaining tripped plants and Davis-Besse (which was already shut down prior to the events of August 14), offsite power was restored to at least one safety bus after a period of time ranging from about 2 hours to about 14 hours, with an average time of about 7 hours. Although Ginna did not lose offsite power, the operators judged offsite power to be unstable and realigned the safety buses to the emergency diesel generators.

The licensees' return to power operation follows a deliberate process controlled by plant procedures and NRC regulations. Ginna, Indian Point 2, Nine Mile 2, and Oyster Creek resumed electrical generation on August 17. FitzPatrick and Nine Mile 1 resumed electrical generation on August 18. Fermi 2 resumed electrical generation on August 20. Perry resumed electrical generation on August 21. Indian Point 3 resumed electrical generation on August 22. Indian Point 3 had equipment issues (failed splices in the control rod drive mechanism power system) that required repair prior to restart. Ginna submitted a special request for enforcement discretion from the NRC to permit mode changes and restart with an inoperable auxiliary feedwater pump. The NRC granted the request for enforcement discretion.

Conclusions of the U.S. Nuclear Working Group

As discussed above, the investigation of the U.S. nuclear power plant responses during the blackout found no significant deficiencies. Accordingly, there are no recommendations here concerning U.S. nuclear power plants. Some areas for consideration on a grid-wide basis were discussed and forwarded to the Electric System Working Group for their review.

On August 14, 2003, nine U.S. nuclear power plants tripped as a result of the loss of offsite power. Nuclear power plants are designed to cope with the loss of offsite power (LOOP) through the use of emergency power supplies (primarily on-site diesel generators). The safety function of most concern during a LOOP is the removal of heat from the reactor core. Although the control rods have been inserted to stop the fission process, the continuing decay of radioactive isotopes in the reactor core produces a significant amount of heat for many weeks. If this decay heat is not removed, it will cause fuel damage and the release of highly radioactive isotopes from the reactor core. The failure of the alternating current emergency power supplies in conjunction with a LOOP is known as a station blackout. Failures of the emergency

Table 8.2. Summary of Events for U. S. Nuclear Power Plants

Nuclear Plant	Unit	Operating Status at Time of Event		Response to Event	
		Full Power	Not Operating	Reactor and Turbine Trip	Emergency Diesels used
Davis-Besse (near Toledo, OH)	1		√		√
Fermi (near Toledo, OH)	2	√		√	√
James A. FitzPatrick (near Oswego, NY)	1	√		√	√
Ginna (near Rochester, NY)	1	√		√	√
Indian Point (near New York City, NY)	2	√		√	√
	3	√		√	√
Nine Mile Point (near Oswego, NY)	1	√		√	√
	2	√		√	√
Oyster Creek (near Toms River, NJ)	1	√		√	
Perry (near Painesville, OH)	1	√		√	√

power supplies would seriously hinder the ability of the plant operators to carry out the required safety functions. Nuclear plants can cope with a station blackout for a limited time without suffering fuel damage. However, recovery of the grid or the restoration of an emergency power supply is needed for long-term decay heat removal. For this reason, the NRC considers LOOP events to be potential precursors to more serious situations. The risk of reactor core damage increases as the LOOP frequency or duration increases.

Offsite power is considered the preferred power source for responding to all off-normal events or accidents. However, if the grid is operated in a stressed configuration, the loss of the nuclear plant generation may result in grid voltage dropping below the level needed for the plant safety loads. In that case, each plant is designed such that voltage relays will automatically disconnect the plant safety-related electrical buses from the grid and reenergize them from the emergency diesel generators (EDGs). Although the resultant safety system responses have been analyzed and found acceptable, the loss of offsite power reduces the plant's safety margin. It also increases the risk associated with failures of the EDGs. For these reasons, the NRC periodically assesses the impact of grid reliability on overall nuclear plant safety.

The NRC monitors grid reliability under its normal monitoring programs, such as the operating experience program, and has previously issued reports related to grid reliability. The NRC is continuing with an internal review of the reliability of the electrical grid and the effect on the risk profile for nuclear power plants. The NRC will consider the implications of the August 14, 2003, Northeast blackout under the NRC's regulations. The NRC is conducting an internal review of its station blackout rule, and the results of the August 14th event will be factored into that review. If there are additional findings, the NRC will address them through the NRC's normal process.

Findings of the Canadian Nuclear Working Group

Summary

On the afternoon of August 14, 2003, southern Ontario, along with the northeastern United States, experienced a widespread electrical power system outage. Eleven nuclear power plants in Ontario operating at high power levels at the time of the event either automatically shut down as a result of the grid disturbance or automatically reduced power while waiting for the grid to be reestablished. In addition, the Point Lepreau Nuclear Generating Station in New Brunswick was forced to reduce electricity production for a short period.

The Canadian NWG (CNWG) was mandated to: review the sequence of events for each Canadian nuclear plant; determine whether any events caused or contributed to the power system outage; evaluate any potential safety issues arising as a result of the event; evaluate the effect on safety and the reliability of the grid of design features, operating procedures, and regulatory requirements at Canadian nuclear power plants; and assess the impact of associated regulator performance and regulatory decisions.

In Ontario, 11 nuclear units were operating and delivering power to the grid at the time of the grid disturbance: 4 at Bruce B, 4 at Darlington, and 3 at Pickering B. Of the 11 reactors, 7 shut down as a result of the event (1 at Bruce B, 3 at Darlington, and 3 at Pickering B). Four reactors (3 at Bruce B and 1 at Darlington) disconnected safely from the grid but were able to avoid shutting down and were available to supply power to the Ontario grid as soon as reconnection was enabled by Ontario's Independent Market Operator (IMO).

New Brunswick Power's Point Lepreau Generating Station responded to the loss of grid event by cutting power to 460 MW, returning to fully stable conditions at 16:35 EDT, within 25 minutes of the event. Hydro Québec's (HQ) grid was not affected by the power system outage, and HQ's Gentilly-2 nuclear station continued to operate normally.

Having reviewed the operating data for each plant and the responses of the power stations and their staff to the event, the CNWG concludes the following:

- None of the reactor operators had any advanced warning of impending collapse of the grid.
  - Trend data obtained indicate stable conditions until a few minutes before the event.
  - There were no prior warnings from Ontario's IMO.
- Canadian nuclear power plants did not trigger the power system outage or contribute to its spread. Rather they responded, as anticipated, in order to protect equipment and systems from

the grid disturbances. Plant data confirm the following.

- ➢ At Bruce B and Pickering B, frequency and/or voltage fluctuations on the grid resulted in the automatic disconnection of generators from the grid. For those units that were successful in maintaining the unit generators operational, reactor power was automatically reduced.
- ➢ At Darlington, load swing on the grid led to the automatic reduction in power of the four reactors. The generators were, in turn, automatically disconnected from the grid.
- ➢ Three reactors at Bruce B and one at Darlington were returned to 60% power. These reactors were available to deliver power to the grid on the instructions of the IMO.
- ➢ Three units at Darlington were placed in a zero-power hot state, and four units at Pickering B and one unit at Bruce B were placed in a guaranteed shutdown state.

- ◆ There were no risks to health and safety of workers or the public as a result of the shutdown of the reactors.
  - ➢ Turbine, generator, and reactor automatic safety systems worked as designed to respond to the loss of grid.
  - ➢ Station operating staff and management followed approved Operating Policies & Principles (OP&Ps) in responding to the loss of grid. At all times, operators and shift supervisors made appropriately conservative decisions in favor of protecting health and safety.

The CNWG commends the staff of Ontario Power Generation and Bruce Power for their response to the power system outage. At all times, staff acted in accordance with established OP&Ps, and took an appropriately conservative approach to decisions.

During the course of its review, the CNWG also identified the following secondary issues:

- ◆ Equipment problems and design limitations at Pickering B resulted in a temporary reduction in the effectiveness of some of the multiple safety barriers, although the equipment failure was within the unavailability targets found in the OP&Ps approved by the CNSC as part of Ontario Power Generation's licence.
- ◆ Existing OP&Ps place constraints on the use of adjuster rods to respond to events involving rapid reductions in reactor power. While greater flexibility with respect to use of adjuster rods would not have prevented the shutdown, some units, particularly those at Darlington, might have been able to return to service less than 1 hour after the initiating event.
- ◆ Off-site power was unavailable for varying periods of time, from approximately 3 hours at Bruce B to approximately 9 hours at Pickering A. Despite the high priority assigned by the IMO to restoring power to the nuclear stations, the stations had some difficulty in obtaining timely information about the status of grid recovery and the restoration of Class IV power. This information is important for Ontario Power Generation's and Bruce Power's response strategy.
- ◆ Required regulatory approvals from CNSC staff were obtained quickly and did not delay the restart of the units; however, CNSC staff was unable to immediately activate the CNSC's Emergency Operation Centre because of loss of power to the CNSC's head office building. CNSC staff, therefore, established communications with licensees and the U.S. NRC from other locations.

Introduction

The primary focus of the CNWG during Phase I was to address nuclear power plant response relevant to the power outage of August 14, 2003. Data were collected from each power plant and analyzed in order to determine: the cause of the power outage; whether any activities at these plants caused or contributed to the power outage; and whether there were any significant safety issues. In order to obtain reliable and comparable information and data from each nuclear power plant, a questionnaire was developed to help pinpoint how each nuclear power plant responded to the August 14 grid transients. Where appropriate, additional information was obtained from the ESWG and SWG.

The operating data from each plant were compared against the plant design specifications to determine whether the plants responded as expected. Based on initial plant responses to the questionnaire, supplemental questions were developed, as required, to further clarify outstanding matters. Supplementary information on the design features of Ontario's nuclear power plants was also provided by Ontario Power Generation and Bruce Power. The CNWG also consulted a

number of subject area specialists, including CNSC staff, to validate the responses to the questionnaire and to ensure consistency in their interpretation.

In addition to the stakeholder consultations discussed in the Introduction to this chapter, CNSC staff met with officials from Ontario's Independent Market Operator on January 7, 2004.

Typical Design, Operational, and Protective Features of CANDU Nuclear Power Plants

There are 22 CANDU nuclear power reactors in Canada—20 located in Ontario at 5 multi-unit stations (Pickering A and Pickering B located in Pickering, Darlington located in the Municipality of Clarington, and Bruce A and Bruce B located near Kincardine). There are also single-unit CANDU stations at Bécancour, Québec (Gentilly-2), and Point Lepreau, New Brunswick.

In contrast to the pressurized water reactors used in the United States, which use enriched uranium fuel and a light water coolant-moderator, all housed in a single, large pressure vessel, a CANDU reactor uses fuel fabricated from natural uranium, with heavy water as the coolant and moderator. The fuel and pressurized heavy water coolant are contained in 380 to 480 pressure tubes housed in a calandria containing the heavy water moderator under low pressure. Heat generated by the fuel is removed by heavy water coolant that flows through the pressure tubes and is then circulated to the boilers to produce steam from demineralized water.

While the use of natural uranium fuel offers important benefits from the perspectives of safeguards and operating economics, one drawback is that it restricts the ability of a CANDU reactor to recover from a large power reduction. In particular, the lower reactivity of natural uranium fuel means that CANDU reactors are designed with a small number of control rods (called "adjuster rods") that are only capable of accommodating power reductions to 60%. The consequence of a larger power reduction is that the reactor will "poison out" and cannot be made critical for up to 2 days following a power reduction. By comparison, the use of enriched fuel enables a typical pressurized water reactor to operate with a large number of control rods that can be withdrawn to accommodate power reductions to zero power.

A unique feature of some CANDU plants—namely, Bruce B and Darlington—is a capability to maintain the reactor at 60% full power if the generator becomes disconnected from the grid and to maintain this "readiness" condition if necessary for days. Once reconnected to the grid, the unit can be loaded to 60% full power within several minutes and can achieve full power within 24 hours.

As with other nuclear reactors, CANDU reactors normally operate continuously at full power except when shut down for maintenance and inspections. As such, while they provide a stable source of baseload power generation, they cannot provide significant additional power in response to sudden increases in demand. CANDU power plants are not designed for black-start operation; that is, they are not designed to start up in the absence of power from the grid.

Electrical Distribution Systems

The electrical distribution systems at nuclear power plants are designed to satisfy the high safety and reliability requirements for nuclear systems. This is achieved through flexible bus arrangements, high capacity standby power generation, and ample redundancy in equipment.

Where continuous power is required, power is supplied either from batteries (for continuous DC power, Class I) or via inverters (for continuous AC power, Class II). AC supply for safety-related equipment, which can withstand short interruption (on the order of 5 minutes), is provided by Class III power. Class III power is nominally supplied through Class IV; when Class IV becomes unavailable, standby generators are started automatically, and the safety-related loads are picked up within 5 minutes of the loss of Class IV power.

The Class IV power is an AC supply to reactor equipment and systems that can withstand longer interruptions in power. Class IV power can be supplied either from the generator through a transformer or from the grid by another transformer. Class IV power is not required for reactors to shut down safely.

In addition to the four classes of power described above, there is an additional source of power known as the Emergency Power System (EPS). EPS is a separate power system consisting of its own on-site power generation and AC and DC distribution systems whose normal supply is from the Class III power system. The purpose of the EPS system is to provide power to selected safety-related loads following common mode incidents, such as seismic events.

Protective Features of CANDU Nuclear Power Plants

CANDU reactors typically have two separate, independent and diverse systems to shut down the reactor in the event of an accident or transients in the grid. Shutdown System 1 (SDS1) consists of a large number of cadmium rods that drop into the core to decrease the power level by absorbing neutrons. Shutdown System 2 (SDS2) consists of high-pressure injection of gadolinium nitrate into the low-pressure moderator to decrease the power level by absorbing neutrons. Although Pickering A does not have a fully independent SDS2, it does have a second shutdown mechanism, namely, the fast drain of the moderator out of the calandria; removal of the moderator significantly reduces the rate of nuclear fission, which reduces reactor power. Also, additional trip circuits and shutoff rods have recently been added to Pickering A Unit 4 (Shutdown System Enhancement, or SDS-E). Both SDS1 and SDS2 are capable of reducing reactor power from 100% to about 2% within a few seconds of trip initiation.

Fuel Heat Removal Features of CANDU Nuclear Power Plants

Following the loss of Class IV power and shutdown of the reactor through action of SDS1 and/or SDS2, significant heat will continue to be generated in the reactor fuel from the decay of fission products. The CANDU design philosophy is to provide defense in depth in the heat removal systems.

Immediately following the trip and prior to restoration of Class III power, heat will be removed from the reactor core by natural circulation of coolant through the Heat Transport System main circuit following rundown of the main Heat Transport pumps (first by thermosyphoning and later by intermittent buoyancy induced flow). Heat will be rejected from the secondary side of the steam generators through the atmospheric steam discharge valves. This mode of operation can be sustained for many days with additional feedwater supplied to the steam generators via the Class III powered auxiliary steam generator feed pump(s).

In the event that the auxiliary feedwater system becomes unavailable, there are two alternate EPS powered water supplies to steam generators, namely, the Steam Generator Emergency Coolant System and the Emergency Service Water System. Finally, a separate and independent means of cooling the fuel is by forced circulation by means of the Class III powered shutdown cooling system; heat removal to the shutdown cooling heat exchangers is by means of the Class III powered components of the Service Water System.

CANDU Reactor Response to Loss-of-Grid Event

Response to Loss of Grid

In the event of disconnection from the grid, power to shut down the reactor safely and maintain essential systems will be supplied from batteries and standby generators. The specific response of a reactor to disconnection from the grid will depend on the reactor design and the condition of the unit at the time of the event.

60% Reactor Power: All CANDU reactors are designed to operate at 60% of full power following the loss of off-site power. They can operate at this level as long as demineralized water is available for the boilers. At Darlington and Bruce B, steam can be diverted to the condensers and recirculated to the boilers. At Pickering A and Pickering B, excess steam is vented to the atmosphere, thereby limiting the operating time to the available inventory of demineralized water.

0% Reactor Power, Hot: The successful transition from 100% to 60% power depends on several systems responding properly, and continued operation is not guaranteed. The reactor may shut down automatically through the operation of the process control systems or through the action of either of the shutdown systems.

Should a reactor shutdown occur following a load rejection, both Class IV power supplies (from the generator and the grid) to that unit will become unavailable. The main Heat Transport pumps will trip, leading to a loss of forced circulation of coolant through the core. Decay heat will be continuously removed through natural circulation (thermosyphoning) to the boilers, and steam produced in the boilers will be exhausted to the atmosphere via atmospheric steam discharge valves. The Heat Transport System will be maintained at around 250 to 265 degrees Celsius during thermosyphoning. Standby generators will start automatically and restore Class III power to key safety-related systems. Forced circulation in the Heat Transport System will be restored once either Class III or Class IV power is available.

When shut down, the natural decay of fission products will lead to the temporary buildup of

neutron absorbing elements in the fuel. If the reactor is not quickly restarted to reverse this natural process, it will "poison-out." Once poisoned-out, the reactor cannot return to operation until the fission products have further decayed, a process which typically takes up to 2 days.

Overpoisoned Guaranteed Shutdown State: In the event that certain problems are identified when reviewing the state of the reactor after a significant transient, the operating staff will cool down and depressurize the reactor, then place it in an overpoisoned guaranteed shutdown state (GSS) through the dissolution of gadolinium nitrate into the moderator. Maintenance will then be initiated to correct the problem.

Return to Service Following Loss of Grid

The return to service of a unit following any one of the above responses to a loss-of-grid event is discussed below. It is important to note that the descriptions provided relate to operations on a single unit. At multi-unit stations, the return to service of several units cannot always proceed in parallel, due to constraints on labor availability and the need to focus on critical evolutions, such as taking the reactor from a subcritical to a critical state.

60% Reactor Power: In this state, the unit can be resynchronized consistent with system demand, and power can be increased gradually to full power over approximately 24 hours.

0% Reactor Power, Hot: In this state, after approximately 2 days for the poison-out, the turbine can be run up and the unit synchronized. Thereafter, power can be increased to high power over the next day. This restart timeline does not include the time required for any repairs or maintenance that might have been necessary during the outage.

Overpoisoned Guaranteed Shutdown State: Placing the reactor in a GSS after it has been shut down requires approximately 2 days. Once the condition that required entry to the GSS is rectified, the restart requires removal of the guarantee, removal of the gadolinium nitrate through ion exchange process, heatup of the Heat Transport System, and finally synchronization to the grid. Approximately 4 days are required to complete these restart activities. In total, 6 days from shutdown are required to return a unit to service from the GSS, and this excludes any repairs that might have been required while in the GSS.

Summary of Canadian Nuclear Power Plant Response to and Safety During the August 14 Outage

On the afternoon of August 14, 2003, 15 Canadian nuclear units were operating: 13 in Ontario, 1 in Québec, and 1 in New Brunswick. Of the 13 Ontario reactors that were critical at the time of the event, 11 were operating at or near full power and 2 at low power (Pickering B Unit 7 and Pickering A Unit 4). All 13 of the Ontario reactors disconnected from the grid as a result of the grid disturbance. Seven of the 11 reactors operating at high power shut down, while the remaining 4 operated in a planned manner that enabled them to remain available to reconnect to the grid at the request of Ontario's IMO. Of the 2 Ontario reactors operating at low power, Pickering A Unit 4 tripped automatically, and Pickering B Unit 7 was tripped manually and shut down. In addition, a transient was experienced at New Brunswick Power's Point Lepreau Nuclear Generating Station, resulting in a reduction in power. Hydro Québec's Gentilly-2 nuclear station continued to operate normally as the Hydro Québec grid was not affected by the grid disturbance.

Nuclear Power Plants With Significant Transients

Pickering Nuclear Generating Station. The Pickering Nuclear Generating Station (PNGS) is located in Pickering, Ontario, on the shores of Lake Ontario, 19 miles (30 km) east of Toronto. It houses 8 nuclear reactors, each capable of delivering 515 MW to the grid. Three of the 4 units at Pickering A (Units 1 through 3) have been shut down since late 1997. Unit 4 was restarted earlier this year following a major refurbishment and was in the process of being commissioned at the time of the event. At Pickering B, 3 units were operating at or near 100% prior to the event, and Unit 7 was being started up following a planned maintenance outage.

Pickering A. As part of the commissioning process, Unit 4 at Pickering A was operating at 12% power in preparation for synchronization to the grid. The reactor automatically tripped on SDS1 due to Heat Transport Low Coolant Flow, when the Heat Transport main circulating pumps ran down following the Class IV power loss. The decision was then made to return Unit 4 to the guaranteed shutdown state. Unit 4 was synchronized to the grid on August 20, 2003. Units 1, 2 and 3 were in lay-up mode.

Pickering B. The Unit 5 Generator Excitation System transferred to manual control due to large voltage oscillations on the grid at 16:10 EDT and then tripped on Loss of Excitation about 1 second later (prior to grid frequency collapse). In response to the generator trip, Class IV buses transferred to the system transformer and the reactor setback. The grid frequency collapse caused the System Service Transformer to disconnect from the grid, resulting in a total loss of Class IV power. The reactor consequently tripped on the SDS1 Low Gross Flow parameter followed by an SDS2 trip due to Low Core Differential Pressure.

The Unit 6 Generator Excitation System also transferred to manual control at 16:10 EDT due to large voltage oscillations on the grid and the generator remained connected to the grid in manual voltage control. Approximately 65 seconds into the event, the grid under-frequency caused all the Class IV buses to transfer to the Generator Service Transformer. Ten seconds later, the generator separated from the Grid. Five seconds later, the generator tripped on Loss of Excitation, which caused a total loss of Class IV power. The reactor consequently tripped on the SDS1 Low Gross Flow parameter, followed by an SDS2 trip due to Low Core Differential Pressure.

Unit 7 was coming back from a planned maintenance outage and was at 0.9% power at the time of the event. The unit was manually tripped after loss of Class IV power, in accordance with procedures and returned to guaranteed shutdown state.

Unit 8 reactor automatically set back on load rejection. The setback would normally have been terminated at 20% power but continued to 2% power because of the low boiler levels. The unit subsequently tripped on the SDS1 Low Boiler Feedline Pressure parameter due to a power mismatch between the reactor and the turbine.

The following equipment problems were noted. At Pickering, the High Pressure Emergency Coolant Injection System (HPECIS) pumps are designed to operate from a Class IV power supply. As a result of the shutdown of all the operating units, the HPECIS at both Pickering A and Pickering B became unavailable for 5.5 hours. (The design of Pickering A and Pickering B HPECIS must be such that the fraction of time for which it is not available can be demonstrated to be less than 10^{-3} years—about 8 hours per year. This was the first unavailability of the HPECIS for 2003.) In addition, Emergency High Pressure Service Water System restoration for all Pickering B units was delayed because of low suction pressure supplying the Emergency High Pressure Service Water pumps. Manual operator intervention was required to restore some pumps back to service.

Units were synchronized to the grid as follows: Unit 8 on August 22, Unit 5 on August 23, Unit 6 on August 25, and Unit 7 on August 29.

Darlington Nuclear Generating Station. Four reactors are located at the Darlington Nuclear Generation Station, which is on the shores of Lake Ontario in the Municipality of Clarington, 43 miles (70 km) east of Toronto. All four of the reactors are licensed to operate at 100% of full power, and each is capable of delivering approximately 880 MW to the grid.

Unit 1 automatically stepped back to the 60% reactor power state upon load rejection at 16:12 EDT. Approval by the shift supervisor to automatically withdraw the adjuster rods could not be provided due to the brief period of time for the shift supervisor to complete the verification of systems as per procedure. The decreasing steam pressure and turbine frequency then required the reactor to be manually tripped on SDS1, as per procedure for loss of Class IV power. The trip occurred at 16:24 EDT, followed by a manual turbine trip due to under-frequency concerns.

Like Unit 1, Unit 2 automatically stepped back upon load rejection at 16:12 EDT. As with Unit 1, there was insufficient time for the shift supervisor to complete the verification of systems, and faced with decreasing steam pressure and turbine frequency, the decision was made to shut down Unit 2. Due to under-frequency on the main Primary Heat Transport pumps, the turbine was tripped manually which resulted in an SDS1 trip at 16:28 EDT.

Unit 3 experienced a load rejection at 16:12 EDT, and during the stepback Unit 3 was able to sustain operation with steam directed to the condensers. After system verifications were complete, approval to place the adjuster rods on automatic was obtained in time to recover, at 59% reactor power. The unit was available to resynchronize to the grid.

Unit 4 experienced a load rejection at 16:12 EDT, and required a manual SDS1 trip due to the loss of Class II bus. This was followed by a manual turbine trip.

The following equipment problems were noted: Unit 4 Class II inverter trip on BUS A3 and

subsequent loss of critical loads prevented unit recovery. The Unit 0 Emergency Power System BUS B135 power was lost until the Class III power was restored. (A planned battery bank B135 change out was in progress at the time of the blackout.)

Units were synchronized to the grid as follows: Unit 3 at 22:00 EDT on August 14; Unit 2 on August 17, 2003; Unit 1 on August 18, 2003; and Unit 4 on August 18, 2003.

Bruce Power. Eight reactors are located at Bruce Power on the eastern shore of Lake Huron between Kincardine and Port Elgin, Ontario. Units 5 through 8 are capable of generating 840 MW each. Presently these reactors are operating at 90% of full power due to license conditions imposed by the CNSC. Units 1 through 4 have been shut down since December 31, 1997. At the time of the event, work was being performed to return Units 3 and 4 to service.

Bruce A. Although these reactors were in guaranteed shutdown state, they were manually tripped, in accordance with operating procedures. SDS1 was manually tripped on Units 3 and 4, as per procedures for a loss of Class IV power event. SDS1 was re-poised on both units when the station power supplies were stabilized. The emergency transfer system functioned as per design, with the Class III standby generators picking up station electrical loads. The recently installed Qualified Diesel Generators received a start signal and were available to pick up emergency loads if necessary.

Bruce B. Units 5, 6, 7, and 8 experienced initial generation rejection and accompanying stepback on all four reactor units. All generators separated from the grid on under-frequency at 16:12 EDT. Units 5, 7, and 8 maintained reactor power at 60% of full power and were immediately available for reconnection to the grid.

Although initially surviving the loss of grid event, Unit 6 experienced an SDS1 trip on insufficient Neutron Over Power (NOP) margin. This occurred while withdrawing Bank 3 of the adjusters in an attempt to offset the xenon transient, resulting in a loss of Class IV power.

The following equipment problems were noted: An adjuster rod on Unit 6 had been identified on August 13, 2003, as not working correctly. Unit 6 experienced a High Pressure Recirculation Water line leak, and the Closed Loop Demineralized Water loop lost inventory to the Emergency Water Supply System.

Units were synchronized to the grid as follows: Unit 8 at 19:14 EDT on August 14, 2003; Unit 5 at 21:04 EDT on August 14; and Unit 7 at 21:14 EDT on August 14, 2003. Unit 6 was resynchronized at 02:03 EDT on August 23, 2003, after maintenance was conducted.

Point Lepreau Nuclear Generating Station. The Point Lepreau nuclear station overlooks the Bay of Fundy on the Lepreau Peninsula, 25 miles (40 km) southwest of Saint John, New Brunswick. Point Lepreau is a single-unit CANDU 6, designed for a gross output of 680 MW. It is owned and operated by New Brunswick Power.

Point Lepreau was operating at 91.5% of full power (610 MWe) at the time of the event. When the event occurred, the unit responded to changes in grid frequency as per design. The net impact was a short-term drop in output by 140 MW, with reactor power remaining constant and excess thermal energy being discharged via the unit steam discharge valves. During the 25 seconds of the event, the unit stabilizer operated numerous times to help dampen the turbine generator speed oscillations that were being introduced by the grid frequency changes. Within 25 minutes of the event initiation, the turbine generator was reloaded to 610 MW. Given the nature of the event that occurred, there were no unexpected observations on the New Brunswick Power grid or at Point Lepreau Generating Station throughout the ensuing transient.

Nuclear Power Plants With No Transient

Gentilly-2 Nuclear Station. Hydro Québec owns and operates Gentilly-2 nuclear station, located on the south shore of the St. Lawrence River opposite the city of Trois-Rivières, Québec. Gentilly-2 is capable of delivering approximately 675 MW to Hydro Québec's grid. The Hydro Québec grid was not affected by the power system outage and Gentilly-2 continued to operate normally.

General Observations Based on the Facts Found During Phase I

Following the review of the data provided by the Canadian nuclear power plants, the CNWG concludes the following:

- None of the reactor operators had any advanced warning of impending collapse of the grid.
- Canadian nuclear power plants did not trigger the power system outage or contribute to its spread.

- There were no risks to the health and safety of workers or the public as a result of the concurrent shutdown of several reactors. Automatic safety systems for the turbine generators and reactors worked as designed. (See Table 8.3 for a summary of shutdown events for Canadian nuclear power plants.)

The CNWG also identified the following secondary issues:

- Equipment problems and design limitations at Pickering B resulted in a temporary reduction in the effectiveness of some of the multiple safety barriers, although the equipment failure was within the unavailability targets found in the OP&Ps approved by the CNSC as part of Ontario Power Generation's license.
- Existing OP&Ps place constraints on the use of adjuster rods to respond to events involving rapid reductions in reactor power. While greater flexibility with respect to use of adjuster rods would not have prevented the shutdown, some units, particularly those at Darlington, might have been able to return to service less than 1 hour after the initiating event.
- Off-site power was unavailable for varying periods of time, from approximately 3 hours at Bruce B to approximately 9 hours at Pickering A. Despite the high priority assigned by the IMO to restoring power to the nuclear stations, the stations had some difficulty obtaining timely information about the status of grid recovery and the restoration of Class IV power. This information is important for Ontario Power Generation's and Bruce Power's response strategy.
- Required regulatory approvals from CNSC staff were obtained quickly and did not delay the

Table 8.3. Summary of Shutdown Events for Canadian Nuclear Power Plants

		Operating Status at Time of Event			Response to Event			
							Reactor Trip	
Generating Station	Unit	Full Power	Startup	Not Operating	Stepback to 60% Power, Available To Supply Grid	Turbine Trip	SDS1	SDS2
Pickering NGS	1			√			(a)	
	2			√				
	3			√				
	4		√				√	(b)
	5	√					√	√
	6	√					√	√
	7		√				√	
	8	√					√	
Darlington NGS	1	√				√	√	
	2	√				√	√	
	3	√			√			
	4	√				√	√	
Bruce Nuclear Power Development	1			√				
	2			√				
	3			√			√	
	4			√			√	
	5	√			√			
	6	√					√	
	7	√			√			
	8	√			√			

[a]Pickering A Unit 1 tripped as a result of electrical bus configuration immediately prior to the event which resulted in a temporary loss of Class II power.

[b]Pickering A Unit 4 also tripped on SDS-E.

Notes: Unit 7 at Pickering B was operating at low power, warming up prior to reconnecting to the grid after a maintenance outage. Unit 4 at Pickering A was producing at low power, as part of the reactor's commissioning after extensive refurbishment since being shut down in 1997.

restart of the units; however, CNSC staff was unable to immediately activate the CNSC's Emergency Operation Centre because of loss of power to the CNSC's head office building. CNSC staff, therefore, established communications with licensees and the U.S. NRC from other locations.

Regulatory Activities Subsequent to the Blackout

The actuation of emergency shutdown systems at Bruce, Darlington and Pickering, and the impairment of the High Pressure Emergency Coolant Injection System (HPECIS) at Pickering are events for which licensees need to file reports with the Canadian Nuclear Safety Commission (CNSC), in accordance with Regulatory Standard S 99, "Reporting Requirements for Operating Nuclear Power Plants." Reports have been submitted by Ontario Power Generation (OPG) and Bruce Power, and are being followed up by staff from the CNSC as part of the CNSC's normal regulatory process. This includes CNSC's review and approval, where appropriate, of any actions taken or proposed to be taken to correct any problems in design, equipment or operating procedures identified by OPG and Bruce Power.

As a result of further information about the event gathered by CNSC staff during followup inspections, the temporary impairment of the HPECIS at Pickering has been rated by CNSC staff as Level 2 on the International Nuclear Event Scale, indicating that there was a significant failure in safety provisions, but with sufficient backup systems, or "defense-in-depth," in place to cope with potential malfunctions. Since August 2003, OPG has implemented procedural and operational changes to improve the performance of the safety systems at Pickering.

Conclusions of the Canadian Nuclear Working Group

As discussed above, Canadian nuclear power plants did not trigger the power system outage or contribute to its spread. The CNWG therefore made no recommendations with respect to the design or operation of Canadian nuclear plants to improve the reliability of the Ontario electricity grid.

The CNWG made two recommendations, one concerning backup electrical generation equipment to the CNSC's Emergency Operations Centre and another concerning the use of adjuster rods during future events involving the loss of off-site power. These are presented in Chapter 10 along with the Task Force's recommendations on other subjects.

Despite some comments to the contrary, the CNWG's investigation found that the time to restart the reactors was reasonable and in line with design specifications for the reactors. Therefore, the CNWG made no recommendations for action on this matter. Comments were also made regarding the adequacy of generation capacity in Ontario and the appropriate mix of technologies for electricity generation. This is a matter beyond the CNWG's mandate, and it made no recommendations on this issue.

Perspective of Nuclear Regulatory Agencies on Potential Changes to the Grid

The NRC and the CNSC, under their respective regulatory authorities, are entrusted with providing reasonable assurance of adequate protection of public health and safety. As the design and operation of the electricity grid is taken into account when evaluating the safety analysis of nuclear power plants, changes to the electricity grid must be evaluated for the impact on plant safety. As the Task Force final recommendations result in actions to affect changes, the NRC and the CNSC will assist by evaluating potential effects on the safety of nuclear power plant operation.

The NRC and the CNSC acknowledge that future improvements in grid reliability will involve coordination among many groups. The NRC and the CNSC intend to maintain the good working relationships that have been developed during the Task Force investigation to ensure that we continue to share experience and insights and work together to maintain an effective and reliable electric supply system.

Endnotes

[1] Further details are available in the NRC Special Inspection Report dated December 22, 2003, ADAMS Accession No. ML033570386.

[2] Further details are available in the NRC Special Inspection Report dated December 22, 2003, ADAMS Accession No. ML033570386.

[3] Further details are available in the NRC Special Inspection Report dated October 10, 2003, ADAMS Acccession No. ML032880107.

9. Physical and Cyber Security Aspects of the Blackout

Summary and Primary Findings

After the Task Force Interim Report was issued in November 2003, the Security Working Group (SWG) continued in its efforts to investigate whether a malicious cyber event directly caused or significantly contributed to the power outage of August 14, 2003. These efforts included additional analyses of interviews conducted prior to the release of the Interim Report and additional consultations with representatives from the electric power sector. The information gathered from these efforts validated the SWG's Interim Report preliminary findings and the SWG found no reason to amend, alter, or negate any of the information submitted to the Task Force for the Interim Report.

Specifically, further analysis by the SWG found no evidence that malicious actors caused or contributed to the power outage, nor is there evidence that worms or viruses circulating on the Internet at the time of the power outage had an effect on power generation and delivery systems of the companies directly involved in the power outage. The SWG acknowledges reports of al-Qaeda claims of responsibility for the power outage of August 14, 2003. However, these claims are not consistent with the SWG's findings. SWG analysis also brought to light certain concerns respecting the possible failure of alarm software; links to control and data acquisition software; and the lack of a system or process for some grid operators to adequately view the status of electric systems outside of their immediate control.

After the release of the Interim Report in November 2003, the SWG determined that the existing data, and the findings derived from analysis of those data, provided sufficient certainty to exclude the probability that a malicious cyber event directly caused or significantly contributed to the power outage events. As such, further data collection efforts to conduct broader analysis were deemed unnecessary. While no additional data were collected, further analysis and interviews conducted after the release of the Interim Report allowed the SWG to validate its preliminary findings and the SWG to make recommendations on those findings:

- Interviews and analyses conducted by the SWG indicate that within some of the companies interviewed there are potential opportunities for cyber system compromise of Energy Management Systems (EMS) and their supporting information technology (IT) infrastructure. Indications of procedural and technical IT management vulnerabilities were observed in some facilities, such as unnecessary software services not denied by default, loosely controlled system access and perimeter control, poor patch and configuration management, and poor system security documentation. This situation caused the SWG to support the promulgation, implementation, and enforcement of cyber and physical security standards for the electric power sector.

Recommendation 32, page 163

- A failure in a software program not linked to malicious activity may have significantly contributed to the power outage. Since the issuance of the Interim Report, the SWG consulted with the software program's vendor and confirmed that since the August 14, 2003, power outage, the vendor provided industry with the necessary information and mitigation steps to address this software failure. In Canada, a survey was posted on the Canadian Electricity Association (CEA) secure members-only web site to determine if the software was in use. The responses indicated that it is not used by Canadian companies in the industry.

Recommendation 33, page 164

- Internal and external links from Supervisory Control and Data Acquisition (SCADA) networks to other systems introduced vulnerabilities.

Recommendation 34, page 165

- In some cases, Control Area (CA) and Reliability Coordinator (RC) visibility into the operations of surrounding areas was lacking.

Recommendation 35, page 165

The SWG's analysis is reflected in a total of 15 recommendations, two of which were combined with similar concerns by the ESWG (Recommendations 19 and 22); for the remaining 13, see Recommendations 32-44 (pages 163-169).

Overall, the SWG's final report was the result of interviews conducted with representatives of Cinergy, FirstEnergy, American Electric Power (AEP), PJM Interconnect, the Midwest Independent System Operator (MISO), the East Central Area Reliability Coordinating Agreement (ECAR), and GE Power Systems Division. These entities were chosen due to their proximity to the causes of the power outage based on the analysis of the Electric System Working Group (ESWG). The findings contained in this report relate only to those entities surveyed. The final report also incorporates information gathered from third party sources as well as federal security and intelligence communities.

In summary, SWG analysis provided no evidence that a malicious cyber attack was a direct or indirect cause of the August 14, 2003, power outage. This conclusion is supported by the SWG's event timeline, detailed later in this chapter, which explains in detail the series of non-malicious human and cyber failures that ultimately resulted in the power outage. In the course of its analysis the SWG, however, did identify a number of areas of concern respecting cyber security aspects of the electricity sector.

SWG Mandate and Scope

It is widely recognized that the increased reliance on IT by critical infrastructure sectors, including the energy sector, has increased the vulnerability of these systems to disruption via cyber means. The ability to exploit these vulnerabilities has been demonstrated in North America. The SWG was comprised of United States and Canadian federal, state, provincial and local experts in both physical and cyber security and its objective was to determine the role, if any, that a malicious cyber event played in causing, or contributing to, the power outage of August 14, 2003. For the purposes of its work, the SWG defined a "malicious cyber event" as the manipulation of data, software or hardware for the purpose of deliberately disrupting the systems that control and support the generation and delivery of electric power.

The SWG worked closely with the United States and Canadian law enforcement, intelligence and homeland security communities to examine the possible role of malicious actors in the power outage. A primary activity in this endeavor was the collection and review of available intelligence related to the power outage of August 14, 2003. The SWG also collaborated with the energy industry to examine the cyber systems that control power generation and delivery operations, the physical security of cyber assets, cyber policies and procedures and the functionality of supporting infrastructures—such as communication systems and backup power generation, which facilitate the smooth running operation of cyber assets—to determine if the operation of these systems was affected by malicious activity. The SWG coordinated its efforts with those of other Working Groups and there was a significant interdependence on each groups work products and findings. The SWG's focus was on the cyber operations of those companies in the United States involved in the early stages of the power outage timeline, as identified by the ESWG.

Outside of the SWG's scope was the examination of the non-cyber physical infrastructure aspects of the power outage of August 14, 2003. The Interim Report detailed the SWG's availability to investigate breaches of physical security unrelated to the cyber dimensions of the infrastructure on behalf of the Task Force but no incidents came to the SWG's attention during its work. Also outside of the scope of the SWG's work was analysis of the impacts the power outage had on other critical infrastructure sectors. Both Public Safety and Emergency Preparedness Canada and the U.S. Department of Homeland Security (DHS) examined these issues, but not within the context of the SWG.

Cyber Security in the Electricity Sector

The generation and delivery of electricity has been, and continues to be, a target of malicious groups and individuals intent on disrupting this system. Even attacks that do not directly target the electricity sector can have disruptive effects on

electricity system operations. Many malicious code attacks, by their very nature, are unbiased and tend to interfere with operations supported by vulnerable applications. One such incident occurred in January 2003, when the "Slammer" Internet worm took down monitoring computers at FirstEnergy Corporation's idled Davis-Besse nuclear plant. A subsequent report by the North American Electric Reliability Council (NERC) concluded that although the infection caused no outages, it blocked commands that operated other power utilities.[1]

This example, among others, highlights the increased vulnerability to disruption via cyber means faced by North America's critical infrastructure sectors, including the energy sector. Of specific concern to the United States and Canadian governments are the SCADA networks, which contain computers and applications that perform a wide variety of functions across many industries. In electric power, SCADA includes telemetry for status and control, as well as EMS, protective relaying and automatic generation control. SCADA systems were developed to maximize functionality and interoperability, with little attention given to cyber security. These systems, many of which were intended to be isolated, now find themselves for a variety of business and operational reasons, either directly or indirectly connected to the global Internet. For example, in some instances, there may be a need for employees to monitor SCADA systems remotely. However, connecting SCADA systems to a remotely accessible computer network can present security risks. These risks include the compromise of sensitive operating information and the threat of unauthorized access to SCADA systems' control mechanisms.

Security has always been a priority for the electricity sector in North America; however, it is a greater priority now than ever before. CAs and RCs recognize that the threat environment is changing and that the risks are greater than in the past, and they have taken steps towards improving their security postures. NERC's Critical Infrastructure Protection Advisory Group has been examining ways to improve both the physical and cyber security dimensions of the North American power grid. This group is comprised of Canadian and U.S. industry experts in the areas of cyber security, physical security and operational security. The creation of a national SCADA program is now also under discussion in the U.S. to improve the physical and cyber security of these control systems. The Canadian Electricity Association's Critical Infrastructure Working Group is examining similar measures.

Information Collection and Analysis

After analyzing information already obtained from stakeholder interviews, telephone transcripts, law enforcement and intelligence information, and other ESWG working documents, the SWG determined that it was not necessary to analyze other sources of data on the cyber operations of those such as log data from routers, intrusion detection systems, firewalls, EMS, change management logs, and physical security materials.

The SWG was divided into six sub-teams to address the discrete components of this investigation: Cyber Analysis, Intelligence Analysis, Physical Analysis, Policies and Procedures, Supporting Infrastructure, and Root Cause Liaison. The SWG organized itself in this manner to create a holistic approach to address each of the main areas of concern with regards to power grid vulnerabilities. Rather than analyze each area of concern separately, the SWG sub-team structure provided a more comprehensive framework in which to investigate whether malicious activity was a cause of the power outage of August 14, 2003. Each sub-team was staffed with Subject Matter Experts (SMEs) from government, industry, and academia to provide the analytical breadth and depth necessary to complete each sub-team's objective. A detailed overview of the sub-team structure and activities for each sub-team is provided below.

1. Cyber Analysis

The Cyber Analysis sub-team was led by the CERT® Coordination Center (CERT/CC) at Carnegie Mellon University and the Royal Canadian Mounted Police (RCMP). This team was focused on analyzing and reviewing electronic media of computer networks in which online communications take place. The sub-team examined these networks to determine if they were maliciously used to cause, or contribute to the August 14, 2003, outage. Specifically, the SWG reviewed materials created on behalf of DHS's National Communication System (NCS). These materials covered the analysis and conclusions of their Internet Protocol (IP) modeling correlation study of Blaster (a malicious Internet worm first noticed on August 11, 2003) and the power outage. This

NCS analysis supports the SWG's finding that viruses and worms prevalent across the Internet at the time of the outage did not have any significant impact on power generation and delivery systems. The team also conducted interviews with vendors to identify known system flaws and vulnerabilities.

This sub-team took a number of steps, including reviewing NERC reliability standards to gain a better understanding of the overall security posture of the electric power industry. Additionally, the sub-team participated in meetings in Baltimore on August 22 and 23, 2003. The meetings provided an opportunity for the cyber experts and the power industry experts to understand the details necessary to conduct an investigation.

Members of the sub-team also participated in the NERC/Department of Energy (DOE) Fact Finding meeting held in Newark, New Jersey on September 8, 2003. Each company involved in the outage provided answers to a set of questions related to the outage. The meeting helped to provide a better understanding of what each company experienced before, during and after the outage. Additionally, sub-team members participated in interviews with grid operators from FirstEnergy on October 8 and 9, 2003, and from Cinergy on October 10, 2003.

2. Intelligence Analysis

The Intelligence Analysis sub-team was led by DHS and the RCMP, which worked closely with Federal, State and local law enforcement, intelligence and homeland security organizations to assess whether the power outage was the result of a malicious attack.

SWG analysis provided no evidence that malicious actors—be they individuals or organizations—were responsible for, or contributed to, the power outage of August 14, 2003. Additionally, the sub-team found no indication of deliberate physical damage to power generating stations and delivery lines on the day of the outage and there were no reports indicating the power outage was caused by a computer network attack.

Both U.S. and Canadian government authorities provide threat intelligence information to their respective energy sectors when appropriate. No intelligence reports prior to, during or after the power outage indicated any specific terrorist plans or operations against the energy infrastructure. There was, however, threat information of a general nature relating to the sector which was provided to the North American energy industry by U.S. and Canadian Government agencies in late July 2003. This information indicated that al-Qaeda might attempt to carry out a physical attack involving explosions at oil production facilities, power plants or nuclear plants on the east coast of the U.S. during the summer of 2003. The type of physical attack described in the intelligence that prompted this threat warning is not consistent with the events causing the power outage as there was no indication of a kinetic event before, during, or immediately after the power outage of August 14, 2003.

Despite all of the above indications that no terrorist activity caused the power outage, al-Qaeda publicly claimed responsibility for its occurrence:

- *August 18, 2003:* Al-Hayat, an Egyptian media outlet, published excerpts from a communiqué attributed to al-Qaeda. Al Hayat claimed to have obtained the communiqué from the website of the International Islamic Media Center. The content of the communiqué asserts that the "brigades of Abu Fahes Al Masri had hit two main power plants supplying the East of the U.S., as well as major industrial cities in the U.S. and Canada, . . . its ally in the war against Islam (New York and Toronto) and their neighbors." Furthermore, the operation "was carried out on the orders of Osama bin Laden to hit the pillars of the U.S. economy," as "a realization of bin Laden's promise to offer the Iraqi people a present." The communiqué does not specify the way the alleged sabotage was carried out, but does elaborate on the alleged damage the sabotage caused to the U.S. economy in the areas of finance, transportation, energy and telecommunications.

Additional claims and commentary regarding the power outage appeared in various Middle Eastern media outlets:

- *August 26, 2003:* A conservative Iranian daily newspaper published a commentary regarding the potential of computer technology as a tool for terrorists against infrastructures dependent on computer networks, most notably water, electric, public transportation, trade organizations and "supranational" companies in the United States.
- *September 4, 2003:* An Islamist participant in a Jihadist chat room forum claimed that sleeper cells associated with al-Qaeda used the power

outage as a cover to infiltrate the U.S. from Canada.

However, these claims as known are not consistent with the SWG's findings. They are also not consistent with congressional testimony of the Federal Bureau of Investigation (FBI). Larry A. Mefford, Executive Assistant Director in charge of the FBI's Counterterrorism and Counterintelligence programs, testified in U.S. Congress on September 4, 2003, that:

> *"To date, we have not discovered any evidence indicating that the outage was a result of activity by international or domestic terrorists or other criminal activity."*[2]

Mr. Mefford also testified that:

> *"The FBI has received no specific, credible threats to electronic power grids in the United States in the recent past and the claim of the Abu Hafs al-Masri Brigade to have caused the blackout appears to be no more than wishful thinking. We have no information confirming the actual existence of this group."*[3]

Current assessments suggest that there are terrorists and other malicious actors who have the capability to conduct a malicious cyber attack with potential to disrupt the energy infrastructure. Although such an attack cannot be ruled out entirely, an examination of available information and intelligence does not support any claims of a deliberate attack against the energy infrastructure on, or leading up to, August 14, 2003. The few instances of physical damage that occurred on power delivery lines were the result of natural events and not of sabotage. No intelligence reports prior to, during or after the power outage indicated any specific terrorist plans or operations against the energy infrastructure. No incident reports detail suspicious activity near the power generation plants or delivery lines in question.

3. Physical Analysis

The Physical Analysis sub-team was led by the United States Secret Service and the RCMP. These organizations have a particular expertise in physical security assessments in the energy sector. The sub-team focused on issues related to how the cyber-related facilities of the energy sector companies were secured, including the physical integrity of data centers and control rooms along with security procedures and policies used to limit access to sensitive areas. Focusing on the facilities identified as having a causal relationship to the outage, the sub-team sought to determine if the physical integrity of these cyber facilities was breached, whether externally or by an insider, prior to or during the outage, and if so, whether such a breach caused or contributed to the power outage.

Although the sub-team analyzed information provided to both the ESWG and Nuclear Working Groups, the Physical Analysis sub-team also reviewed information resulting from face-to-face meetings with energy sector personnel and site-visits to energy sector facilities to determine the physical integrity of the cyber infrastructure.

The sub-team compiled a list of questions covering location, accessibility, cameras, alarms, locks, fire protection and water systems as they apply to computer server rooms. Based on discussions of these questions during its interviews, the sub-team found no evidence that the physical integrity of the cyber infrastructure was breached. Additionally, the sub-team examined access and control measures used to allow entry into command and control facilities and the integrity of remote facilities.

The sub-team also concentrated on mechanisms used by the companies to report unusual incidents within server rooms, command and control rooms and remote facilities. The sub-team also addressed the possibility of an insider attack on the cyber infrastructure.

4. Policies and Procedures

The Policies and Procedures sub-team was led by DHS and Public Safety and Emergency Preparedness Canada. Personnel from these organizations have strong backgrounds in the fields of electric delivery operations, automated control systems including SCADA and EMS, and information security.

This sub-team was focused on examining the overall policies and procedures that may or may not have been in place during the events leading up to and during the power outage of August 14, 2003. Policies that the team examined revolved centrally around the cyber systems of the companies identified in the early stages of the power outage. Of specific interest to the team were policies and procedures regarding the upgrade and maintenance (to include system patching) of the command and control (C2) systems, including SCADA and EMS. The Policies and Procedures sub-team was also interested in the procedures for contingency operations and restoration of systems in the

event of a computer system failure, or a cyber event such as an active hack or the discovery of malicious code.

5. Supporting Infrastructure

The Supporting Infrastructure sub-team was led by a DHS expert with experience assessing supporting infrastructure elements such as water cooling for computer systems, back-up power systems, heating, ventilation and air conditioning (HVAC), and supporting telecommunications networks. Public Safety and Emergency Preparedness Canada was the Canadian co-lead for this effort. This team analyzed the integrity of the supporting infrastructure and its role, if any, in the power outage on August 14, 2003. It sought to determine whether the supporting infrastructure was performing at a satisfactory level leading up to and during the power outage of August 14, 2003. In addition, the team verified with vendors if there were maintenance issues that may have impacted operations prior to and during the outage.

The sub-team specifically focused on the following key issues in visits to each of the designated electrical entities:

1. Carrier/provider/vendor for the supporting infrastructure services and/or systems at select company facilities;
2. Loss of service before and/or after the power outage;
3. Conduct of maintenance activities before and/or after the power outage;
4. Conduct of installation activities before and/or after the power outage;
5. Conduct of testing activities before and/or after the power outage;
6. Conduct of exercises before and/or after the power outage; and
7. Existence of a monitoring process (log, checklist etc.) to document the status of supporting infrastructure services.

6. Root Cause Analysis

The SWG Root Cause Liaison Sub-Team (SWG/RC) followed the work of the ESWG to identify potential root causes of the power outage. As these root cause elements were identified, the sub-team assessed with the ESWG any potential linkages to physical and/or cyber malfeasance. The final analysis of the SWG/RC team found no causal link between the power outage and malicious activity, whether physical or cyber initiated.

Cyber Timeline

The following sequence of events was derived from discussions with representatives of FirstEnergy and the Midwest Independent System Operator (MISO). All times are approximate.

The first significant cyber-related event of August 14, 2003, occurred at 12:40 EDT at the MISO. At this time, a MISO EMS engineer purposely disabled the automatic periodic trigger on the State Estimator (SE) application, an application that allows MISO to determine the real-time state of the power system for its region. The disablement of the automatic periodic trigger, a program feature that causes the SE to run automatically every five minutes, is a necessary operating procedure when resolving a mismatched solution produced by the SE. The EMS engineer determined that the mismatch in the SE solution was due to the SE model depicting Cinergy's Bloomington-Denois Creek 230-kV line as being in service, when it had actually been out of service since 12:12 EDT.

At 13:00 EDT, after making the appropriate changes to the SE model and manually triggering the SE, the MISO EMS engineer achieved two valid solutions.

At 13:30 EDT, the MISO EMS engineer went to lunch. However, he forgot to re-engage the automatic periodic trigger.

At 14:14 EDT, FirstEnergy's "Alarm and Event Processing Routine," (AEPR) a key software program that gives grid operators visual and audible indications of events occurring on their portion of the grid, began to malfunction. FirstEnergy grid operators were unaware that the software was not functioning properly. This software did not become functional again until much later that evening.

At 14:40 EDT, an Ops Engineer discovered the SE was not solving and went to notify an EMS engineer that the SE was not solving.

At 14:41 EDT, FirstEnergy's server running the AEPR software failed to the backup server. Control room staff remained unaware that the AEPR software was not functioning properly.

At 14:44 EDT, a MISO EMS engineer, after being alerted by the Ops Engineer, re-activated the automatic periodic trigger and, for speed, manually triggered the program. However, the SE program again showed a mismatch.

At 14:54 EDT, FirstEnergy's backup server failed. AEPR continued to malfunction. The Area Control Error Calculations (ACE) and Strip Charting routines malfunctioned and the dispatcher user interface slowed significantly.

At 15:00 EDT, FirstEnergy used its emergency backup system to control the system and make ACE calculations. ACE calculations and control systems continued to run on the emergency backup system until roughly 15:08 EDT, when the primary server was restored.

At 15:05 EDT, FirstEnergy's Harding-Chamberlin 345-kV line tripped and locked out. FirstEnergy grid operators did not receive notification from the AEPR software which continued to malfunction, unbeknownst to the FirstEnergy grid operators.

At 15:08 EDT, using data obtained at roughly 15:04 EDT (it takes roughly five minutes for the SE to provide a result), the MISO EMS engineer concluded that the SE mismatched due to a line outage. His experience allowed him to isolate the outage to the Stuart-Atlanta 345-kV line (which tripped about an hour earlier at 14:02 EDT). He took the Stuart-Atlanta line out of service in the SE model and got a valid solution.

Also at 15:08 EDT, the FirstEnergy primary server was restored. ACE calculations and control systems were now running on the primary server. AEPR continued to malfunction, unbeknownst to the FirstEnergy grid operators.

At 15:09 EDT, the MISO EMS engineer went to the control room to tell the grid operators that he thought the Stuart-Atlanta line was out of service. Grid operators referred to their "Outage Scheduler" and informed the EMS Engineer that their data showed the Stuart-Atlanta line was "up" and that the EMS engineer should depict the line as in service in the SE model. At 15:17 EDT, the EMS engineer ran the SE with the Stuart-Atlanta line "live," but the model again mismatched.

At 15:29 EDT, the MISO EMS Engineer asked MISO grid operators to call PJM Interconnect, LLC to determine the status of the Stuart-Atlanta line. MISO was informed that the Stuart-Atlanta line tripped at 14:02 EDT. The EMS Engineer adjusted the model, which by this time had been updated with the 15:05 EDT Harding-Chamberlin 345-kV line trip, and came up with a valid solution.

At 15:32 EDT, FirstEnergy's Hanna-Juniper 345-kV line tripped and locked out. The AEPR continued to malfunction.

At 15:41 EDT, the lights flickered at the FirstEnergy's control facility. This occurred because they had lost grid power and switched over to their emergency power supply.

At 15:42 EDT, a FirstEnergy dispatcher realized that the AEPR was not working and made technical support staff aware of the problem.

Endnotes

[1] http://www.nrc.gov/reading-rm/doc-collections/news/2003/ 03-108.html.

[2] http://www.fbi.gov/congress/congress03/mefford090403.htm.

[3] http://www.fbi.gov/congress/congress03/mefford090403.htm.

10. Recommendations to Prevent or Minimize the Scope of Future Blackouts

Introduction

As reported in previous chapters, the blackout on August 14, 2003, was preventable. It had several direct causes and contributing factors, including:

- Failure to maintain adequate reactive power support
- Failure to ensure operation within secure limits
- Inadequate vegetation management
- Inadequate operator training
- Failure to identify emergency conditions and communicate that status to neighboring systems
- Inadequate regional-scale visibility over the bulk power system.

Further, as discussed in Chapter 7, after each major blackout in North America since 1965, an expert team of investigators has probed the causes of the blackout, written detailed technical reports, and issued lists of recommendations to prevent or minimize the scope of future blackouts. Yet several of the causes of the August 14 blackout are strikingly similar to those of the earlier blackouts. Clearly, efforts to implement earlier recommendations have not been adequate.[1] Accordingly, the recommendations presented below emphasize comprehensiveness, monitoring, training, and enforcement of reliability standards when necessary to ensure compliance.

It is useful to think of the recommendations presented below in terms of four broad themes:

1. Government bodies in the U.S. and Canada, regulators, the North American electricity industry, and related organizations should commit themselves to making adherence to high reliability standards paramount in the planning, design, and operation of North America's vast bulk power systems. Market mechanisms should be used where possible, but in circumstances where conflicts between reliability and commercial objectives cannot be reconciled, they must be resolved in favor of high reliability.[2]

2. Regulators and consumers should recognize that reliability is not free, and that maintaining it requires ongoing investments and operational expenditures by many parties. Regulated companies will not make such outlays without assurances from regulators that the costs will be recoverable through approved electric rates, and unregulated companies will not make such outlays unless they believe their actions will be profitable.[3]

3. Recommendations have no value unless they are implemented. Accordingly, the Task Force emphasizes strongly that North American governments and industry should commit themselves to working together to put into effect the suite of improvements mapped out below. Success in this area will require particular attention to the mechanisms proposed for performance monitoring, accountability of senior management, and enforcement of compliance with standards.

4. The bulk power systems are among the most critical elements of our economic and social infrastructure. Although the August 14 blackout was not caused by malicious acts, a number of security-related actions are needed to enhance reliability.

Over the past decade or more, electricity demand has increased and the North American interconnections have become more densely woven and heavily loaded, over more hours of the day and year. In many geographic areas, the number of single or multiple contingencies that could create serious problems has increased. Operating the

grids at higher loadings means greater stress on equipment and a smaller range of options and a shorter period of time for dealing with unexpected problems. The system operator's job has become more challenging, leading to the need for more sophisticated grid management tools and more demanding operator training programs and certification requirements.

The recommendations below focus on changes of many kinds that are needed to ensure reliability, for both the summer of 2004 and for the years to follow. Making these changes will require higher and broader awareness of the importance of reliability, and some of them may require substantial new investments. However, the cost of *not* making these changes, i.e., the cost of chronic large-scale blackouts, would be far higher than the cost of addressing the problem. Estimates of the cost of the August 14 blackout range between $4 and $10 billion (U.S.).[4]

The need for additional attention to reliability is not necessarily at odds with increasing competition and the improved economic efficiency it brings to bulk power markets. Reliability and economic efficiency can be compatible, but this outcome requires more than reliance on the laws of physics and the principles of economics. It requires sustained, focused efforts by regulators, policy makers, and industry leaders to strengthen and maintain the institutions and rules needed to protect both of these important goals. Regulators must ensure that competition does not erode incentives to comply with reliability requirements, and that reliability requirements do not serve as a smokescreen for noncompetitive practices.

The metric for gauging achievement of this goal—making the changes needed to maintain a high level of reliability for the next decade or longer—will be the degree of compliance obtained with the recommendations presented below. The single most important step in the United States is for the U.S. Congress to enact the reliability provisions in pending energy bills (H.R. 6 and S. 2095). If that can be done, many of the actions recommended below could be accomplished readily in the course of implementing the legislation.

Some commenters asserted that the Interim Report did not analyze all factors they believe may have contributed to the August 14 blackout. Implementation of the recommendations presented below will address all remaining issues, through the ongoing work of government bodies and agencies in the U.S. and Canada, the electricity industry, and the non-governmental institutions responsible for the maintenance of electric reliability in North America.

Recommendations

Forty-six numbered recommendations are presented below, grouped into four substantive areas. Some recommendations concern subjects that were addressed in some detail by commenters on the Interim Report or participants in the Task Force's two technical conferences. In such cases, the commenters are listed in the Endnotes section of this chapter. Citation in the endnotes does not necessarily mean that the commenter supports the position expressed in the recommendation. A "table of contents" overview of the recommendations is provided in the text box on pages 141-142.

Group I. Institutional Issues Related to Reliability

1. Make reliability standards mandatory and enforceable, with penalties for noncompliance.[5]

Appropriate branches of government in the United States and Canada should take action as required to make reliability standards mandatory and enforceable, and to provide appropriate penalties for noncompliance.

A. Action by the U.S. Congress

The U.S. Congress should enact reliability legislation no less stringent than the provisions now included in the pending comprehensive energy bills, H.R. 6 and S. 2095. Specifically, these provisions would require that:

- Reliability standards are to be mandatory and enforceable, with penalties for noncompliance.
- Reliability standards should be developed by an independent, international electric reliability organization (ERO) with fair stakeholder representation in the selection of its directors and balanced decision-making in any ERO committee or subordinate organizational structure. (See text box on NERC and an ERO below.)

Overview of Task Force Recommendations: Titles Only

Group I. Institutional Issues Related to Reliability

1. Make reliability standards mandatory and enforceable, with penalties for noncompliance.
2. Develop a regulator-approved funding mechanism for NERC and the regional reliability councils, to ensure their independence from the parties they oversee.
3. Strengthen the institutional framework for reliability management in North America.
4. Clarify that prudent expenditures and investments for bulk system reliability (including investments in new technologies) will be recoverable through transmission rates.
5. Track implementation of recommended actions to improve reliability.
6. FERC should not approve the operation of new RTOs or ISOs until they have met minimum functional requirements.
7. Require any entity operating as part of the bulk power system to be a member of a regional reliability council if it operates within the council's footprint.
8. Shield operators who initiate load shedding pursuant to approved guidelines from liability or retaliation.
9. Integrate a "reliability impact" consideration into the regulatory decision-making process.
10. Establish an independent source of reliability performance information.
11. Establish requirements for collection and reporting of data needed for post-blackout analyses.
12. Commission an independent study of the relationships among industry restructuring, competition, and reliability.
13. DOE should expand its research programs on reliability-related tools and technologies.
14. Establish a standing framework for the conduct of future blackout and disturbance investigations.

Group II. Support and Strengthen NERC's Actions of February 10, 2004

15. Correct the direct causes of the August 14, 2003 blackout.
16. Establish enforceable standards for maintenance of electrical clearances in right-of-way areas.
17. Strengthen the NERC Compliance Enforcement Program.
18. Support and strengthen NERC's Reliability Readiness Audit Program.
19. Improve near-term and long-term training and certification requirements for operators, reliability coordinators, and operator support staff.
20. Establish clear definitions for *normal, alert* and *emergency* operational system conditions. Clarify roles, responsibilities, and authorities of reliability coordinators and control areas under each condition.
21. Make more effective and wider use of system protection measures.
22. Evaluate and adopt better real-time tools for operators and reliability coordinators.
23. Strengthen reactive power and voltage control practices in all NERC regions.
24. Improve quality of system modeling data and data exchange practices.
25. NERC should reevaluate its existing reliability standards development process and accelerate the adoption of enforceable standards.
26. Tighten communications protocols, especially for communications during alerts and emergencies. Upgrade communication system hardware where appropriate.
27. Develop enforceable standards for transmission line ratings.
28. Require use of time-synchronized data recorders.
29. Evaluate and disseminate lessons learned during system restoration.
30. Clarify criteria for identification of operationally critical facilities, and improve dissemination of updated information on unplanned outages.
31. Clarify that the transmission loading relief (TLR) process should not be used in situations involving an actual violation of an Operating Security Limit. Streamline the TLR process.

(continued on page 142)

Overview of Task Force Recommendations: Titles Only (Continued)

Group III. Physical and Cyber Security of North American Bulk Power Systems

32. Implement NERC IT standards.
33. Develop and deploy IT management procedures.
34. Develop corporate-level IT security governance and strategies.
35. Implement controls to manage system health, network monitoring, and incident management.
36. Initiate U.S.-Canada risk management study.
37. Improve IT forensic and diagnostic capabilities.
38. Assess IT risk and vulnerability at scheduled intervals.
39. Develop capability to detect wireless and remote wireline intrusion and surveillance.
40. Control access to operationally sensitive equipment.
41. NERC should provide guidance on employee background checks.
42. Confirm NERC ES-ISAC as the central point for sharing security information and analysis.
43. Establish clear authority for physical and cyber security.
44. Develop procedures to prevent or mitigate inappropriate disclosure of information.

Group IV. Canadian Nuclear Power Sector

45. The Task Force recommends that the Canadian Nuclear Safety Commission request Ontario Power Generation and Bruce Power to review operating procedures and operator training associated with the use of adjuster rods.
46. The Task Force recommends that the Canadian Nuclear Safety Commission purchase and install backup generation equipment.

- Reliability standards should allow, where appropriate, flexibility to accommodate regional differences, including more stringent reliability requirements in some areas, but regional deviations should not be allowed to lead to lower reliability expectations or performance.
- An ERO-proposed standard or modification to a standard should take effect within the United States upon approval by the Federal Energy Regulatory Commission (FERC).
- FERC should remand to the ERO for further consideration a proposed reliability standard or a modification to a reliability standard that it disapproves of in whole or in part, with explanation for its concerns and rationale.

B. Action by FERC

In the absence of such reliability legislation, FERC should review its statutory authorities under existing law, and to the maximum extent permitted by those authorities, act to enhance reliability by making compliance with reliability standards enforceable in the United States. In doing so, FERC should consult with state regulators, NERC, and the regional reliability councils to determine whether certain enforcement practices now in use in some parts of the U.S. and Canada might be applied more broadly. For example, in the Western U.S. and Canada, many members of the Western Electricity Coordinating Council (WECC) include clauses in contracts for the purchase of wholesale power that require the parties to comply with reliability standards. In the areas of the U.S. and Canada covered by the Northeast Power Coordinating Council (NPCC), parties found not to be in compliance with NERC and NPCC reliability requirements are subject to escalating degrees of scrutiny by their peers and the public. Both of these approaches have had positive effects. FERC should examine other approaches as well, and work with state regulatory authorities to ensure

NERC and the ERO

If the proposed U.S. reliability legislation passes, the North American Electric Reliability Council (NERC) may undertake various organizational changes and seek recognition as the electric reliability organization (ERO) called for in H.R. 6 and S. 2095. For simplicity of presentation, the many forward-looking references below to "NERC" are intended to apply to the ERO if the legislation is passed, and to NERC if the legislation is not passed.

that any other appropriate actions to make reliability standards enforceable are taken.

Action by FERC under its existing authorities would not lessen the need for enactment of reliability legislation by the Congress. Many U.S. parties that should be required by law to comply with reliability requirements are not subject to the Commission's full authorities under the Federal Power Act.

C. Action by Appropriate Authorities in Canada

The interconnected nature of the transmission grid requires that reliability standards be identical or compatible on both sides of the Canadian/U.S. border. Several provincial governments in Canada have already demonstrated support for mandatory and enforceable reliability standards and have either passed legislation or have taken steps to put in place the necessary framework for implementing such standards in Canada. The federal and provincial governments should work together and with appropriate U.S. authorities to complete a framework to ensure that identical or compatible standards apply in both countries, and that means are in place to enforce them in all interconnected jurisdictions.

D. Joint Actions by U.S. and Canadian Governments

International coordination mechanisms should be developed between the governments in Canada and the United States to provide for government oversight of NERC or the ERO, and approval and enforcement of reliability standards.

E. Memoranda of Understanding between U.S. or Canadian Government Agencies and NERC

Government agencies in both countries should decide (individually) whether to develop a memorandum of understanding (MOU) with NERC that would define the agency's working relationship with NERC, government oversight of NERC activities if appropriate, and the reliability responsibilities of the signatories.

2. Develop a regulator-approved mechanism for funding NERC and the regional reliability councils, to ensure their independence from the parties they oversee.[6]

U.S. and Canadian regulatory authorities should work with NERC, the regional councils, and the industry to develop and implement a new funding mechanism for NERC and the regional councils based on a surcharge in transmission rates. The purpose would be to ensure that NERC and the councils are appropriately funded to meet their changing responsibilities without dependence on the parties that they oversee. Note: Implementation of this recommendation should be coordinated with the review called for in Recommendation 3 concerning the future role of the regional councils.

NERC's current $13 million/year budget is funded as part of the dues that transmission owners, generators, and other market participants pay to the ten regional reliability councils, which then fund NERC. This arrangement makes NERC subject to the influence of the reliability councils, which are in turn subject to the influence of their control areas and other members. It also compromises the independence of both NERC and the councils in relation to the entities whose actions they oversee, and makes it difficult for them to act forcefully and objectively to maintain the reliability of the North American bulk power system. Funding NERC and the councils through a transmission rate surcharge administered and disbursed under regulatory supervision would enable the organizations to be more independent of the industry, with little impact on electric bills. The dues that companies pay to the regional councils are passed through to electricity customers today, so the net impacts on customer bills from shifting to a rate surcharge would be minimal.

Implementation of the recommendations presented in this report will involve a substantial increase in NERC's functions and responsibilities, and require an increase in NERC's annual budget. The additional costs, however, would be small in comparison to the cost of a single major blackout.

3. Strengthen the institutional framework for reliability management in North America.[7]

FERC, DOE and appropriate authorities in Canada should work with the states, NERC, and the industry, to evaluate and develop appropriate modifications to the existing institutional framework for reliability management. In particular, the affected government agencies should:

A. Commission an independent review by qualified experts in organizational design and management to address issues concerning how best to structure an international reliability organization for the long term.

B. Based in part on the results of that review, develop metrics for gauging the adequacy of NERC's performance, and specify the functions of the NERC Board of Trustees and the procedure for selecting the members of the Board.

C. Examine and clarify the future role of the regional reliability councils, with particular attention to their mandate, scope, structure, responsibilities, and resource requirements.

D. Examine NERC's proposed Functional Model and set minimum requirements under which NERC would certify applicants' qualifications to perform critical functions.

E. Request NERC and the regional councils to suspend designation of any new control areas (or sub-control areas) until the minimum requirements in section D (above) have been established, unless an applicant shows that such designation would significantly enhance reliability.

F. Determine ways to enhance reliability operations in the United States through simplified organizational boundaries and resolution of seams issues.

A and B. Reshaping NERC

The far-reaching organizational changes in the North American electricity industry over the past decade have already induced major changes in the nature of NERC as an organization. However, the process of change at NERC is far from complete. Important additional changes are needed such as the shift to enforceable standards, development of an effective monitoring capability, and funding that is not dependent on the industry. These changes will strengthen NERC as an organization. In turn, to properly serve overarching public policy concerns, this strengthening of NERC's capabilities will have to be balanced with increased government oversight, more specific metrics for gauging NERC's performance as an organization, and greater transparency concerning the functions of its senior management team (including its Board of Trustees) and the procedures by which those individuals are selected. The affected government agencies should jointly commission an independent review of these and related issues to aid them in making their respective decisions.

C. The Role of the Regional Reliability Councils

North America's regional reliability councils have evolved into a disparate group of organizations with varying responsibilities, expertise, roles, sizes and resources. Some have grown from a reliability council into an ISO or RTO (ERCOT and SPP), some span less than a single state (FRCC and ERCOT) while others cover many states and provinces and cross national boundaries (NPCC and WECC). Several cross reliability coordinator boundaries. It is time to evaluate the appropriate size and scope of a regional council, the specific tasks that it should perform, and the appropriate level of resources, expertise, and independence that a regional reliability council needs to perform those tasks effectively. This evaluation should also address whether the councils as currently constituted are appropriate to meet future reliability needs.

D. NERC's Functional Model

The transition to competition in wholesale power markets has been accompanied by increasing diversity in the kinds of entities that need to be in compliance with reliability standards. Rather than resist or attempt to influence this evolution, NERC's response—through the Functional Model—has been to seek a means of enabling reliability to be maintained under virtually any institutional framework. The Functional Model identifies sixteen basic functions associated with operating the bulk electric systems and maintaining reliability, and the capabilities that an organization must have in order to perform a given function. (See Functional Model text box below.)

NERC acknowledges that maintaining reliability in some frameworks may be more difficult or more expensive than in others, but it stresses that as long as some responsible party addresses each function and the rules are followed, reliability will be preserved. By implication, the pros and cons of alternative institutional frameworks in a given region—which may affect aspects of electric industry operations other than reliability—are matters for government agencies to address, not NERC.

One of the major purposes of the Functional Model is to create a vehicle through which NERC will be able to identify an entity responsible for performing each function in every part of the three North American interconnections. NERC considers four of the sixteen functions to be especially critical for reliability. For these functions, NERC intends, upon application by an entity, to review the entity's capabilities, and if appropriate, certify that the entity has the qualifications to perform that function within the specified geographic area. For the other twelve functions, NERC proposes to

"register" entities as responsible for a given function in a given area, upon application.

All sixteen functions are presently being performed to varying degrees by one entity or another today in all areas of North America. Frequently an entity performs a combination of functions, but there is great variety from one region to another in how the functions are bundled and carried out. Whether all of the parties who are presently performing the four critical functions would meet NERC's requirements for certification is not known, but the proposed process provides a means of identifying any weaknesses that need to be rectified.

At present, after protracted debate, the Functional Model appears to have gained widespread but cautious support from the diverse factions across the industry, while the regulators have not taken a position. In some parts of North America, such as the Northeast, large regional organizations will probably be certified to perform all four of the critical functions for their respective areas. In other areas, capabilities may remain less aggregated, and the institutional structure may remain more complex.

Sixteen Functions in NERC's Functional Model

- **Operating Reliability**
- **Planning Reliability**
- **Balancing** (generation and demand)
- **Interchange**
- Transmission service
- Transmission ownership
- Transmission operations
- Transmission planning
- Resource planning
- Distribution
- Generator ownership
- Generator operations
- Load serving
- Purchasing and selling
- Standards development
- Compliance monitoring

NERC regards the four functions shown above in bold as especially critical to reliability. Accordingly, it proposes to certify applicants that can demonstrate that they have the capabilities required to perform those functions. The Operating Reliability authority would correspond to today's reliability coordinator, and the Balancing authority to today's control area operator.

Working with NERC and the industry, FERC and authorities in Canada should review the Functional Model to ensure that operating hierarchies and entities will facilitate, rather than hinder, efficient reliability operations. At a minimum, the review should identify ways to eliminate inappropriate commercial incentives to retain control area status that do not support reliability objectives; address operational problems associated with institutional fragmentation; and set minimum requirements with respect to the capabilities requiring NERC certification, concerning subjects such as:

1. Fully operational backup control rooms.
2. System-wide (or wider) electronic map boards or functional equivalents, with data feeds that are independent of the area's main energy management system (EMS).
3. Real-time tools that are to be available to the operator, with backups. (See Recommendation 22 below for more detail concerning minimum requirements and guidelines for real-time operating tools.)
4. SCADA and EMS requirements, including backup capabilities.
5. Training programs for all personnel who have access to a control room or supervisory responsibilities for control room operations. (See Recommendation 19 for more detail on the Task Force's views regarding training and certification requirements.)
6. Certification requirements for control room managers and staff.

E. Designation of New Control Areas

Significant changes in the minimum functional requirements for control areas (or balancing authorities, in the context of the Functional Model) may result from the review called for above. Accordingly, the Task Force recommends that regulatory authorities should request NERC and the regional councils not to certify any new control areas (or sub-control areas) until the appropriate regulatory bodies have approved the minimum functional requirements for such bodies, unless an applicant shows that such designation would significantly enhance reliability.

F. Boundary and Seam Issues and Minimum Functional Requirements

Some observers believe that some U.S. regions have too many control areas performing one or more of the four critical reliability functions. In many cases, these entities exist to retain commercial advantages associated with some of these functions. The resulting institutional fragmentation and decentralization of control leads to a higher number of operating contacts and seams, complex coordination requirements, misalignment of control areas with other electrical boundaries and/or operating hierarchies, inconsistent practices and tools, and increased compliance monitoring requirements. These consequences hamper the efficiency and reliability of grid operations.

As shown above (text box on page 14), MISO, as reliability coordinator for its region, is responsible for dealing with 37 control areas, whereas PJM now spans 9 control areas, ISO-New England has 2, and the New York ISO, Ontario's IMO, Texas' ERCOT, and Québec's Trans-Energie are themselves the control area operators for their respective large areas. Moreover, it is not clear that small control areas are financially able to provide the facilities and services needed to perform control area functions at the level needed to maintain reliability. This concern applies also to the four types of entities that NERC proposes to certify under the Functional Model (i.e., Reliability Authority, Planning Authority, Balancing Authority, and Interchange Authority).

For the long term, the regulatory agencies should continue to seek ways to ensure that the regional operational frameworks that emerge through the implementation of the Functional Model promote reliable operations. Any operational framework will represent some combination of tradeoffs, but reliability is a critically important public policy objective and should be a primary design criterion.

4. Clarify that prudent expenditures and investments for bulk system reliability (including investments in new technologies) will be recoverable through transmission rates.[8]

FERC and appropriate authorities in Canada should clarify that prudent expenditures and investments by regulated companies to maintain or improve bulk system reliability will be recoverable through transmission rates.

In the U.S., FERC and DOE should work with state regulators to identify and resolve issues related to the recovery of reliability costs and investments through retail rates. Appropriate authorities in Canada should determine whether similar efforts are warranted.

Companies will not make the expenditures and investments required to maintain or improve the reliability of the bulk power system without credible assurances that they will be able to recover their costs.

5. Track implementation of recommended actions to improve reliability.[9]

In the requirements issued on February 10, 2004, NERC announced that it and the regional councils would 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. The regions are to report on a quarterly basis to NERC.

In addition, NERC intends to initiate by January 1, 2005 a reliability performance monitoring function that will evaluate and report on trends in bulk electric system reliability performance.

The Task Force supports these actions strongly. However, many of the Task Force's recommendations pertain to government bodies as well as NERC. Accordingly:

A. Relevant agencies in the U.S. and Canada should cooperate to establish mechanisms for tracking and reporting to the public on implementation actions in their respective areas of responsibility.

B. NERC should draw on the above-mentioned quarterly reports from its regional councils to prepare annual reports to FERC, appropriate authorities in Canada, and the public on the status of the industry's compliance with recommendations and important trends in electric system reliability performance.

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

confirming that the lessons and recommendations from earlier blackouts had not been adequately implemented, at least in some geographic areas. Accordingly, parallel and coordinated efforts are needed by the relevant government agencies and NERC to track the implementation of recommendations by governments and the electricity industry. WECC and NPCC have already established programs that could serve as models for tracking implementation of recommendations.

6. FERC should not approve the operation of a new RTO or ISO until the applicant has met the minimum functional requirements for reliability coordinators.

The events of August 14 confirmed that MISO did not yet have all of the functional capabilities required to fulfill its responsibilities as reliability coordinator for the large area within its footprint. FERC should not authorize a new RTO or ISO to become operational until the RTO or ISO has verified that all critical reliability capabilities will be functional upon commencement of RTO or ISO operations.

7. Require any entity operating as part of the bulk power system to be a member of a regional reliability council if it operates within the council's footprint.[10]

The Task Force recommends that FERC and appropriate authorities in Canada be empowered through legislation, if necessary, to require all entities that operate as part of the bulk electric system to certify that they are members of the regional reliability council for all NERC regions in which they operate.

This requirement is needed to ensure that all relevant parties are subject to NERC standards, policies, etc., in all NERC regions in which they operate. Action by the Congress or legislative bodies in Canada may be necessary to provide appropriate authority.

8. Shield operators who initiate load shedding pursuant to approved guidelines from liability or retaliation.[11]

Legislative bodies and regulators should: 1) establish that operators (whether organizations or individuals) who initiate load shedding pursuant to operational guidelines are not subject to liability suits; and 2) affirm publicly that actions to shed load pursuant to such guidelines are not indicative of operator failure.

Timely and sufficient action to shed load on August 14 would have prevented the spread of the blackout beyond northern Ohio. NERC has directed all the regional councils in all areas of North America to review the applicability of plans for under-voltage load shedding, and to support the development of such capabilities where they would be beneficial. However, organizations and individual operators may hesitate to initiate such actions in appropriate circumstances without assurances that they will not be subject to liability suits or other forms of retaliation, provided their action is pursuant to previously approved guidelines.

9. Integrate a "reliability impact" consideration into the regulatory decision-making process.[12]

The Task Force recommends that FERC, appropriate authorities in Canada, and state regulators integrate a formal reliability impact consideration into their regulatory decision-making to ensure that their actions or initiatives either improve or at minimum do no harm to reliability.

Regulatory actions can have unintended consequences. For example, in reviewing proposed utility company mergers, FERC's primary focus has been on financial and rate issues, as opposed to the reliability implications of such mergers. To minimize unintended harm to reliability, and aid the improvement of reliability where appropriate, the Task Force recommends that regulators incorporate a formal reliability impact consideration into their decision processes. At the same time, regulators should be watchful for use of alleged reliability impacts as a smokescreen for anti-competitive or discriminatory behavior.

10. Establish an independent source of reliability performance information.[13]

The U.S. Department of Energy's Energy Information Administration (EIA), in coordination with other interested agencies and data sources (FERC, appropriate Canadian government agencies, NERC, RTOs, ISOs, the regional councils, transmission operators, and generators) should establish common definitions and information collection standards. If the necessary resources can be identified, EIA should expand its current activities to include information on reliability performance.

Energy policy makers and a wide range of economic decision makers need objective, factual information about basic trends in reliability performance. EIA and the other organizations cited above should identify information gaps in federal data collections covering reliability performance and physical characteristics. Plans to fill those gaps should be developed, and the associated resource requirements determined. Once those resources have been acquired, EIA should publish information on trends, patterns, costs, etc. related to reliability performance.

11. Establish requirements for collection and reporting of data needed for post-blackout analyses.

FERC and appropriate authorities in Canada should require generators, transmission owners, and other relevant entities to collect and report data that may be needed for analysis of blackouts and other grid-related disturbances.

The investigation team found that some of the data needed to analyze the August 14 blackout fully was not collected at the time of the events, and thus could not be reported. Some of the data that was reported was based on incompatible definitions and formats. As a result, there are aspects of the blackout, particularly concerning the evolution of the cascade, that may never be fully explained. FERC, EIA and appropriate authorities in Canada should consult with NERC, key members of the investigation team, and the industry to identify information gaps, adopt common definitions, and establish filing requirements.

12. Commission an independent study of the relationships among industry restructuring, competition, and reliability.[14]

DOE and Natural Resources Canada should commission an independent study of the relationships among industry restructuring, competition in power markets, and grid reliability, and how those relationships should be managed to best serve the public interest.

Some participants at the public meetings held in Cleveland, New York and Toronto to review the Task Force's Interim Report expressed the view that the restructuring of electricity markets for competition in many jurisdictions has, itself, increased the likelihood of major supply interruptions. Some of these commenters assert that the transmission system is now being used to transmit power over distances and at volumes that were not envisioned when the system was designed, and that this functional shift has created major risks that have not been adequately addressed. Indeed, some commenters believe that restructuring was a major cause of the August 14 blackout.

The Task Force believes that the Interim Report accurately identified the primary causes of the blackout. It also believes that had existing reliability requirements been followed, either the disturbance in northern Ohio that evolved on August 14 into a blackout would not have occurred, or it would have been contained within the FE control area.

Nevertheless, as discussed at the beginning of this chapter, the relationship between competition in power markets and reliability is both important and complex, and careful management and sound rules are required to achieve the public policy goals of reasonable electricity prices and high reliability. At the present stage in the evolution of these markets, it is worthwhile for DOE and Natural Resources Canada (in consultation with FERC and the Canadian Council of Energy Ministers) to commission an independent expert study to provide advice on how to achieve and sustain an appropriate balance in this important area.

Among other things, this study should take into account factors such as:

- Historical and projected load growth
- Location of new generation in relation to old generation and loads
- Zoning and NIMBY[15] constraints on siting of generation and transmission
- Lack of new transmission investment and its causes
- Regional comparisons of impact of wholesale electric competition on reliability performance and on investments in reliability and transmission
- The financial community's preferences and their effects on capital investment patterns
- Federal vs. state jurisdictional concerns
- Impacts of state caps on retail electric rates
- Impacts of limited transmission infrastructure on energy costs, transmission congestion, and reliability

- Trends in generator fuel and wholesale electricity prices
- Trends in power flows, line losses, voltage levels, etc.

13. DOE should expand its research programs on reliability-related tools and technologies.[16]

DOE should expand its research agenda, and consult frequently with Congress, FERC, NERC, state regulators, Canadian authorities, universities, and the industry in planning and executing this agenda.

More investment in research is needed to improve grid reliability, with particular attention to improving the capabilities and tools for system monitoring and management. Research on reliability issues and reliability-related technologies has a large public-interest component, and government support is crucial. DOE already leads many research projects in this area, through partnerships with industry and research under way at the national laboratories and universities. DOE's leadership and frequent consultation with many parties are essential to ensure the allocation of scarce research funds to urgent projects, bring the best talent to bear on such projects, and enhance the dissemination and timely application of research results.

Important areas for reliability research include but are not limited to:

- Development of practical real-time applications for wide-area system monitoring using phasor measurements and other synchronized measuring devices, including post-disturbance applications.
- Development and use of enhanced techniques for modeling and simulation of contingencies, blackouts, and other grid-related disturbances.
- Investigation of protection and control alternatives to slow or stop the spread of a cascading power outage, including demand response initiatives to slow or halt voltage collapse.
- Re-evaluation of generator and customer equipment protection requirements based on voltage and frequency phenomena experienced during the August 14, 2003, cascade.
- Investigation of protection and control of generating units, including the possibility of multiple steps of over-frequency protection and possible effects on system stability during major disturbances.
- Development of practical human factors guidelines for power system control centers.
- Study of obstacles to the economic deployment of demand response capability and distributed generation.
- Investigation of alternative approaches to monitoring right-of-way vegetation management.
- Study of air traffic control, the airline industry, and other relevant industries for practices and ideas that could reduce the vulnerability of the electricity industry and its reliability managers to human error.

Cooperative and complementary research and funding between nations and between government and industry efforts should be encouraged.

14. Establish a standing framework for the conduct of future blackout and disturbance investigations.[17]

The U.S., Canadian, and Mexican governments, in consultation with NERC, should establish a standing framework for the investigation of future blackouts, disturbances, or other significant grid-related incidents.

Fortunately, major blackouts are not frequent, which makes it important to study such events carefully to learn as much as possible from the experience. In the weeks immediately after August 14, important lessons were learned pertaining not only to preventing and minimizing future blackouts, but also to the efficient and fruitful investigation of future grid-related events.

Appropriate U.S., Canadian, and Mexican government agencies, in consultation with NERC and other organizations, should prepare an agreement that, among other considerations:

- Establishes criteria for determining when an investigation should be initiated.
- Establishes the composition of a task force to provide overall guidance for the inquiry. The task force should be international if the triggering event had international consequences.
- Provides for coordination with state and provincial governments, NERC and other appropriate entities.

- Designates agencies responsible for issuing directives concerning preservation of records, provision of data within specified periods to a data warehouse facility, conduct of onsite interviews with control room personnel, etc.
- Provides guidance on confidentiality of data.
- Identifies types of expertise likely to be needed on the investigation team.

Group II. Support and Strengthen NERC's Actions of February 10, 2004

On February 10, 2004, after taking the findings of the Task Force's investigation into the August 14, 2003, blackout into account, the NERC Board of Trustees approved a series of actions and strategic and technical initiatives intended to protect the reliability of the North American bulk electric system. (See Appendix D for the full text of the Board's statement of February 10.) Overall, the Task Force supports NERC's actions and initiatives strongly. On some subjects, the Task Force advocates additional measures, as shown in the next 17 recommendations.

15. Correct the direct causes of the August 14, 2003 blackout.[18]

NERC played an important role in the Task Force's blackout investigation, and as a result of the findings of the investigation, NERC issued directives on February 10, 2004 to FirstEnergy, MISO, and PJM to complete a series of remedial actions by June 30, 2004 to correct deficiencies identified as factors contributing to the blackout of August 14, 2003. (For specifics on the actions required by NERC, see Appendix D.)

The Task Force supports and endorses NERC's near-term requirements strongly. It recommends the addition of requirements pertaining to ECAR, and several other additional elements, as described below.

A. Corrective Actions to Be Completed by FirstEnergy by June 30, 2004

The full text of the remedial actions NERC has required that FirstEnergy (FE) complete by June 30 is provided in Appendix D. The Task Force recommends the addition of certain elements to these requirements, as described below.

1. Examination of Other FE Service Areas

The Task Force's investigation found severe reactive power and operations criteria deficiencies in the Cleveland-Akron area.

NERC:

Specified measures required in that area to help ensure the reliability of the FE system and avoid undue risks to neighboring systems. However, the blackout investigation did not examine conditions in FE service areas in other states.

Task Force:

Recommends that NERC require FE to review its entire service territory, in all states, to determine whether similar vulnerabilities exist and require prompt attention. This review should be completed by June 30, 2004, and the results reported to FERC, NERC, and utility regulatory authorities in the affected states.

2. Interim Voltage Criteria

NERC:

Required that FE, consistent with or as part of a study ordered by FERC on December 24, 2003,[19] determine the minimum acceptable location-specific voltages at all 345 kV and 138 kV buses and all generating stations within the FE control area (including merchant plants). Further, FE is to 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.[20] Criteria and minimum voltage requirements must comply with NERC planning criteria, including Table 1A, Category C3, and Operating Policy 2.[21]

Task Force:

Recommends that NERC appoint a team, joined by representatives from FERC and the Ohio Public Utility Commission, to review and approve all such criteria.

3. FE Actions Based on FERC-Ordered Study

NERC:

Required that 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 reinforcement, FE is to develop a plan for developing such resources as soon as practical and develop operational procedures or other mitigating programs to maintain safe operating conditions until such time that the necessary system reinforcements can be made.

Task Force:

Recommends that a team appointed by NERC and joined by representatives from FERC and the Ohio Public Utility Commission should review and approve this plan.

4. Reactive Resources

NERC:

Required that FE inspect all reactive resources, including generators, and ensure that all are fully operational. FE is also required to verify that all installed capacitors have no blown fuses and that at least 98% of installed capacitors (69 kV and higher) are available for service during the summer of 2004.

Task Force:

Recommends that NERC also require FE to confirm that all non-utility generators in its area have entered into contracts for the sale of generation committing them to producing increased or maximum reactive power when called upon by FE or MISO to do so. Such contracts should ensure that the generator would be compensated for revenue losses associated with a reduction in real power sales in order to increase production of reactive power.

5. Operational Preparedness and Action Plan

NERC:

Required that FE prepare and submit to ECAR an Operational Preparedness and Action Plan to ensure system security and full compliance with NERC and planning and operating criteria, including ECAR Document 1.

Task Force:

Recommends that NERC require copies of this plan to be provided to FERC, DOE, the Ohio Public Utility Commission, and the public utility commissions in other states in which FE operates. The Task Force also recommends that NERC require FE to invite its system operations partners—control areas adjacent to FE, plus MISO, ECAR, and PJM—to participate in the development of the plan and agree to its implementation in all aspects that could affect their respective systems and operations.

6. Emergency Response Resources

NERC:

Required that FE develop a capability to reduce load in the Cleveland-Akron area by 1500 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 1500 MW of reduction in ten minutes without adversely affecting other interconnected systems. The amount of required load reduction capability may be modified to an amount shown by the FERC-ordered study to be sufficient for response to severe contingencies *and* if approved by ECAR and NERC.

Task Force:

Recommends that NERC require MISO's approval of any change in the amount of required load reduction capability. It also recommends that NERC require FE's load reduction plan to be shared with the Ohio Public Utilities Commission and that FE should communicate with all communities in the affected areas about the plan and its potential consequences.

7. Emergency Response Plan

NERC:

Required that FE develop an emergency response plan, including arrangements for deploying the load reduction capabilities noted above. The plan is to include criteria for determining the existence of an emergency and identify various possible states of emergency. The plan is to include detailed operating procedures and communication protocols with all the relevant entities including MISO, FE operators, and market participants within the FE area that have an ability to vary generation output or shed load upon orders from FE operators. The plan should include procedures for load restoration after the declaration that the FE system is no longer in an emergency operating state.

Task Force:

Recommends that NERC require FE to offer its system operations partners—i.e., control areas adjacent to FE, plus MISO, ECAR, and PJM—an opportunity to contribute to the development of the plan and agree to its key provisions.

8. Operator Communications

NERC:

Required that FE 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 should allow control room staff to focus on reliable system operations and avoid distractions such as calls from customers and others who are not responsible for operation of a portion of the transmission system.

Task Force:

Recommends that NERC require these procedures to be shared with and agreed to by control areas adjacent to FE, plus MISO, ECAR, and PJM, and any other affected system operations partners, and that these procedures be tested in a joint drill.

9. Reliability Monitoring and System Management Tools

NERC:

Required that FE ensure that its state estimator and real-time contingency analysis functions are used to execute reliably full contingency analyses automatically every ten minutes or on demand, and used to notify operators of potential first contingency violations.

Task Force:

Recommends that NERC also require FE to ensure that its information technology support function does not change the effectiveness of reliability monitoring or management tools in any way without the awareness and consent of its system operations staff.

10. GE XA21 System Updates and Transition to New Energy Management System

NERC:

Required that until FE replaces its GE XA21 Energy Management System, FE should implement all current known fixes for the GE XA21 system necessary to ensure reliable and stable operation of critical reliability functions, and particularly to correct the alarm processor failure that occurred on August 14, 2003.

Task Force:

Recommends that NERC require FE to design and test the transition to its planned new energy management system to ensure that the system functions effectively, that the transition is made smoothly, that the system's operators are adequately trained, and that all operating partners are aware of the transition.

11. Emergency Preparedness Training for Operators

NERC:

Required that all reliability coordinators, control areas, and transmission operators provide at least five days of training and drills using realistic simulation of system emergencies 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. The term "realistic simulation" 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.

Task Force:

Recommends that to provide effective training before June 30, 2004, NERC should require FE to consider seeking the assistance of another control area or reliability coordinator known to have a quality training program (such as IMO or ISO-New England) to provide the needed training with appropriate FE-specific modifications.

B. Corrective Actions to be Completed by MISO by June 30, 2004

1. Reliability Tools

NERC:

Required that MISO fully implement and test its topology processor to provide its operating personnel a 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 and voltage violations. MISO is to establish a means of exchanging outage information with its members and adjacent systems such that the MISO state estimator has accurate and timely information to perform as designed. MISO is to 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 is to provide backup capability for all functions critical to reliability.

Task Force:

Recommends that NERC require MISO to ensure that its information technology support staff does not change the effectiveness of reliability monitoring or management tools in any way without the awareness and consent of its system operations staff.

2. Operating Agreements

NERC:

Required that MISO 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.

Task Force:

Recommends that NERC require that any problems or concerns related to these operating issues be raised promptly with FERC and MISO's members for resolution.

C. Corrective Actions to be Completed by PJM by June 30, 2004

NERC:

Required that PJM reevaluate and improve its communications protocols and procedures between PJM and its neighboring control areas and reliability coordinators.

Task Force:

Recommends that NERC require definitions and usages of key terms be standardized, and non-essential communications be minimized during disturbances, alerts, or emergencies. NERC should also require PJM, MISO, and their member companies to conduct one or more joint drills using the new communications procedures.

D. Task Force Recommendations for Corrective Actions to be Completed by ECAR by August 14, 2004

1. Modeling and Assessments

Task Force:

Recommends that NERC require ECAR to reevaluate its modeling procedures, assumptions, scenarios and data for seasonal assessments and extreme conditions evaluations. ECAR should consult with an expert team appointed by NERC—joined by representatives from FERC, DOE, interested state commissions, and MISO—to develop better modeling procedures and scenarios, and obtain review of future assessments by the expert team.

2. Verification of Data and Assumptions

Task Force:

Recommends that NERC require ECAR to reexamine and validate all data and model assumptions against current physical asset capabilities and match modeled assets (such as line characteristics and ratings, and generator reactive power output capabilities) to current operating study assessments.

3. Ensure Consistency of Members' Data

Task Force:

Recommends that NERC require ECAR to conduct a data validation and exchange exercise to be sure that its members are using accurate, consistent, and current physical asset characteristics and capabilities for both long-term and seasonal assessments and operating studies.

E. Task Force Recommendation for Corrective Actions to be Completed by Other Parties by June 30, 2004

Task Force:

Recommends that NERC require each North American reliability coordinator, reliability council, control area, and transmission company not directly addressed above to review the actions required above and determine whether it has adequate system facilities, operational procedures, tools, and training to ensure reliable operations for the summer of 2004. If any entity finds that improvements are needed, it should immediately undertake the needed improvements, and coordinate them with its neighbors and partners as necessary.

The Task Force also recommends that FERC and government agencies in Canada require all entities under their jurisdiction who are users of GE/Harris XA21 Energy Management Systems to consult the vendor and ensure that appropriate actions have been taken to avert any recurrence of the malfunction that occurred on FE's system on August 14.

16. Establish enforceable standards for maintenance of electrical clearances in right-of-way areas.[22]

On February 10, the NERC Board directed the NERC Compliance Program and the regional councils to initiate a joint program for reporting all bulk electric system transmission line trips resulting from vegetation contact. Based on the results of these filings, NERC is to consider the development of minimum line clearance standards to ensure reliability.

The Task Force believes that more aggressive action is warranted. NERC should work with FERC, appropriate authorities in Canada, state regulatory agencies, the Institute of Electrical and Electronic Engineers (IEEE), utility arborists, and other experts from the US and Canada to develop clear, unambiguous standards pertaining to maintenance of safe clearances of transmission lines from obstructions in the lines' right-of-way areas, and to develop a mechanism to verify compliance with the standards and impose penalties for noncompliance.

Ineffective vegetation management was a major cause of the August 14, 2003, blackout and it was also a causal factor in other large-scale North American outages such as those that occurred in the summer of 1996 in the western United States. Maintaining transmission line rights-of-way, including maintaining safe clearances of energized lines from vegetation, man-made structures, bird nests, etc., requires substantial expenditures in many areas of North America. However, such maintenance is a critical investment for ensuring a reliable electric system. For a review of current issues pertaining to utility vegetation management programs, see *Utility Vegetation Management Final Report*, March 2004.[23]

NERC does not presently have standards for right-of-way maintenance. However, it has standards requiring that line ratings be set to maintain safe clearances from all obstructions. Line rating standards should be reviewed to ensure that they are sufficiently clear and explicit. In the United States, National Electrical Safety Code (NESC) rules specify safety clearances required for overhead conductors from grounded objects and other types of obstructions, but those rules are subject to broad interpretation. Several states have adopted their own electrical safety codes and similar codes apply in Canada and its provinces. A mechanism is needed to verify compliance with these requirements and to penalize noncompliance.

A. Enforceable Standards

NERC should work with FERC, government agencies in Canada, state regulatory agencies, the Institute of Electrical and Electronic Engineers (IEEE), utility arborists, and other experts from the U.S. and Canada to develop clear, unambiguous standards pertaining to maintenance of safe clearances of transmission lines from obstructions in the lines' right-of-way areas, and procedures to verify compliance with the standards. States, provinces, and local governments should remain free to set more specific or higher standards as they deem necessary for their respective areas.

B. Right-of-Way Management Plan

NERC should require each bulk electric transmission operator to publish annually a proposed right-of-way management plan on its public website, and a report on its right-of-way management activities for the previous year. The management plan should include the planned frequency of actions such as right-of-way trimming, herbicide treatment, and inspections, and the report should give the dates when the rights-of-way in a given district were last inspected and corrective actions taken.

C. Requirement to Report Outages Due to Ground Faults in Right-of-Way Areas

Beginning with an effective date of March 31, 2004, NERC should require each transmission owner/operator to submit quarterly reports of all ground-fault line trips, including their causes, on lines of 115 kV and higher in its footprint to the regional councils. Failure to report such trips should lead to an appropriate penalty. Each regional council should assemble a detailed annual report on ground fault line trips and their causes in its area to FERC, NERC, DOE, appropriate authorities in Canada, and state regulators no later than March 31 for the preceding year, with the first annual report to be filed in March 2005 for calendar year 2004.

D. Transmission-Related Vegetation Management Expenses, if Prudently Incurred, Should be Recoverable through Electric Rates

The level of activity in vegetation management programs in many utilities and states has fluctuated widely from year to year, due in part to inconsistent funding and varying management support. Utility managers and regulators should recognize the importance of effective vegetation management to transmission system reliability, and that

changes in vegetation management may be needed in response to weather, insect infestations, and other factors. Transmission vegetation management programs should be consistently funded and proactively managed to maintain and improve system reliability.

17. Strengthen the NERC Compliance Enforcement Program.

On February 10, 2004, the NERC Board of Trustees approved directives to the regional reliability councils that will significantly strengthen NERC's existing Compliance Enforcement Program. The Task Force supports these directives strongly, and recommends certain additional actions, as described below.[24]

A. Reporting of Violations

NERC:

Requires each regional council to report to the NERC Compliance Enforcement Program within one month of occurrence all "significant violations" of NERC operating policies and planning standards and regional standards, whether verified or still under investigation by the regional council. (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.) In addition, each regional council is to report quarterly to NERC, in a format prescribed by NERC, all violations of NERC and regional reliability standards.

Task Force:

Recommends that NERC require the regional councils' quarterly reports and reports on significant violations be filed as public documents with FERC and appropriate authorities in Canada, at the same time that they are sent to NERC.

B. Enforcement Action by NERC Board

NERC:

After being presented with the results of the investigation of a significant violation, the Board is to require an offending organization to correct the violation within a specified time. If the Board determines that the 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 from appropriate regulatory authorities in the United States and Canada.

Task Force:

Recommends that NERC inform the federal and state or provincial authorities of both countries of the final results of all enforcement proceedings, and make the results of such proceedings public.

C. Violations in August 14, 2003 Blackout

NERC:

The Compliance and Standards investigation team will issue a final report in March or April of 2004 of violations of NERC and regional standards that occurred on August 14. (Seven violations are noted in this report (pages 19-20), but additional violations may be identified by NERC.) Within three months of the issuance of the report, NERC is to develop recommendations to improve the compliance process.

Task Force:

Recommends that NERC make its recommendations available to appropriate U.S. federal and state authorities, to appropriate authorities in Canada, and to the public.

D. Compliance Audits

NERC:

Established plans for two types of audits, compliance audits and readiness audits. Compliance audits would determine whether the subject entity is in documented compliance with NERC standards, policies, etc. Readiness audits focus on whether the entity is functionally capable of meeting the terms of its reliability responsibilities. Under the terms approved by NERC's Board, the readiness audits to be completed by June 30, 2004, will be conducted using existing NERC rules, policies, standards, and NERC compliance templates. Requirements for control areas will be based on the existing NERC Control Area Certification Procedure, and updated as new criteria are approved.

Task Force:

Supports the NERC effort to verify that all entities are compliant with reliability standards. Effective compliance and auditing will require that the NERC standards be improved rapidly to make them clear, unambiguous, measurable, and consistent with the Functional Model.

E. Audit Standards and Composition of Audit Teams

NERC:

Under the terms approved by the Board, the regional councils are to have primary responsibility for conducting the compliance audits, under the oversight and direct participation of staff from the NERC Compliance Enforcement Program. FERC and other relevant regulatory agencies will be invited to participate in the audits, subject to the same confidentiality conditions as the other team members.

Task Force:

Recommends that each team should have some members who are electric reliability experts from outside the region in which the audit is occurring. Also, some team members should be from outside the electricity industry, i.e., individuals with experience in systems engineering and management, such as persons from the nuclear power industry, the U.S. Navy, the aerospace industry, air traffic control, or other relevant industries or government agencies. To improve the objectivity and consistency of investigation and performance, NERC-organized teams should conduct these compliance audits, using NERC criteria (with regional variations if more stringent), as opposed to the regional councils using regionally developed criteria.

F. Public Release of Compliance Audit Reports

Task Force:

Recommends that NERC require all compliance audit reports to be publicly posted, excluding portions pertaining to physical and cyber security according to predetermined criteria. Such reports should draw clear distinctions between serious and minor violations of reliability standards or related requirements.

18. Support and strengthen NERC's Reliability Readiness Audit Program.[25]

On February 10, 2004, the NERC Board of Trustees approved the establishment of a NERC program for periodic reviews of the reliability readiness of all reliability coordinators and control areas. The Task Force strongly supports this action, and recommends certain additional measures, as described below.

A. Readiness Audits

NERC:

In its directives of February 10, 2004, NERC indicated that it and the regional councils would jointly establish a program to audit the reliability readiness of all reliability coordinators and control areas within three years and continuing thereafter on a three-year cycle. Twenty audits of high-priority areas will be completed by June 30, 2004, with particular attention to deficiencies identified in the investigation of the August 14 blackout.

Task Force:

Recommends that the remainder of the first round of audits be completed within two years, as compared to NERC's plan for three years.

B. Public Release of Readiness Audit Reports

Task Force:

Recommends that NERC require all readiness audit reports to be publicly posted, excluding portions pertaining to physical and cyber security. Reports should also be sent directly to DOE, FERC, and relevant authorities in Canada and state commissions. Such reports should draw clear distinctions between serious and minor violations of reliability standards or related requirements.

19. Improve near-term and long-term training and certification requirements for operators, reliability coordinators, and operator support staff.[26]

In its requirements of February 10, 2004, NERC directed that all reliability coordinators, control areas, and transmission operators are to provide at least five days per year of training and drills in system emergencies, using realistic simulations, 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 by June 30, 2004.

The Task Force supports these near-term requirements strongly. For the long term, the Task Force recommends that:

A. NERC should require training for the planning staff at control areas and reliability coordinators concerning power system characteristics

and load, VAr, and voltage limits, to enable them to develop rules for operating staff to follow.

B. NERC should require control areas and reliability coordinators to train grid operators, IT support personnel, and their supervisors to recognize and respond to abnormal automation system activity.

C. NERC should commission an advisory report by an independent panel to address a wide range of issues concerning reliability training programs and certification requirements.

The Task Force investigation team found 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 to train and verify the capabilities of operating personnel. Such simulations are essential if operators and other staff are to be able to respond adequately to emergencies. This training deficiency contributed to the lack of situational awareness and failure to declare an emergency on August 14 while operator intervention was still possible (before events began to occur at a speed beyond human control).

Control rooms must remain functional under a wide range of possible conditions. Any person with access to a control room should be trained so that he or she understands the basic functions of the control room, and his or her role in relation to those of others in the room under any conditions. Information technology (IT) staff, in particular, should have a detailed understanding of the information needs of the system operators under alternative conditions.

The Task Force's cyber investigation team noted in its site visits an increasing reliance by control areas and utilities on automated systems to measure, report on, and change a wide variety of physical processes associated with utility operations.[27] If anything, this trend is likely to intensify in the future. These systems enable the achievement of major operational efficiencies, but their failure could cause or contribute to blackouts, as evidenced by the alarm failures at FirstEnergy and the state estimator deactivation at MISO.

Grid operators should be trained to recognize and respond more efficiently to security and automation problems, reinforced through the use of periodic exercises. Likewise, IT support personnel should be better trained to understand and respond to the requirements of grid operators during security and IT incidents.

NERC's near-term requirements for emergency preparedness training are described above. For the long term, training for system emergencies should be fully integrated into the broader training programs required for all system planners, system operators, their supervisors, and other control room support staff.

Advisory Report by Independent Panel on Industry Training Programs and Certification Requirements

Under the oversight of FERC and appropriate Canadian authorities, the Task Force recommends that NERC commission an independent advisory panel of experts to design and propose minimum training programs and certification procedures for the industry's control room managers and staff. This panel should be comprised of experts from electric industry organizations with outstanding training programs, universities, and other industries that operate large safety or reliability-oriented systems and training programs. (The Institute of Nuclear Power Operations (INPO), for example, provides training and other safety-related services to operators of U.S. nuclear power plants and plants in other countries.) The panel's report should provide guidance on issues such as:

1. Content of programs for new trainees
2. Content of programs for existing operators and other categories of employees
3. Content of continuing education programs and fraction of employee time to be committed to ongoing training
4. Going beyond paper-based, fact-oriented "knowledge" requirements for operators—i.e., confirming that an individual has the ability to cope with unforeseen situations and emergencies
5. In-house training vs. training by independent parties
6. Periodic accreditation of training programs
7. Who should certify trained staff?
8. Criteria to establish grades or levels of operator qualifications from entry level to supervisor or manager, based on education, training, and experience.

The panel's report should be delivered by March 31, 2005. FERC and Canadian authorities, in consultation with NERC and others, should evaluate the report and consider its findings in setting

minimum training and certification requirements for control areas and reliability coordinators.

20. Establish clear definitions for *normal, alert* and *emergency* operational system conditions. Clarify roles, responsibilities, and authorities of reliability coordinators and control areas under each condition.[28]

NERC should develop by June 30, 2004 definitions for normal, alert, and emergency system conditions, and clarify reliability coordinator and control area functions, responsibilities, required capabilities, and required authorities under each operational system condition.

System operators need common definitions for normal, alert, and emergency conditions to enable them to act appropriately and predictably as system conditions change. On August 14, the principal entities involved in the blackout did not have a shared understanding of whether the grid was in an emergency condition, nor did they have a common understanding of the functions, responsibilities, capabilities, and authorities of reliability coordinators and control areas under emergency or near-emergency conditions.

NERC:

On February 10, 2004, NERC's Board of Trustees directed NERC's Operating Committee to "clarify reliability coordinator and control area functions, responsibilities, capabilities, and authorities" by June 30, 2004.

Task Force:

Recommends that NERC go further and develop clear definitions of three operating system conditions, along with clear statements of the roles and responsibilities of all participants, to ensure effective and timely actions in critical situations.

Designating three alternative system conditions (normal, alert, and emergency) would help grid managers to avert and deal with emergencies through preventive action. Many difficult situations are avoidable through strict adherence to sound procedures during normal operations. However, unanticipated difficulties short of an emergency still arise, and they must be addressed swiftly and skillfully to prevent them from becoming emergencies. Doing so requires a high level of situational awareness that is difficult to sustain indefinitely, so an intermediate "alert" state is needed, between "normal" and "emergency." In some areas (e.g., NPCC) an "alert" state has already been established.

21. Make more effective and wider use of system protection measures.[29]

In its requirements of February 10, 2004, NERC:

A. Directed all transmission owners to evaluate the settings of zone 3 relays on all transmission lines of 230 kV and higher.

B. Directed all regional councils to evaluate the feasibility and benefits of installing under-voltage load shedding capability in load centers.

C. Called for an evaluation within one year of its planning standard on system protection and control to take into account the lessons from the August 14 blackout.

The Task Force supports these actions strongly, and recommends certain additional measures, as described below.

A. Evaluation of Zone 3 Relays

NERC:

Industry is to review zone 3 relays on lines of 230 kV and higher.

Task Force:

Recommends that NERC broaden the review to include operationally significant 115 kV and 138 kV lines, e.g., lines that are part of monitored flowgates or interfaces. Transmission owners should also look for zone 2 relays set to operate like zone 3s.

B. Evaluation of Applicability of Under-Voltage Load Shedding

NERC:

Required each regional reliability council to evaluate the feasibility and benefits of under-voltage load shedding (UVLS) capability in load centers that could become unstable as a result of insufficient reactive power following credible multiple-contingency events. The regions should complete the initial studies and report the results to NERC within one year. The regions should promote the installation of under-voltage load shedding capabilities within critical areas where beneficial, as determined by the studies to be effective in preventing or containing an uncontrolled cascade of the power system.

Task Force:

Recommends that NERC require the results of the regional studies to be provided to federal and state or provincial regulators at the same time that they are reported to NERC. In addition, NERC should require every entity with a new or existing UVLS program to have a well-documented set of guidelines for operators that specify the conditions and triggers for UVLS use.

C. Evaluation of NERC's Planning Standard III

NERC:

Plans to evaluate Planning Standard III, System Protection and Control, and propose, by March 1, 2005, specific revisions to the criteria to address adequately the issue of slowing or limiting the propagation of a cascading failure, in light of the experience gained on August 14.

Task Force:

Recommends that NERC, as part of the review of Planning Standard III, determine the goals and principles needed to establish an integrated approach to relay protection for generators and transmission lines and the use of under-frequency and under-voltage load shedding (UFLS and UVLS) programs. An integrated approach is needed to ensure that at the local and regional level these interactive components provide an appropriate balance of risks and benefits in terms of protecting specific assets and facilitating overall grid survival. This review should take into account the evidence from August 14 of some unintended consequences of installing Zone 3 relays and using manufacturer-recommended settings for relays protecting generators. It should also include an assessment of the appropriate role and scope of UFLS and UVLS, and the appropriate use of time delays in relays.

Recommends that in this effort NERC should work with industry and government research organizations to assess the applicability of existing and new technology to make the interconnections less susceptible to cascading outages.

22. Evaluate and adopt better real-time tools for operators and reliability coordinators.[30]

NERC's requirements of February 10, 2004, direct its Operating Committee to evaluate within one year the real-time operating tools necessary for reliability operation and reliability coordination, including backup capabilities. The committee's report is to address both minimum acceptable capabilities for critical reliability functions and a guide to best practices.

The Task Force supports these requirements strongly. It recommends that NERC require the committee to:

A. Give particular attention in its report to the development of guidance to control areas and reliability coordinators on the use of automated wide-area situation visualization display systems and the integrity of data used in those systems.

B. Prepare its report in consultation with FERC, appropriate authorities in Canada, DOE, and the regional councils. The report should also inform actions by FERC and Canadian government agencies to establish minimum functional requirements for control area operators and reliability coordinators.

The Task Force also recommends that FERC, DHS, and appropriate authorities in Canada should require annual independent testing and certification of industry EMS and SCADA systems to ensure that they meet the minimum requirements envisioned in Recommendation 3.

A principal cause of the August 14 blackout was a lack of situational awareness, which was in turn the result of inadequate reliability tools and backup capabilities. In addition, 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 to supply its state estimator with correct system data on August 14 contributed to the lack of situational awareness. The need for improved visualization capabilities over a wide geographic area has been a recurrent theme in blackout investigations. Some wide-area tools to aid situational awareness (e.g., real-time phasor measurement systems) have been tested in some regions but are not yet in general use. Improvements in this area will require significant new investments involving existing or emerging technologies.

The investigation of the August 14 blackout revealed that there has been no consistent means across the Eastern Interconnection to provide an understanding of the status of the power grid outside of a control area. Improved visibility of the status of the grid beyond an operator's own area of control would aid the operator in making adjustments in its operations to mitigate potential

problems. The expanded view advocated above would also enable facilities to be more proactive in operations and contingency planning.

Annual testing and certification by independent, qualified parties is needed because EMS and SCADA systems are the nerve centers of bulk electric networks. Ensuring that these systems are functioning properly is critical to sound and reliable operation of the networks.

23. Strengthen reactive power and voltage control practices in all NERC regions.[31]

NERC's requirements of February 10, 2004 call for a reevaluation within one year of existing reactive power and voltage control standards and how they are being implemented in the ten NERC regions. However, by June 30, 2004, ECAR is required to 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.

The Task Force supports these requirements strongly. It recommends that NERC require the regional analyses to include recommendations for appropriate improvements in operations or facilities, and to be subject to rigorous peer review by experts from within and outside the affected areas.

The Task Force also recommends that FERC and appropriate authorities in Canada require all tariffs or contracts for the sale of generation to include provisions specifying that the generators can be called upon to provide or increase reactive power output if needed for reliability purposes, and that the generators will be paid for any lost revenues associated with a reduction of real power sales attributable to a required increase in the production of reactive power.

Reactive power problems were a significant factor in the August 14 outage, and they were also important elements in several of the earlier outages detailed in Chapter 7.[32] Accordingly, the Task Force agrees that a comprehensive review is needed of North American practices with respect to managing reactive power requirements and maintaining an appropriate balance among alternative types of reactive resources.

Regional Analyses, Peer Reviews, and Follow-Up Actions

The Task Force recommends that each regional reliability council, working with reliability coordinators and the control areas serving major load centers, should conduct a rigorous reliability and adequacy analysis comparable to that outlined in FERC's December 24, 2003, Order[33] to FirstEnergy concerning the Cleveland-Akron area. The Task Force recommends that NERC develop a prioritized list for which areas and loads need this type of analysis and a schedule that ensures that the analysis will be completed for all such load centers by December 31, 2005.

24. Improve quality of system modeling data and data exchange practices.[34]

NERC's requirements of February 10, 2004 direct that within one year the regional councils are to 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.

The Task Force supports these requirements strongly. The Task Force also recommends that FERC and appropriate authorities in Canada require all generators, regardless of ownership, to collect and submit generator data to NERC, using a regulator-approved template.

The after-the-fact models developed to simulate August 14 conditions and events found that the dynamic modeling assumptions for generator and load power factors in regional planning and operating models were frequently inaccurate. In particular, the assumptions of load power factor were overly optimistic—loads were absorbing much more reactive power than the pre-August 14 models indicated. Another suspected problem concerns modeling of shunt capacitors under depressed voltage conditions.

NERC should work with the regional reliability councils to establish regional power system models that enable the sharing of consistent and validated data among entities in the region. Power flow and transient stability simulations should be periodically 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.

During the data collection phase of the blackout investigation, when control areas were asked for information pertaining to merchant generation within their area, the requested data was

frequently not available because the control area had not recorded the status or output of the generator at a given point in time. Some control area operators also asserted that some of the data that did exist was commercially sensitive or confidential. To correct such problems, the Task Force recommends that FERC and authorities in Canada require all generators, regardless of ownership, to collect and submit generator data, according to a regulator-approved template.

25. NERC should reevaluate its existing reliability standards development process and accelerate the adoption of enforceable standards.[35]

The Task Force recommends that, with support from FERC and appropriate authorities in Canada, NERC should:

A. Re-examine its existing body of standards, guidelines, etc., to identify those that are most important and ensure that all concerns that merit standards are addressed in the plan for standards development.

B. Re-examine the plan to ensure that those that are the most important or the most out-of-date are addressed early in the process.

C. Build on existing provisions and focus on what needs improvement, and incorporate compliance and readiness considerations into the drafting process.

D. Re-examine the Standards Authorization Request process to determine whether, for each standard, a review and modification of an existing standard would be more efficient than development of wholly new text for the standard.

NERC has already begun a long-term, systematic process to reevaluate its standards. It is of the greatest importance, however, that this process not dilute the content of the existing standards, nor conflict with the right of regions or other areas to impose more stringent standards. The state of New York, for example, operates under mandatory and more stringent reliability rules and standards than those required by NERC and NPCC.[36]

Similarly, several commenters on the Interim Report wrote jointly that:

> *NERC standards are the minimum—national standards should always be minimum rather than absolute or "one size fits all" criteria. [Systems for] densely populated areas, like the metropolitan areas of New York, Chicago, or Washington, must be designed and operated in accordance with a higher level of reliability than would be appropriate for sparsely populated parts of the country. It is essential that regional differences in terms of load and population density be recognized in the application of planning and operating criteria. Any move to adopt a national, "one size fits all" formula for all parts of the United States would be disastrous to reliability . . . .*
>
> *A strong transmission system designed and operated in accordance with weakened criteria would be disastrous. Instead, a concerted effort should be undertaken to determine if existing reliability criteria should be strengthened. Such an effort would recognize the geo-electrical magnitude of today's interconnected networks, and the increased complexities deregulation and restructuring have introduced in planning and operating North American power systems. Most important, reliability should be considered a higher priority than commercial use. Only through strong standards and careful engineering can unacceptable power failures like the August 14 blackout be avoided in the future.*[37]

26. Tighten communications protocols, especially for communications during alerts and emergencies. Upgrade communication system hardware where appropriate.[38]

NERC should work with reliability coordinators and control area operators to improve the effectiveness of internal and external communications during alerts, emergencies, or other critical situations, and ensure that all key parties, including state and local officials, receive timely and accurate information. NERC should task the regional councils to work together to develop communications protocols by December 31, 2004, and to assess and report on the adequacy of emergency communications systems within their regions against the protocols by that date.

On August 14, 2003, reliability coordinator and control area communications regarding conditions in northeastern Ohio were in some cases ineffective, unprofessional, and 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 alerts and emergencies, is essential to reliability. Standing hotline networks,

or a functional equivalent, should be established for use in alerts and emergencies (as opposed to one-on-one phone calls) to ensure that all key parties are able to give and receive timely and accurate information.

27. Develop enforceable standards for transmission line ratings.[39]

NERC should develop clear, unambiguous requirements for the calculation of transmission line

ratings (including dynamic ratings), and require that all lines of 115 kV or higher be rerated according to these requirements by June 30, 2005.

As seen on August 14, inadequate vegetation management can lead to the loss of transmission lines that are not overloaded, at least not according to their rated limits. The investigation of the blackout, however, also found that even after allowing for regional or geographic differences, there is still significant variation in how the ratings of existing lines have been calculated. This variation—in terms of assumed ambient temperatures, wind speeds, conductor strength, and the purposes and duration of normal, seasonal, and emergency ratings—makes the ratings themselves unclear, inconsistent, and unreliable across a region or between regions. This situation creates unnecessary and unacceptable uncertainties about the safe carrying capacity of individual lines on the transmission networks. Further, the appropriate use of dynamic line ratings needs to be included in this review because adjusting a line's rating according to changes in ambient conditions may enable the line to carry a larger load while still meeting safety requirements.

28. Require use of time-synchronized data recorders.[40]

In its requirements of February 10, 2004, NERC directed the regional councils to define within one year regional criteria for the application of synchronized recording devices in key power plants and substations.

The Task Force supports the intent of this requirement strongly, but it recommends a broader approach:

A. FERC and appropriate authorities in Canada should require the use of data recorders synchronized by signals from the Global Positioning System (GPS) on all categories of facilities whose data may be needed to investigate future system disturbances, outages, or blackouts.

B. NERC, reliability coordinators, control areas, and transmission owners should determine where high speed power system disturbance recorders are needed on the system, and ensure that they are installed by December 31, 2004.

C. NERC should establish data recording protocols.

D. FERC and appropriate authorities in Canada should ensure that the investments called for in this recommendation will be recoverable through transmission rates.

A valuable lesson from the August 14 blackout is the importance of having time-synchronized system data recorders. The Task Force's investigators labored over thousands of data items to determine the sequence of events, much like putting together small pieces of a very large puzzle. That process would have been significantly faster and easier if there had been wider use of synchronized data recording devices.

NERC Planning Standard I.F, Disturbance Monitoring, requires the use of recording devices for disturbance analysis. On August 14, time recorders were frequently used but not synchronized to a time standard. Today, at a relatively modest cost, all digital fault recorders, digital event recorders, and power system disturbance recorders can and should be time-stamped at the point of observation using a Global Positioning System (GPS) synchronizing signal. (The GPS signals are synchronized with the atomic clock maintained in Boulder, Colorado by the U.S. National Institute of Standards and Technology.) Recording and time-synchronization equipment should be monitored and calibrated to assure accuracy and reliability.

It is also important that data from automation systems be retained at least for some minimum period, so that if necessary it can be archived to enable adequate analysis of events of particular interest.

29. Evaluate and disseminate lessons learned during system restoration.[41]

In the requirements it issued on February 10, 2004, NERC directed its Planning Committee to work with the Operating Committee, NPCC, ECAR, and PJM to evaluate the black start and system restoration performance following the outage of August 14, and to report within one year the results of that evaluation, with recommendations for

improvement. Within six months of the Planning Committee's report, all regional councils are to have reevaluated their plans and procedures to ensure an effective black start and restoration capability within their region.

The Task Force supports these requirements strongly. In addition, the Task Force recommends that NERC should require the Planning Committee's review to include consultation with appropriate stakeholder organizations in all areas that were blacked out on August 14.

The efforts to restore the power system and customer service following the outage were generally 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 compare them with previous blackout/restoration studies and determine opportunities for improvement. Black start 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 review actual events and experiences to learn how to better prepare for system black start and restoration in the future. That opportunity should not be lost.

30. Clarify criteria for identification of operationally critical facilities, and improve dissemination of updated information on unplanned outages.[42]

NERC should work with the control areas and reliability coordinators to clarify the criteria for identifying critical facilities whose operational status can affect the reliability of neighboring areas, and to improve mechanisms for sharing information about unplanned outages of such facilities in near real-time.

The lack of accurate, near real-time information about unplanned outages degraded the performance of state estimator and reliability assessment functions on August 14. NERC and the industry must improve the mechanisms for sharing outage information in the operating time horizon (e.g., 15 minutes or less), to ensure the accurate and timely sharing of outage data needed by real-time operating tools such as state estimators, real-time contingency analyzers, and other system monitoring tools.

Further, NERC's present operating policies do not specify adequately criteria for identifying those critical facilities within reliability coordinator and control area footprints whose operating status could affect the reliability of neighboring systems. This leads to uncertainty about which facilities should be monitored by both the reliability coordinator for the region in which the facility is located and by one or more neighboring reliability coordinators.

31. Clarify that the transmission loading relief (TLR) process should not be used in situations involving an actual violation of an Operating Security Limit. Streamline the TLR process.[43]

NERC should clarify that the TLR procedure is often too slow for use in situations in which an affected system is already in violation of an Operating Security Limit. NERC should also evaluate experience to date with the TLR procedure and propose by September 1, 2004, ways to make it less cumbersome.

The reviews of control area and reliability coordinator transcripts from August 14 confirm that the TLR process is cumbersome, perhaps unnecessarily so, and not fast and predictable enough for use situations in which an Operating Security Limit is close to or actually being violated. NERC should develop an alternative to TLRs that can be used quickly to address alert and emergency conditions.

Group III. Physical and Cyber Security of North American Bulk Power Systems

32. Implement NERC IT standards.

The Task Force recommends that NERC standards related to physical and cyber security should be understood as being included within the body of standards to be made mandatory and enforceable in Recommendation No. 1. Further:

A. NERC should ensure that the industry has implemented its Urgent Action Standard 1200; finalize, implement, and ensure membership compliance with its Reliability Standard 1300 for Cyber Security and take actions to better communicate and enforce these standards.

B. CAs and RCs should implement existing and emerging NERC standards, develop and implement best practices and policies for IT and

security management, and authenticate and authorize controls that address EMS automation system ownership and boundaries.

Interviews and analyses conducted by the SWG indicate that within some of the companies interviewed there are potential opportunities for cyber system compromise of EMS and their supporting IT infrastructure. Indications of procedural and technical IT management vulnerabilities were observed in some facilities, such as unnecessary software services not denied by default, loosely controlled system access and perimeter control, poor patch and configuration management, and poor system security documentation.

An analysis of the more prevalent policies and standards within the electricity sector revealed that there is existing and expanding guidance on standards within the sector to perform IT and information security management.[44] NERC issued a temporary standard (Urgent Action Standard 1200, Cyber Security) on August 13, 2003, and is developing the formal Reliability Standard 1300 for Cyber Security. Both start the industry down the correct path, but there is a need to communicate and enforce these standards by providing the industry with recommended implementation guidance. Implementation guidance regarding these sector-wide standards is especially important given that implementation procedures may differ among CAs and RCs.

In order to address the finding described above, the Task Force recommends:

- NERC:
  - Ensure that the industry has implemented its Urgent Action Standard 1200 and determine if the guidance contained therein needs to be strengthened or amended in the ongoing development of its Reliability Standard 1300 for Cyber Security.
  - Finalize, implement, and ensure membership compliance of its Reliability Standard 1300 for Cyber Security and take actions to better communicate and enforce these standards. These actions should include, but not necessarily be limited to:
    1. The provision of policy, process, and implementation guidance to CAs and RCs; and
    2. The establishment of mechanisms for compliance, audit, and enforcement. This may include recommendations, guidance, or agreements between NERC, CAs and RCs that cover self-certification, self-assessment, and/or third-party audit.
  - Work with federal, state, and provincial/territorial jurisdictional departments and agencies to regularly update private and public sector standards, policies, and other guidance.
- CAs and RCs:
  - Implement existing and emerging NERC standards.
  - Develop and implement best practices and policies for IT and security management drawing from existing NERC and government authorities' best practices.[45] These should include, but not necessarily be limited to:
    1. Policies requiring that automation system products be delivered and installed with unnecessary services deactivated in order to improve "out-of-the-box security."
    2. The creation of centralized system administration authority within each CA and RC to manage access and permissions for automation access (including vendor management backdoors, links to other automation systems, and administrative connections).
  - Authenticate and authorize controls that address EMS automation system ownership and boundaries, and ensure access is granted only to users who have corresponding job responsibilities.

33. Develop and deploy IT management procedures.

CAs' and RCs' IT and EMS support personnel should develop procedures for the development, testing, configuration, and implementation of technology related to EMS automation systems and also define and communicate information security and performance requirements to vendors on a continuing basis. Vendors should ensure that system upgrades, service packs, and bug fixes are made available to grid operators in a timely manner.

Interviews and analyses conducted by the SWG indicate that, in some instances, there were ill-defined and/or undefined procedures for EMS automation systems software and hardware development, testing, deployment, and backup. In addition, there were specific instances of failures to perform system upgrade, version control, maintenance, rollback, and patch management tasks.

At one CA, these procedural vulnerabilities were compounded by inadequate, out-of-date, or non-

existing maintenance contracts with EMS vendors and contractors. This could lead to situations where grid operators could alter EMS components without vendor notification or authorization as well as scenarios in which grid operators are not aware of or choose not to implement vendor-recommended patches and upgrades.

34. Develop corporate-level IT security governance and strategies.

CAs and RCs and other grid-related organizations should have a planned and documented security strategy, governance model, and architecture for EMS automation systems.

Interviews and analysis conducted by the SWG indicate that in some organizations there is evidence of an inadequate security policy, governance model, strategy, or architecture for EMS automation systems. This is especially apparent with legacy EMS automation systems that were originally designed to be stand-alone systems but that are now interconnected with internal (corporate) and external (vendors, Open Access Same Time Information Systems (OASIS), RCs, Internet, etc.) networks. It should be noted that in some of the organizations interviewed this was not the case and in fact they appeared to excel in the areas of security policy, governance, strategy, and architecture.

In order to address the finding described above, the Task Force recommends that CAs, RCs, and other grid-related organizations have a planned and documented security strategy, governance model, and architecture for EMS automation systems covering items such as network design, system design, security devices, access and authentication controls, and integrity management as well as backup, recovery, and contingency mechanisms.

35. Implement controls to manage system health, network monitoring, and incident management.

IT and EMS support personnel should implement technical controls to detect, respond to, and recover from system and network problems. Grid operators, dispatchers, and IT and EMS support personnel should be provided the tools and training to ensure that the health of IT systems is monitored and maintained.

Interviews and analysis conducted by the SWG indicate that in some organizations there was ineffective monitoring and control over EMS-supporting IT infrastructure and overall IT network health. In these cases, both grid operators and IT support personnel did not have situational awareness of the health of the IT systems that provide grid information both globally and locally. This resulted in an inability to detect, assess, respond to, and recover from IT system-related cyber failures (failed hardware/software, malicious code, faulty configurations, etc.).

In order to address the finding described above, the Task Force recommends:

- IT and EMS support personnel implement technical controls to detect, respond to, and recover from system and network problems.
- Grid operators, dispatchers, and IT and EMS support personnel be provided with the tools and training to ensure that:
  - The health of IT systems is monitored and maintained.
  - These systems have the capability to be repaired and restored quickly, with a minimum loss of time and access to global and internal grid information.
  - Contingency and disaster recovery procedures exist and can serve to temporarily substitute for systems and communications failures during times when EMS automation system health is unknown or unreliable.
  - Adequate verbal communication protocols and procedures exist between operators and IT and EMS support personnel so that operators are aware of any IT-related problems that may be affecting their situational awareness of the power grid.

36. Initiate a U.S.-Canada risk management study.

In cooperation with the electricity sector, federal governments should strengthen and expand the scope of the existing risk management initiatives by undertaking a bilateral (Canada-U.S.) study of the vulnerabilities of shared electricity infrastructure and cross border interdependencies. Common threat and vulnerability assessment methodologies should be also developed, based on the work undertaken in the pilot phase of the current joint Canada-U.S. vulnerability assessment initiative, and their use promoted by CAs and RCs. To coincide with these initiatives, the electricity sector, in association with federal governments, should

develop policies and best practices for effective risk management and risk mitigation.

Effective risk management is a key element in assuring the reliability of our critical infrastructures. It is widely recognized that the increased reliance on IT by critical infrastructure sectors, including the energy sector, has increased the vulnerability of these systems to disruption via cyber means. The breadth of the August 14, 2003, power outage illustrates the vulnerabilities and interdependencies inherent in our electricity infrastructure.

Canada and the United States, recognizing the importance of assessing the vulnerabilities of shared energy systems, included a provision to address this issue in the Smart Border Declaration,[46] signed on December 12, 2001. Both countries committed, pursuant to Action Item 21 of the Declaration, to "conduct bi-national threat assessments on trans-border infrastructure and identify necessary protection measures, and initiate assessments for transportation networks and other critical infrastructure." These joint assessments will serve to identify critical vulnerabilities, strengths and weaknesses while promoting the sharing and transfer of knowledge and technology to the energy sector for self-assessment purposes.

A team of Canadian and American technical experts, using methodology developed by the Argonne National Laboratory in Chicago, Illinois, began conducting the pilot phase of this work in January 2004. The work involves a series of joint Canada-U.S. assessments of selected shared critical energy infrastructure along the Canada-U.S. border, including the electrical transmission lines and dams at Niagara Falls - Ontario and New York. The pilot phase will be completed by March 31, 2004.

The findings of the ESWG and SWG suggest that among the companies directly involved in the power outage, vulnerabilities and interdependencies of the electric system were not well understood and thus effective risk management was inadequate. In some cases, risk assessments did not exist or were inadequate to support risk management and risk mitigation plans.

In order to address these findings, the Task Force recommends:

- In cooperation with the electricity sector, federal governments should strengthen and expand the scope of the existing initiatives described above by undertaking a bilateral (Canada-U.S.) study of the vulnerabilities of shared electricity infrastructure and cross border interdependencies. The study should encompass cyber, physical, and personnel security processes and include mitigation and best practices, identifying areas that would benefit from further standardization.
- Common threat and vulnerability assessment methodologies should be developed, based on the work undertaken in the pilot phase of the current joint Canada-U.S. vulnerability assessment initiative, and their use promoted by CAs and RCs.
- The electricity sector, in association with federal governments, should develop policies and best practices for effective risk management and risk mitigation.

37. Improve IT forensic and diagnostic capabilities.

CAs and RCs should seek to improve internal forensic and diagnostic capabilities, ensure that IT support personnel who support EMS automation systems are familiar with the systems' design and implementation, and make certain that IT support personnel who support EMS automation systems have are trained in using appropriate tools for diagnostic and forensic analysis and remediation.

Interviews and analyses conducted by the SWG indicate that, in some cases, IT support personnel who are responsible for EMS automation systems are unable to perform forensic and diagnostic routines on those systems. This appears to stem from a lack of tools, documentation and technical skills. It should be noted that some of the organizations interviewed excelled in this area but that overall performance was lacking.

In order to address the finding described above, the Task Force recommends:

- CAs and RCs seek to improve internal forensic and diagnostic capabilities as well as strengthen coordination with external EMS vendors and contractors who can assist in servicing EMS automation systems;
- CAs and RCs ensure that IT support personnel who support EMS automation systems are familiar with the systems' design and implementation; and
- CAs and RCs ensure that IT support personnel who support EMS automation systems have access to and are trained in using appropriate

tools for diagnostic and forensic analysis and remediation.

38. Assess IT risk and vulnerability at scheduled intervals.

IT and EMS support personnel should perform regular risk and vulnerability assessment activities for automation systems (including EMS applications and underlying operating systems) to identify weaknesses, high-risk areas, and mitigating actions such as improvements in policy, procedure, and technology.

Interviews and analysis conducted by the SWG indicate that in some instances risk and vulnerability management were not being performed on EMS automation systems and their IT supporting infrastructure. To some CAs, EMS automation systems were considered "black box"[47] technologies; and this categorization removed them from the list of systems identified for risk and vulnerability assessment.

39. Develop capability to detect wireless and remote wireline intrusion and surveillance.

Both the private and public sector should promote the development of the capability of all CAs and RCs to reasonably detect intrusion and surveillance of wireless and remote wireline access points and transmissions. CAs and RCs should also conduct periodic reviews to ensure that their user base is in compliance with existing wireless and remote wireline access rules and policies.

Interviews conducted by the SWG indicate that most of the organizations interviewed had some type of wireless and remote wireline intrusion and surveillance detection protocol as a standard security policy; however, there is a need to improve and strengthen current capabilities regarding wireless and remote wireline intrusion and surveillance detection. The successful detection and monitoring of wireless and remote wireline access points and transmissions are critical to securing grid operations from a cyber security perspective.

There is also evidence that although many of the organizations interviewed had strict policies against allowing wireless network access, periodic reviews to ensure compliance with these policies were not undertaken.

40. Control access to operationally sensitive equipment.

RCs and CAs should implement stringent policies and procedures to control access to sensitive equipment and/or work areas.

Interviews conducted by the SWG indicate that at some CAs and RCs operationally sensitive computer equipment was accessible to non-essential personnel. Although most of these non-essential personnel were escorted through sensitive areas, it was determined that this procedure was not always enforced as a matter of everyday operations.

In order to address the finding described above, the Task Force recommends:

- That RCs and CAs develop policies and procedures to control access to sensitive equipment and/or work areas to ensure that:
  - Access is strictly limited to employees or contractors who utilize said equipment as part of their job responsibilities.
  - Access for other staff who need access to sensitive areas and/or equipment but are not directly involved in their operation (such as cleaning staff and other administrative personnel) is strictly controlled (via escort) and monitored.

41. NERC should provide guidance on employee background checks.

NERC should provide guidance on the implementation of its recommended standards on background checks, and CAs and RCs should review their policies regarding background checks to ensure they are adequate.

Interviews conducted with sector participants revealed instances in which certain company contract personnel did not have to undergo background check(s) as stringent as those performed on regular employees of a CA or RC. NERC Urgent Action Standard Section 1207 Paragraph 2.3 specifies steps to remediate sector weaknesses in this area but there is a need to communicate and enforce this standard by providing the industry with recommended implementation guidance, which may differ among CAs and RCs.

In order to address the finding described above, the Task Force recommends:

- NERC provide guidance on the implementation of its recommended standards on background checks, especially as they relate to the screening of contracted and sub-contracted personnel.
- CAs and RCs review their policies regarding background checks to ensure they are adequate before allowing sub-contractor personnel to access their facilities.

42. Confirm NERC ES-ISAC as the central point for sharing security information and analysis.

The NERC ES-ISAC should be confirmed as the central electricity sector point of contact for security incident reporting and analysis. Policies and protocols for cyber and physical incident reporting should be further developed including a mechanism for monitoring compliance. There also should be uniform standards for the reporting and sharing of physical and cyber security incident information across both the private and public sectors.

There are currently both private and public sector information sharing and analysis initiatives in place to address the reporting of physical and cyber security incidents within the electricity sector. In the private sector, NERC operates an Electricity Sector Information Sharing and Analysis Center (ES-ISAC) specifically to address this issue. On behalf of the U.S. Government, the Department of Homeland Security (DHS) operates the Information Analysis and Infrastructure Protection (IAIP) Directorate to collect, process, and act upon information on possible cyber and physical security threats and vulnerabilities. In Canada, Public Safety and Emergency Preparedness Canada has a 24/7 operations center for the reporting of incidents involving or impacting critical infrastructure. As well, both in Canada and the U.S., incidents of a criminal nature can be reported to law enforcement authorities of jurisdiction.

Despite these private and public physical and cyber security information sharing and analysis initiatives, an analysis of policies and procedures within the electricity sector reveals that reporting of security incidents to internal corporate security, law enforcement, or government agencies was uneven across the sector. The fact that these existing channels for incident reporting—whether security- or electricity systems-related—are currently underutilized is an operating deficiency which could hamper the industry's ability to address future problems in the electricity sector.

Interviews and analysis conducted by the SWG further indicate an absence of coherent and effective mechanisms for the private sector to share information related to critical infrastructure with government. There was also a lack of confidence on the part of private sector infrastructure owners and grid operators that information shared with governments could be protected from disclosure under Canada's Access to Information Act (ATIA) and the U.S. Freedom of Information Act (FOIA). On the U.S. side of the border, however, the imminent implementation of the Critical Infrastructure Information (CII) Act of 2002 should mitigate almost all industry concerns about FOIA disclosure. In Canada, Public Safety and Emergency Preparedness Canada relies on a range of mechanisms to protect the sensitive information related to critical infrastructure that it receives from its private sector stakeholders, including the exemptions for third party information that currently exist in the ATIA and other instruments. At the same time, Public Safety and Emergency Preparedness Canada is reviewing options for stronger protection of CI information, including potential changes in legislation.

In order to address the finding described above, the Task Force recommends:

- Confirmation of the NERC ES-ISAC as the central electricity sector point of contact for security incident reporting and analysis.
- Further development of NERC policies and protocols for cyber and physical incident reporting including a mechanism for monitoring compliance.
- The establishment of uniform standards for the reporting of physical and cyber security incidents to internal corporate security, private sector sector-specific information sharing and analysis bodies (including ISACs), law enforcement, and government agencies.
- The further development of new mechanisms and the promulgation of existing[48] Canadian and U.S. mechanisms to facilitate the sharing of electricity sector threat and vulnerability information across governments as well as between the private sector and governments.
- Federal, state, and provincial/territorial governments work to further develop and promulgate measures and procedures that protect critical, but sensitive, critical infrastructure-related information from disclosure.

43. Establish clear authority for physical and cyber security.

The task force recommends that corporations establish clear authority and ownership for physical and cyber security. This authority should have the ability to influence corporate decision-making and the authority to make physical and cyber security-related decisions.

Interviews and analysis conducted by the SWG indicate that some power entities did not implement best practices when organizing their security staff. It was noted at several entities that the Information System (IS) security staff reported to IT support personnel such as the Chief Information Officer (CIO).

Best practices across the IT industry, including most large automated businesses, indicate that the best way to balance security requirements properly with the IT and operational requirements of a company is to place security at a comparable level within the organizational structure. By allowing the security staff a certain level of autonomy, management can properly balance the associated risks and operational requirements of the facility.

44. Develop procedures to prevent or mitigate inappropriate disclosure of information.

The private and public sectors should jointly develop and implement security procedures and awareness training in order to mitigate or prevent disclosure of information by the practices of open source collection, elicitation, or surveillance.

SWG interviews and intelligence analysis provide no evidence of the use of open source collection, elicitation or surveillance against CAs or RCs leading up to the August 14, 2003, power outage. However, such activities may be used by malicious individuals, groups, or nation states engaged in intelligence collection in order to gain insights or proprietary information on electric power system functions and capabilities. Open source collection is difficult to detect and thus is best countered through careful consideration by industry stakeholders of the extent and nature of publicly-available information. Methods of elicitation and surveillance, by comparison, are more detectable activities and may be addressed through increased awareness and security training. In addition to prevention and detection, it is equally important that suspected or actual incidents of these intelligence collection activities be reported to government authorities.

In order to address the findings described above, the Task Force recommends:

- The private and public sectors jointly develop and implement security procedures and awareness training in order to mitigate disclosure of information not suitable for the public domain and/or removal of previously available information in the public domain (web sites, message boards, industry publications, etc.).
- The private and public sector jointly develop and implement security procedures and awareness training in order to mitigate or prevent disclosure of information by the practices of elicitation.
- The private and public sector jointly develop and implement security procedures and awareness training in order to mitigate, prevent, and detect incidents of surveillance.
- Where no mechanism currently exists, the private and public sector jointly establish a secure reporting chain and protocol for use of the information for suspected and known attempts and incidents of elicitation and surveillance.

Group IV. Canadian Nuclear Power Sector

The U.S. nuclear power plants affected by the August 14 blackout performed as designed. After reviewing the design criteria and the response of the plants, the U.S. members of the Nuclear Working Group had no recommendations relative to the U.S. nuclear power plants.

As discussed in Chapter 8, Canadian nuclear power plants did not trigger the power system outage or contribute to its spread. Rather, they disconnected from the grid as designed. The Canadian members of the Nuclear Working Group have, therefore, no specific recommendations with respect to the design or operation of Canadian nuclear plants that would improve the reliability of the Ontario electricity grid. The Canadian Nuclear Working Group, however, made two recommendations to improve the response to future events involving the loss of off-site power, one concerning backup electrical generation equipment to the CNSC's Emergency Operations Centre and another concerning the use of adjuster rods during future events involving the loss of off-site power. The Task Force accepted

these recommendations, which are presented below.

45. The Task Force recommends that the Canadian Nuclear Safety Commission request Ontario Power Generation and Bruce Power to review operating procedures and operator training associated with the use of adjuster rods.

OPG and Bruce Power should review their operating procedures to see whether alternative procedures could be put in place to carry out or reduce the number of system checks required before placing the adjuster rods into automatic mode. This review should include an assessment of any regulatory constraints placed on the use of the adjuster rods, to ensure that risks are being appropriately managed.

Current operating procedures require independent checks of a reactor's systems by the reactor operator and the control room supervisor before the reactor can be put in automatic mode to allow the reactors to operate at 60% power levels. Alternative procedures to allow reactors to run at 60% of power while waiting for the grid to be re-established may reduce other risks to the health and safety of Ontarians that arise from the loss of a key source of electricity. CNSC oversight and approval of any changes to operating procedures would ensure that health and safety, security, or the environment are not compromised. The CNSC would assess the outcome of the proposed review to ensure that health and safety, security, and the environment would not be compromised as a result of any proposed action.

46. The Task Force recommends that the Canadian Nuclear Safety Commission purchase and install backup generation equipment.

In order to ensure that the CNSC's Emergency Operations Center (EOC) is available and fully functional during an emergency situation requiring CNSC response, whether the emergency is nuclear-related or otherwise, and that staff needed to respond to the emergency can be accommodated safely, the CNSC should have backup electrical generation equipment of sufficient capacity to provide power to the EOC, telecommunications and Information Technology (IT) systems and accommodations for the CNSC staff needed to respond to an emergency.

The August 2003 power outage demonstrated that the CNSC's Emergency Operations Center, IT, and communications equipment are vulnerable if there is a loss of electricity to the Ottawa area.

Endnotes

[1] In fairness, it must be noted that reliability organizations in some areas have worked diligently to implement recommendations from earlier blackouts. According to the *Initial Report by the New York State Department of Public Service on the August 14, 2003 Blackout*, New York entities implemented all 100 of the recommendations issued after the New York City blackout of 1977.

[2] The need for a systematic recommitment to reliability by all affected organizations was supported in various ways by many commenters on the *Interim Report*, including Anthony J. Alexander, FirstEnergy; David Barrie, Hydro One Networks, Inc.; Joseph P. Carson, P.E.; Harrison Clark; F. J. Delea, J.A. Casazza, G.C. Loehr, and R. M. Malizewski, Power Engineers Seeking Truth; Ajay Garg and Michael Penstone, Hydro One Networks, Inc.; and Raymond K. Kershaw, International Transmission Company.

[3] See supporting comments expressed by Anthony J. Alexander, FirstEnergy; Deepak Divan, SoftSwitching Technologies; Pierre Guimond, Canadian Nuclear Association; Hans Konow, Canadian Electricity Association; Michael Penstone, Hydro One Networks, Inc.; and James K. Robinson, PPL.

[4] See "The Economic Impacts of the August 2003 Blackout," Electric Consumers Resource Council (ELCON), February 2, 2004.

[5] The need for action to make standards enforceable was supported by many commenters, including David Barrie, Hydro One Networks, Inc.; Carl Burrell, IMO Ontario; David Cook, North American Electric Reliability Council; Deepak Divan, SoftSwitching Technologies; Charles J. Durkin, Northeast Power Coordinating Council; David Goffin, Canadian Chemical Producers' Association; Raymond K. Kershaw, International Transmission Company; Hans Konow, Canadian Electricity Association; Barry Lawson, National Rural Electric Cooperative Association; William J. Museler, New York Independent System Operator; Eric B. Stephens, Ohio Consumers' Counsel; Gordon Van Welie, ISO New England, Inc.; and C. Dortch Wright, on behalf of James McGreevey, Governor of New Jersey.

[6] This recommendation was suggested by some members of the Electric System Working Group.

[7] The need to evaluate and where appropriate strengthen the institutional framework for reliability management was supported in various respects by many commenters, including Anthony J. Alexander, FirstEnergy Corporation; David Barrie, Hydro One Networks, Inc.; Chris Booth, Experienced Consultants LLC; Carl Burrell, IMO Ontario;Linda Campbell, Florida Reliability Coordinating Council; Linda Church Ciocci, National Hydropower Association; David Cook, NERC; F.J. Delea, J.A. Casazza, G.C. Loehr, and R.M. Malizewski, Power Engineers Seeking Truth; Charles J. Durkin, Northeast Power Coordinating Council; Ajay Garg and Michael Penstone, Hydro One Networks, Inc.; Michael W. Golay, Massachusetts Institute of Technology; Leonard S. Hyman, Private Sector Advisors, Inc; Marija Ilic, Carnegie Mellon University; Jack Kerr, Dominion Virginia Power; Raymond K. Kershaw,

International Transmission Company; Paul Kleindorfer, University of Pennsylvania; Michael Kormos, PJM Interconnection; Bill Mittelstadt, Bonneville Power Administration; William J. Museler, New York Independent System Operator; James K. Robinson, PPL; Eric B. Stephens, Ohio Consumers' Counsel; John Synesiou, IMS Corporation; Gordon Van Welie, ISO New England; Vickie Van Zandt, Bonneville Power Administration; and C. Dortch Wright, on behalf of James McGreevey, Governor of New Jersey.

[8] Several commenters noted the importance of clarifying that prudently incurred reliability expenses and investments will be recoverable through regulator-approved rates. These commenters include Anthony J. Alexander, FirstEnergy Corporation; Deepak Divan, SoftSwitching Technologies; Stephen Fairfax, MTechnology, Inc.; Michael W. Golay, Massachusetts Institute of Technology; Pierre Guimond, Canadian Nuclear Association; Raymond K. Kershaw, International Transmission Company; Paul R. Kleindorfer, University of Pennsylvania: Hans Konow, Canadian Electricity Association; Barry Lawson, National Rural Electric Cooperative Association; and Michael Penstone, Hydro One Networks, Inc.

[9] The concept of an ongoing NERC process to track the implementation of existing and subsequent recommendations was initated by NERC and broadened by members of the Electric System Working Group. See comments by David Cook, North American Electric Reliability Council.

[10] This recommendation was suggested by NERC and supported by members of the Electric System Working Group.

[11] See comments by Jack Kerr, Dominion Virginia Power, and Margie Phillips, Pennsylvania Services Integration Consortium.

[12] The concept of a "reliability impact consideration" was suggested by NERC and supported by the Electric System Working Group.

[13] The suggestion that EIA should become a source of reliability data and information came from a member of the Electric System Working Group.

[14] Several commenters raised the question of whether there was a linkage between the emergence of competition (or increased wholesale electricity trade) in electricity markets and the August 14 blackout. See comments by Anthony J. Alexander, FirstEnergy Corporation; F.J. Delea, J.A. Casazza, G.C. Loehr, and R.M. Malizewski, Power Engineers Seeking Truth; Ajay Garg and Michael Penstone, Hydro One Networks, Inc.; Brian O'Keefe, Canadian Union of Public Employees; Les Pereira; and John Wilson.

[15] NIMBY: "Not In My Back Yard."

[16] Several commenters either suggested that government agencies should expand their research in reliability-related topics, or emphasized the need for such R&D more generally. See comments by Deepak Divan, SoftSwitching Technologies; Marija Ilic, Carnegie Mellon University; Hans Konow, Canadian Electricity Association; Stephen Lee, Electric Power Research Institute; James K. Robinson, PPL; John Synesiou, IMS Corporation; and C. Dortch Wright on behalf of Governor James McGreevey of New Jersey.

[17] The concept of a standing framework for grid-related investigations was initiated by members of the Electric System Working Group, after noting that the U.S. National Aeronautics and Space Administration (NASA) had created a similar arrangement after the *Challenger* explosion in 1986. This framework was put to use immediately after the loss of the shuttle *Columbia* in 2003.

[18] This subject was addressed in detail in comments by David Cook, North American Electric Reliability Council; and in part by comments by Anthony J. Alexander, FirstEnergy Corporation; Ajay Garg, Hydro One Networks, Inc.; George Katsuras, IMO Ontario; and Vickie Van Zandt, Bonneville Power Administration.

[19] U.S. Federal Energy Regulatory Commission, 105 FERC ¶ 61,372, December 24, 2003.

[20] See ECAR website, http://www.ecar.org/documents/document%201_6-98.pdf.

[21] See NERC website, http://www.nerc.com/standards/.

[22] The need to ensure better maintenance of required electrical clearances in transmission right of way areas was emphasized by several commenters, including Richard E. Abbott, arborist; Anthony J. Alexander, FirstEnergy Corporation; David Barrie, Hydro One Networks, Inc.; David Cook, North American Electric Reliability Council; Ajay Garg and Michael Penstone, Hydro One Networks, Inc.; Tadashi Mano, Tokyo Electric Power Company; Eric B. Stephens, Ohio Consumers' Counsel; Vickie Van Zandt, Bonneville Power Administration; and Donald Wightman, Utility Workers Union of America.

[23] *Utility Vegetation Management Final Report*, CN Utility Consulting, LLC, March 2004, commissioned by the U.S. Federal Energy Regulatory Commission to support the investigation of the August 14, 2003 blackout.

[24] The need to strengthen and verify compliance with NERC standards was noted by several commenters. See comments by David Barrie, Hydro One Networks, Inc.; Carl Burrell, IMO Ontario; David Cook, North American Electric Reliability Council; and Eric B. Stephens, Ohio Consumers' Counsel.

[25] The need to verify application of NERC standards via readiness audits—before adverse incidents occur—was noted by several commenters. See comments by David Barrie, Hydro One Networks, Inc.; David Cook, North American Electric Reliability Council; Barry Lawson, National Rural Electric Cooperative Association; Bill Mittelstadt, Bonneville Power Administration; and Eric B. Stephens, Ohio Consumers' Counsel.

[26] The need to improve the training and certification requirements for control room management and staff drew many comments. See comments by David Cook, North American Electric Reliability Council; F.J. Delea, J.A. Casazza, G.C. Loehr, and R.M. Malizewski, Power Engineers Seeking Truth; Victoria Doumtchenko, MPR Associates; Pat Duran, IMO Ontario; Ajay Garg and Michael Penstone, Hydro One Networks, Inc.; George Katsuras, IMO Ontario; Jack Kerr, Dominion Virginia Power; Tim Kucey, National Energy Board, Canada; Stephen Lee, Electric Power Research Institute; Steve Leovy, personal comment; Ed Schwerdt, Northeast Power Coordinating Council; Tapani O. Seppa, The Valley Group, Inc.; Eric B. Stephens, Ohio Consumers' Counsel; Vickie Van Zandt, Bonneville Power Company; Don Watkins, Bonneville Power Administration; and Donald Wightman, Utility Workers Union of America.

[27] This reliance, and the risk of an undue dependence, is often unrecognized in the industry.

[28] Many parties called for clearer statement of the roles, responsibilities, and authorities of control areas and reliability coordinators, particularly in emergency situations. See comments by Anthony J. Alexander, FirstEnergy Corporation; Chris Booth, Experienced Consultants LLC; Michael Calimano, New York ISO; Linda Campbell, Florida Reliability Coordinating Council; David Cook, North American Electric

Reliability Council; F.J. Delea, J.A. Casazza, G.C. Loehr, and R.M. Malizewski, Power Engineers Seeking Truth; Mark Fidrych, Western Area Power Authority; Ajay Garg and Michael Penstone, Hydro One Networks, Inc.; Carl Hauser, Washington State University; Stephen Kellat; Jack Kerr, Dominion Virginia Power; Raymond K. Kershaw, International Transmission Company; Michael Kormos, PJM Interconnection; William J. Museler, New York Independent System Operator; Tapani O. Seppa, The Valley Group, Inc.; John Synesiou, IMS Corporation; Gordon Van Welie, ISO New England, Inc.; Vickie Van Zandt, Bonneville Power Administration; Kim Warren, IMO Ontario; and Tom Wiedman, Consolidated Edison. Members of the Electric System Working Group initiated the concept of defining an "alert" status, between "normal" and "emergency," and associated roles, responsibilities, and authorities.

[29] The need to make better use of system protection measures received substantial comment, including comments by James L. Blasiak, International Transmission Company; David Cook, North American Electric Reliability Council; Charles J. Durkin, Northeast Power Coordinating Council; F.J. Delea, J.A. Casazza, G.C. Loehr, and R.M. Malizewski, Power Engineers Seeking Truth; Ajay Garg and Michael Penstone, Hydro One Networks, Inc.; Gurgen and Spartak Hakobyan, personal study; Marija Ilic, Carnegie Mellon University; Shinichi Imai, Tokyo Electric Power Company; Jack Kerr, Dominion Virginia Power; Stephen Lee, Electric Power Research Institute; Ed Schwerdt, Northeast Power Coordinating Council; Robert Stewart, PG&E; Philip Tatro, National Grid Company; Carson Taylor, Bonneville Power Administration; Vickie Van Zandt, Bonneville Power Company; Don Watkins, Bonneville Power Administration; and Tom Wiedman, Consolidated Edison.

[30] The subject of developing and adopting better real-time tools for control room operators and reliability coordinators drew many comments, including those by Anthony J. Alexander, FirstEnergy Corporation; Eric Allen, New York ISO; Chris Booth, Experienced Consultants, LLC; Mike Calimano, New York ISO; Claudio Canizares, University of Waterloo (Ontario); David Cook, North American Electric Reliability Council; Deepak Divan, SoftSwitching Technologies Victoria Doumtchenko, MPR Associates; Pat Duran, IMO Ontario; Bill Eggertson, Canadian Association for Renewable Energies; Ajay Garg and Michael Penstone, Hydro One Networks, Inc.; Jack Kerr, Dominion Virginia Power; Raymond K. Kershaw, International Transmission Company; Michael Kormos, PJM Interconnection; Tim Kucey, National Energy Board, Canada; Steve Lapp, Lapp Renewables; Stephen Lee, Electric Power Research Institute; Steve Leovy; Tom Levy; Peter Love, Canadian Energy Efficiency Alliance; Frank Macedo, Hydro One Networks, Inc.; Bill Mittelstadt, Bonneville Power Administration; Fiona Oliver, Canadian Energy Efficiency Alliance; Peter Ormund, Mohawk College; Don Ross, Prince Edward Island Wind Co-op Limited; James K. Robinson, PPL; Robert Stewart, PG&E; John Synesiou, IMS Corporation; Gordon Van Welie, ISO New England, Inc.; Vickie Van Zandt, Bonneville Power Administration; Don Watkins, Bonneville Power Administration; Chris Winter, Conservation Council of Ontario; David Zwergel, Midwest ISO. The concept of requiring annual testing and certification of operators' EMS and SCADA systems was initiated by a member of the Electric System Working Group. Also, see comments by John Synesiou, IMS Corporation.

[31] The need to strengthen reactive power and voltage control practices was the subject of several comments. See comments by Claudio Canizares, University of Waterloo (Ontario); David Cook, North American Electric Reliability Council; F.J. Delea, J.A. Casazza, G.C. Loehr, and R.M. Malizewski, Power Engineers Seeking Truth; Stephen Fairfax, MTechnology, Inc.; Ajay Garg and Michael Penstone, Hydro One Networks, Inc.; Shinichi Imai and Toshihiko Furuya, Tokyo Electric Power Company; Marija Ilic, Carnegie Mellon University; Frank Macedo, Hydro One Networks, Inc.; and Tom Wiedman, Consolidated Edison. Several commenters addressed issues related to the production of reactive power by producers of power for sale in wholesale markets. See comments by Anthony J. Alexander, FirstEnergy Corporation; K.K. Das, PowerGrid Corporation of India, Limited; F.J. Delea, J.A. Casazza, G.C. Loehr, and R.M. Malizewski, Power Engineers Seeking Truth; Stephen Fairfax, MTechnology, Inc.; and Carson Taylor, Bonneville Power Administration.

[32] See pages 107-108.

[33] U.S. Federal Energy Regulatory Commission, 105 FERC ¶ 61,372, December 24, 2003.

[34] The need to improve the quality of system modeling data and data exchange practices received extensive comment. See comments from Michael Calimano, New York ISO; David Cook, North American Electric Reliability Council; Robert Cummings, North American Electric Reliability Council; F.J. Delea, J.A. Casazza, G.C. Loehr, and R.M. Malizewski, Power Engineers Seeking Truth; Mark Fidrych, Western Area Power Administration; Jack Kerr, Dominion Virginia Power; Raymond K. Kershaw, International Transmission Company; Frank Macedo, Hydro One Networks, Inc.; Vickie Van Zandt, Bonneville Power Administration; Don Watkins, Bonneville Power Administration; and David Zwergel, Midwest ISO.

[35] Several commenters addressed the subject of NERC's standards in various respects, including Anthony J. Alexander, FirstEnergy Corporation; Carl Burrell, IMO Ontario; David Cook, North American Electric Reliability Council; F.J. Delea, J.A. Casazza, G.C. Loehr, and R.M. Malizewski, Power Engineers Seeking Truth; Charles J. Durkin, Northeast Power Coordinating Council; Ajay Garg and Michael Penstone, Hydro One Networks, Inc.; Jack Kerr, Dominion Virginia Power; James K. Robinson, PPL; Mayer Sasson, New York State Reliability Council; and Kim Warren, IMO Ontario.

[36] See *Initial Report by the New York State Department of Public Service on the August 14, 2003 Blackout* (2004), and comments by Mayer Sasson, New York State Reliability Council.

[37] F.J. Delea, J.A. Casazza, G.C. Loehr, and R.M. Malizewski, "The Need for Strong Planning and Operating Criteria to Assure a Reliable Bulk Power Supply System," January 29, 2004.

[38] The need to tighten communications protocols and improve communications systems was cited by several commenters. See comments by Anthony J. Alexander, FirstEnergy Corporation; David Barrie, Hydro One Networks, Inc.; Carl Burrell, IMO Ontario; Michael Calimano, New York ISO; David Cook, North American Electric Reliability Council; Mark Fidrych, Western Area Power Administration; Ajay Garg and Michael Penstone, Hydro One Networks, Inc.; Jack Kerr, Dominion Virginia Power; William Museler, New York ISO; John Synesiou, IMS Corporation; Vickie Van Zandt, Bonneville Power Administration; Don Watkins, Bonneville Power Administration; Tom Wiedman, Consolidated Edison.

[39] See comments by Tapani O. Seppa, The Valley Group, Inc.

[40] Several commenters noted the need for more systematic use of time-synchronized data recorders. In particular, see David Cook, North American Electric Reliability Council; Ajay Garg and Michael Penstone, Hydro One Networks, Inc.; and Robert Stewart, PG&E.

[41] The importance of learning from the system restoration experience associated with the August 14 blackout was stressed by Linda Church Ciocci, National Hydropower Association; David Cook, North American Electric Reliability Council; Frank Delea; Bill Eggertson, Canadian Association for Renewable Energies; Stephen Lee, Electric Power Research Institute; and Kim Warren, IMO Ontario.

[42] The need to clarify the criteria for identifying critical facilities and improving dissemination of updated information about unplanned outages was cited by Anthony J. Alexander, FirstEnergy Corporation; and Raymond K. Kershaw, International Transmission Company.

[43] The need to streamline the TLR process and limit the use of it to non-urgent situations was discussed by several commenters, including Anthony J. Alexander, FirstEnergy Corporation; Carl Burrell, IMO Ontario; Jack Kerr, Dominion Virginia Power; Raymond K. Kershaw, International Transmission Company; and Ed Schwerdt, Northeast Power Coordinating Council.

[44] NERC Standards at www.nerc.com (Urgent Action Standard 1200, Cyber Security, Reliability Standard 1300, Cyber Security) and Joint DOE/PCIB standards guidance at www.ea.doe.gov/pdfs/21stepsbooklet.pdf ("21 Steps to Improve Cyber Security of SCADA Networks").

[45] For example: "21 Steps to Improve Cyber Security of SCADA Networks," http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf.

[46] Canadian reference: http://www.dfait-maeci.gc.ca/anti-terrorism/actionplan-en.asp; U.S. reference: http://www.whitehouse.gov/news/releases/2001/12/20011212-6.html.

[47] A "black box" technology is any device, sometimes highly important, whose workings are not understood by or accessible to its user.

[48] DOE Form 417 is an example of an existing, but underutilized, private/public sector information sharing mechanism.