

Agenda Board of Trustees

May 9, 2012 | 8:00 a.m.-12:00 p.m. Eastern

Westin Arlington Gateway
801 North Glebe Road
Arlington, VA 22203
703-717-6200

Introductions and Chair's Remarks

NERC Antitrust Compliance Guidelines and Public Announcement

Consent Agenda — Approve

1. **Minutes***
 - a. March 14, 2012
 - b. February 23, 2012
 - c. February 9, 2012
2. **Election/Membership Appointments and Changes***
 - a. Personnel Certification Governance Committee
 - b. Compliance and Certification Committee

Regular Agenda

3. **Remarks by Commissioner John Norris**
4. **Remarks by Commissioner Cheryl LaFleur**
5. **President's Report**
6. **Standards***
 - a. FAC-003-3 – Transmission Vegetation Management Program — **Adopt**
 - b. PRC-005-1.1b – Transmission and Generation Protection System Maintenance and Testing — **Adopt**
 - c. TOP-001-2-Transmission Operations; TOP-002-3-Operations Planning; and TOP-003-2-Operational Reliability Data—Real-Time Operations — **Adopt**
 - d. Interpretation 2010-05 of CIP-002-1 for Duke Energy — **Adopt**

~~e. ReliabilityFirst Corporation Regional Standards Development Procedure — Approve~~

The changes to the ReliabilityFirst Corporation Regional Standards Development Procedure are being removed from this agenda so that they can be presented concurrently with related changes to ReliabilityFirst Bylaws and amendments to the NERC-RFC Delegation Agreement during the May 24 Board of Trustees conference call.

- f. Western Electricity Coordinating Council Regional Variance — **Adopt**
- g. Update on Frequency Response (Project 2007-12) — **Discussion**
- h. **Request to Shorten Comment Period for Proposed Data Request Under Section 1606 of the NERC Rules of Procedure — Approve**
- 7. **Proposed Amendments to Delegation Agreement with Midwest Reliability Organization (MRO) – Amended Exhibit B (MRO Bylaws)* — Approve**
- 8. **Proposed Renewal Agreement Between SERC Reliability Corporation and Florida Reliability Coordinating Council and Between SERC Reliability Corporation and Southwest Power Pool, Inc.* — Approve**
- 9. **MRC Standards Process Input Group Recommendations* — Discussion**
- 10. **2012 State of Reliability Report* — Review and Accept**
- 11. **Severe Impact Resilience: Considerations and Recommendations Report* — Review and Accept**
- 12. **Cyber Attack Task Force Report* — Review and Accept**
- 13. **Electricity Sector Information Sharing and Analysis Center (ES-ISAC) Update: Enhancing Capability* — Information**
- 14. **Legislative and External Affairs Update* — Information**

Standing Committee Reports* (Item 15)

- a. Operating Committee
- b. Planning Committee
- c. Critical Infrastructure Protection Committee
 - i. Strategic Work Plan
- d. Member Representatives Committee
- e. Personnel Certification Governance Committee
- f. Standards Committee
- g. Compliance and Certification Committee
- h. Electricity Sub-Sector Coordinating Council

Forum and Group Reports* (Item 16)

- a. North American Energy Standards Board
- b. Regional Entity Management Group
- c. North American Transmission Forum
- d. North American Generator Forum

Board Committee Reports**17. Corporate Governance and Human Resources**

- a. Approve Amendments to Savings and Investment Plan
- b. Risk Management and Internal Controls Subcommittee Mandate

18. Compliance**19. Finance and Audit**

- a. Approve 2011 Audited Financial Statements
- b. Accept First Quarter Statement of Activities
- c. Status of NERC 2013 Business Plan and Budget and Process for Reviewing Regional Entities' Business Plans and Budgets

20. Standards Oversight and Technology

*Background materials included.

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Draft Minutes Board of Trustees

March 14, 2012 | 2:00 p.m. Eastern
Conference Call

Chair John Q. Anderson convened a duly noticed open meeting by conference call of the Board of Trustees of the North American Electric Reliability Corporation on March 14, 2012 at 2:00 p.m. Eastern. As required by the bylaws of the Corporation, dial-in listen-only access was provided to members of the Corporation and the public for the meeting. The agenda is attached as **Exhibit A**.

Trustees present on the call in addition to Chair Anderson were Vicky Bailey, Paul Barber, Tom Berry, Fred Gorbet, Ken Peterson, Jan Schori, Roy Thilly, Janice Case, Bruce Scherr and President and CEO Gerry Cauley. Additional attendees are listed in **Exhibit B**.

Antitrust Compliance Guidelines

David Cook, vice president and general counsel, directed the participants' attention to the NERC Antitrust Compliance Guidelines.

NERC Rules of Procedure: Substantive Revisions

Mr. Cook reviewed and recommended for approval the substantive revisions to the NERC Rules of Procedure that had been circulated with the agenda package (**Exhibit C**), with one exception. Mr. Cook recommended that the Board defer action on the proposed changes to Section 500 and Appendix 5A to the Board's May 2012 meeting, to allow time for further discussion with stakeholders on issues related to those items. After discussion by the Trustees and on motion by Paul Barber, the Board approved the proposed changes to the Rules of Procedure, with the exception that action on the proposed changes to Section 500 and Appendix 5A be deferred.

There being no further business, the call was terminated at 2:45 p.m.

Submitted by,



David N. Cook
Secretary

Draft Minutes Board of Trustees

February 23, 2012 | 2:00 p.m. Eastern
Conference Call

Chair John Q. Anderson convened a duly noticed open meeting by conference call of the Board of Trustees of the North American Electric Reliability Corporation on February 23, 2012 at 2:00 p.m. Eastern. As required by the bylaws of the Corporation, dial-in listen-only access was provided to members of the Corporation and the public for the meeting. The agenda is attached as **Exhibit A**.

Trustees present on the call in addition to Chair Anderson were Vicky Bailey, Paul Barber, Tom Berry, Fred Gorbet, David Goulding, Ken Peterson, Jan Schori, Roy Thilly, Janice Case, Bruce Scherr and President and CEO Gerry Cauley. Additional attendees are listed in **Exhibit B**.

Antitrust Compliance Guidelines

David Cook, vice president and general counsel, directed the participants' attention to the NERC Antitrust Compliance Guidelines.

Geomagnetic Disturbance Task Force Report

Chair Anderson referred the Trustees to the report as presented in the Agenda package (**Exhibit C**) and opened to questions and or comments from the members. After significant discussion and on motion by Fred Gorbet, the Board approved the following resolution:

RESOLVED, that the Board accepts the proposed Geomagnetic Disturbance Task Force Report, subject to its being revised in accordance with the discussion during the meeting, that the Board approves the release of the report as so modified, and that the Board endorses the recommendations in the report.

Proposed Amendments to Delegation Agreement with SERC Reliability Corporation – Amended Exhibit B (SERC Bylaws)

Mr. Cook reviewed and presented for approval the Proposed Amendments to Delegation Agreement with SERC Reliability Corporation – Amended Exhibit B (SERC Bylaws) (**Exhibit D**). Following discussion, on motion by Bruce Scherr the Board approved the following resolution:

WHEREAS, the SERC Board of Directors, acting in accordance with the SERC Bylaws at a meeting on October 26, 2011, approved certain amendments to the SERC Bylaws, as set forth in Agenda Item 2 of the NERC Board of Trustees agenda for its February 23, 2012 meeting (the "Amendments"); and

WHEREAS, on January 18, 2012, SERC requested that NERC approve the Amendments and file them with the Federal Energy Regulatory Commission for approval; and

WHEREAS, the NERC Board of Trustees finds that SERC followed appropriate procedures in adopting the Amendments and that the Amendments are consistent with SERC's obligations and responsibilities under the delegation agreement between NERC and SERC and otherwise meet the requirements set forth in 18 C.F.R. §39.10 of the Commission's regulations; and

WHEREAS, the Amendments will constitute amendments to the Amended and Restated Delegation Agreement between NERC and SERC, in the form of amendments to Exhibit B – the SERC Bylaws,

RESOLVED, that the Board approves the proposed amendments to the Amended and Restated Delegation Agreement between NERC and SERC;

FURTHER RESOLVED, that NERC staff shall make the appropriate filings with the Federal Energy Regulatory Commission.

2012 NERC Corporate Performance Measures

Mr. Cauley reviewed and presented for approval NERC's 2012 Corporate Performance Measures highlighting the areas amended based on the input received during the Member Representatives Committee and Board of Trustees' February 2012 meetings.

On motion by Fred Gorbet the Board approved the 2012 NERC Corporate Performance Measures as presented (**Exhibit E**).

Personnel Certification Governance Committee Manual

Rebecca Michael, associate general counsel, reviewed and presented for acceptance the Personnel Certification Governance Committee Manual (**Exhibit F**). Ms. Michael noted if the manual is accepted Appendix 6 will be removed from NERC's Rules of Procedure. Following discussion, on motion by Bruce Scherr the Board approved the Manual as presented.

There being no further business, the call was terminated at 2:41 p.m.

Submitted by,



David N. Cook
Secretary

Draft Minutes Board of Trustees

February 9, 2012 | 8:00 a.m.-12:00 p.m. Mountain

Arizona Grand Resort
8000 S. Arizona Grand Parkway
Phoenix, AZ 85044
602-438-9000

Chair John Q. Anderson called to order a duly noticed meeting of the North American Electric Reliability Corporation Board of Trustees on February 9, 2012 at 8 a.m., local time, and a quorum was declared present. The Agenda and list of attendees are attached as **Exhibits A** and **B**, respectively.

NERC Antitrust Compliance Guidelines

David Cook, senior vice president and general counsel, directed participants' attention to the NERC Antitrust Compliance Guidelines included in the agenda.

Executive Session

Chairman Anderson reported that, as is its custom, the board met in executive session before the open meeting, without the chief executive officer present, to review management activities.

Consent Agenda

On motion of President and CEO Gerry Cauley, the board approved the consent agenda, as follows:

Minutes

The board approved the following draft minutes (**Exhibit C**):

- January 18, 2012 Conference Call
- November 22, 2011 Conference Call
- November 18, 2011 Conference Call
- November 3, 2011 Meeting

Committee Membership Appointments and Charter Changes

The board approved the proposed nominations to the membership of the Compliance and Certification, and Critical Infrastructure Protection committees (**Exhibit D**).

President's Report

Mr. Cauley's report addressed a look back at 2011 and looking forward to 2012, noting items of priority in 2011: reliability concerns, risk-based approaches, accountability, learning industry are all still priorities for 2012. The challenge for 2012 is continuing to turn those priorities into actionable goals.

Mr. Cauley reviewed additional items of focus for 2012: (i) the cold weather event and determining the necessary interventions, if any to ensure that this type of event does not reoccur, (ii) work with the Regional Entities in areas such as relay protection and human performance and begin to identify specific risk areas and solutions, (iii) based on industry feedback regarding the deratings and the transition implementation and the burden in terms of cost, look for opportunities on how that cost burden can be lessened while still ensuring a sustainable program; (iv) continue to focus on cyber security and NERC's readiness and resilience in terms of high impact, low frequency (HILF) events.

In conclusion, Mr. Cauley stated in 2012 NERC and the Regional Entities need to continue to ensure the strength of the compliance programs and that the enforcement actions are consistent and meaningful for reliability and further the understanding of the relationship of the compliance programs to reliability of the bulk power system.

Elections

Chair Anderson reviewed the items for approval and on motion of Ms. Janice Case, the board elected the following officers for 2012:

- John Q. Anderson as Chairman of the Board
- Fred Gorbet as Vice Chairman and Chairman-Elect
- Gerry Cauley as President and Chief Executive Officer

And on the recommendation of CEO Gerry Cauley and the motion of Janice Case, the board appointed the following additional officers:

- David Cook, Senior Vice President, Corporate Secretary, and General Counsel
- Michael Walker, Senior Vice President, Chief Financial and Administrative Officer, and Treasurer
- David Nevius, Senior Vice President
- Mark Lauby, Vice President and Director of Reliability Assessment and Performance Analysis
- Janet Sena, Vice President and Director of Policy and External Affairs
- Herb Schrayshuen, Vice President and Director of Standards and Training

Board of Trustees Self-Assessment Results

Chair Anderson provided an overview of the Board of Trustees Self-Assessment results, as well as the Member Representatives Committee (MRC) Effectiveness of the Board Survey results. Mr. Anderson stated the results are extremely useful to the board and they will address the noted areas of concern.

Electric Reliability Organization Enterprise Strategic Plan 2013-2015

Mr. Cauley noted the version of the ERO Enterprise Strategic Plan as presented is a refresh from the previous year and organized into three distinct focus areas: (i) standards and compliance, (ii) problem solving and risk-based controls, and (iii) collaboration and utilization of all resources in the industry. Mr. Cauley stated there are currently 33 targets that formulate the new plan. He also acknowledged the feedback from the MRC meeting and agreed to complete a review and pare down any applicable

targets. Further, Mr. Cauley committed to the board to modify the style from target/stretch to target/threshold, as well complete the allocations across program areas and bring back to the board during its February 23, 2012 conference call.

Reliability Standards

Herb Schrayshuen, vice president of standards and training, gave a presentation on the Reliability Standards Program (**Exhibit E**) and presented the following items for board action.

Project 2010-07: Generator Requirements at the Transmission Interface

Following discussion among the trustees, on motion of Ken Peterson, the board approved the following resolutions:

RESOLVED, that the board approves the proposed Reliability Standard FAC-001-1 – Facility Connection Requirements and the associated Violation Risk Factors (VRFs), Violation Severity Levels (VSLs) and implementation plan for FAC-001-1;

FURTHER RESOLVED, that the board approves Reliability Standard PRC-004-2.1a – Analysis and Mitigation of Transmission and Generation Protection System Misoperations and the associated implementation plan for PRC-004-2.1a;

FURTHER RESOLVED, that the board approves the retirement of FAC-001-0 – Facility Connection Requirements at midnight of the day immediately prior to the effective date of FAC-001-1, and the retirement of PRC-004-2a – Analysis and Mitigation of Transmission and Generation Protection System Misoperations at midnight of the day immediately prior to the effective date of PRC-004-2.1a.

FURTHER RESOLVED, that Reliability Standards FAC-001-1 – Facility Connection Requirements and PRC-004-2.1a – Analysis and Mitigation of Transmission and Generation Protection System Misoperations shall not be filed at the present time but shall be held, pending completion of development activities on Reliability Standards FAC-003-3 and PRC-005-1.1a, with the expectation that Reliability Standards FAC-003-3 and PRC-005-1.1a, along with a technical analysis of remaining issues, will be presented to the board at its May 2012 meeting.

Project 2008-10 Interpretation of CIP-006

On motion of Ken Peterson, the board approved the following resolutions:

RESOLVED, that the board approves the proposed interpretation of requirement R1.1 of CIP-006- — Cyber Security — Physical Security of Critical Cyber Assets

FURTHER RESOLVED, that NERC Staff shall make the appropriate filings with ERO governmental authorities.

Project 2009-22 Interpretation of COM-002-2

Janice Case moved to approve the proposed Interpretation of Reliability Standard COM-002-2, and the motion received a second. After extended discussion, Tom Berry moved to amend the motion to add a direction to the Standards Committee to complete developmental activities on proposed Reliability Standard COM-003 on a high priority basis and a further direction that a memorandum describing best communications practices, including appropriate use of three-step communications, be sent to registered entities promptly.

After further discussion, the vote on the amendment to the motion was Trustees Anderson, Berry, Case, Cauley, Gorbet, Goulding, Peterson, Scherr, Schori, and Thilly voting in the affirmative, no Trustees voting in the negative, and Trustee Barber abstaining. The amendment to the motion passed (10-0-1). The vote on the motion as amended was Trustees Anderson, Berry, Case, Gorbet, Goulding, Peterson, Scherr, Schori, and Thilly voting in the affirmative, Trustee Barber voting in the negative, and Trustee Cauley abstaining. The motion, as amended, passed (9-1-1).

The motion, as amended, approved the following resolutions:

RESOLVED, that the board approves the proposed Interpretation of COM-002-2 and directs that it be filed with ERO governmental authorities;

FURTHER RESOLVED, that the board directs the Standards Committee to complete developmental activities on proposed Reliability Standard COM-003 on a high priority basis; and

FURTHER RESOLVED, that the board directs that NERC management, working with stakeholders, prepare a memorandum describing best communications practices, including appropriate use of three-step communications, to be sent to registered entities promptly.

Project 2011-INT-01-Revision of MOD-028-1

On motion of Ken Peterson, the board approved the following resolutions:

RESOLVED, that the board approves Reliability Standard MOD-028-2 – Area Interchange Methodology and the proposed implementation plan for MOD-028-2, to become effective on the first day of the first calendar quarter after applicable regulatory approval or where no regulatory approval is required, on the first day of the first calendar quarter after board approval;

FURTHER RESOLVED, that the board approves the retirement of MOD-028-1 – Area Interchange Methodology at midnight of the day immediately prior to the effective date of MOD-028-2;

FURTHER RESOLVED, that NERC staff shall make the appropriate filings with ERO governmental authorities.

The board also noted that this was the first successful use of the rapid revision process for targeted amendments to reliability standards and encouraged the Standards Committee to make further use of the process where appropriate.

Regional Standard and Standards Development Procedure

Mr. Schrayshuen also provided presentation on the Regional Standard and Standards Development Procedure (**Exhibit F**) and presented the following items for board action.

Reliability Standard PRC-006-NPCC-1 – Automatic Underfrequency Load Shedding

On motion of David Goulding, the board approved the following resolutions:

RESOLVED, that the board approves the following proposed reliability standards and associated documents:

1. Reliability Standard PRC-006-NPCC-1 – Automatic Underfrequency Load Shedding
2. Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for PRC-006-NPCC-1
3. Implementation Plan for PRC-006-NPCC-1

- (a) For the Eastern Interconnection and Québec Interconnection portions of NPCC excluding the Independent Electricity System Operator (IESO) Planning Coordinator's area of NPCC in Ontario, Canada:

The effective date for Requirements R1, R2, R3, R4, R5, R6, and R7 is the first day of the first calendar quarter following applicable regulatory approval but no earlier than January 1, 2016. The effective date for Requirements R8 through R23 is the first day of the first calendar quarter two years following applicable governmental and regulatory approval.

- (b) For the Independent Electricity System Operator (IESO) Planning Coordinator's area of NPCC in Ontario, Canada:

All requirements are effective the first day of the first calendar quarter following applicable governmental and regulatory approval but no earlier than April 1, 2017.

FURTHER RESOLVED, that NERC Staff shall make the appropriate filings with ERO governmental authorities.

The board requested that there be further discussion on the general topic of regional standards at the next board meeting.

Revision to SERC Standards Development Procedure

Mr. Cook presented a proposal for approval of amendments to the SERC standards development procedure. On motion of Bruce Scherr, the board approved the following resolutions:

RESOLVED, that the board approves the proposed Revision 2 of SERC Reliability Corporation Regional Standards Development Procedure, as an amendment to Exhibit C to the Revised Amended and Restated Delegation Agreement that NERC has with SERC by replacing the SERC Regional Standards Development Procedure Revision 1;

FURTHER RESOLVED, that NERC staff shall make the appropriate filings with ERO governmental authorities.

Amendments to NERC Rules of Procedure: Substantive Revisions

Ms. Rebecca Michael, associate general counsel, briefly discussed the proposed substantive revisions to NERC's Rules of Procedure (**Exhibit G**) and recommended that the board defer action on the amendments until its March 14 meeting.

Following discussion among the trustees, on the motion of Fred Gorbet, the board approved the following resolution:

RESOLVED,

1. That action on the proposed amendments to the NERC Rules of Procedure be deferred;
2. That comments be accepted on the current posting of the proposed amendments to the Rules of Procedure through February 17, 2012; and
3. That the board consider the proposed amendments to the Rules of Procedure, with whatever further changes may be appropriate in light of the comments received, during its conference call scheduled for March 14, 2012.

Electricity Sector–Information Sharing and Analysis Center (ES-ISAC) Policy Statement

Mr. Cook reviewed the proposed ES-ISAC Policy Statement and recommended it for approval.

Following discussion, on motion of Paul Barber, the board approved the following resolution:

RESOLVED, that the board approves the proposed policy statement on the role of the Electricity Sector–Information Sharing and Analysis Center vis-à-vis NERC's Compliance Monitoring and Enforcement Program, attached to minutes as **Exhibit H**.

Proposed Amendments to Delegation Agreement with Florida Reliability Coordinating Council (FRCC) – Amended Exhibit B (FRCC Bylaws) and Exhibit D (Compliance Monitoring and Enforcement Program)

Mr. Cook reviewed and presented for approval the requested amendments to the NERC/FRCC Delegation Agreement and noted Exhibits (**Exhibit I**).

On motion of Bruce Scherr, the board approved the following resolutions:

WHEREAS, the FRCC Board of Directors, acting in accordance with the FRCC Bylaws at a series of meetings in the Fall of 2011, approved certain amendments to the FRCC Bylaws and Compliance Monitoring and Enforcement Program, as set forth in Agenda Item 11 of the NERC Board of Trustees agenda for its February 9, 2012 meeting (the “Amendments”); and

WHEREAS, on January 10, 2012, FRCC requested that NERC approve the Amendments and file them with the Federal Energy Regulatory Commission for approval; and

WHEREAS, the NERC Board of Trustees finds that FRCC followed appropriate procedures in adopting the Amendments and that the Amendments are consistent with FRCC’s obligations and responsibilities under the delegation agreement between NERC and FRCC and otherwise meet the requirements set forth in 18 C.F.R. §39.10 of the Commission’s regulations; and

WHEREAS, the Amendments will constitute amendments to the Amended and Restated Delegation Agreement between NERC and FRCC, consisting of amendments to Exhibit B – the FRCC Bylaws, and to Exhibit D – the FRCC Compliance Monitoring and Enforcement Program,

RESOLVED, that the board approves the proposed amendments to the Amended and Restated Delegation Agreement between NERC and FRCC;

FURTHER RESOLVED, that NERC staff shall make the appropriate filings with the Federal Energy Regulatory Commission.

ERO Event Analysis Process Document

Mr. Earl Shockley, director of reliability risk management, presented for approval the ERO Event Analysis Process Document attached as (**Exhibit J**).

On motion of Paul Barber, the board approved the following resolution:

RESOLVED, that the board approves the proposed ERO Event Analysis Process Document.

Status of Action Items from NERC Three-Year ERO Performance Assessment

Mr. Dave Nevius, senior vice president, provided an update on the more significant developments in each NERC program area since the March 16, 2011 report to the board, “Progress in Implementing Specific NERC Actions from the Three-Year ERO Performance Assessment.” Details of the developments are contained in the report attached here as **Exhibit K**. Mr. Nevius provided the next steps of the process which are to create a dashboard to track the actions which will allow an efficient means to observe the progress of the actions, as well as work to show the alignment of these actions to the NERC Strategic Plan with a goal of bringing another update to the board at the May 2012 meeting.

Status of Critical Infrastructure Initiatives

Mr. Matt Blizzard, director of critical infrastructure protection provided a report on the status of NERC's various critical infrastructure initiatives (**Exhibit L**).

Government Relations Update

Ms. Janet Sena, vice president and director of policy and external affairs made a brief presentation updating the Board on certain matters of particular importance to NERC's relationships with governmental entities attached here as (**Exhibit M**).

Standing Committee Reports

Operating Committee

Tom Bowe, chair, highlighted items from the committee's written report to the Board (**Exhibit N**) to include the work completed in 2011 on event analysis, the work as part of the Geomagnetic Task Force and the SIRTf which were led by operating committee members, and frequency response. For 2012, Mr. Bowe noted the continued work with the EAWG and lessons learned, as well as actively engage in the human performance area to gain an understanding on how best to address field personnel. Mr. Jim Castle, vice chair, reviewed and presented the Operating Committee Strategic Plan for acceptance and on motion of Gerry Cauley, the board accepted the strategic plan of the NERC Operating Committee.

Planning Committee

Jeff Mitchell, chair, highlighted the accomplishments of 2011 and goals for 2012 as contained in his written report to the board (**Exhibit O**). Mr. Mitchell also reviewed the Planning Committee's Strategic Plan noting at the Planning Committee's December 2010 meeting, the Planning Committee initiated the development of a strategic plan to guide the PC and its subgroups in the development of their work plans. This Strategic Plan provides a clear focus for the NERC Planning Committee efforts over the 2011–2016 timeframe. Mr. Mitchell further noted that the strategic plan emphasizes the alignment of PC activities from several perspectives, including:

- Conforming with priorities of the NERC ERO enterprise, Federal, state/provincial regulators, and the Electricity Sub-Sector Coordinating Council (ESCC);
- Providing a technical foundation for reliability issues;
- Matching PC resources with priorities; and
- Efficiently using PC resources.

On motion of Gerry Cauley, the board agreed to add two items to the strategic plan of the NERC Planning Committee, as follows:

1. Performance Analysis Subcommittee, State of Reliability Report by end of Second Quarter of 2012; and
2. Reliability Assessment Subcommittee and Integration of Variable Generation Task Force to support ongoing work with California Independent System Operator on wind penetration.

Critical Infrastructure Protection Committee

Chuck Abell, chair, highlighted items from the committee's written report to the board (**Exhibit P**).

Member Representatives Committee

Scott Helyer, chair, noted the very beneficial discussion held during the MRC meeting acknowledging a couple of the challenges the MRC has for 2012 to include the standards process and adequate level of reliability. Mr. Helyer also committed, on behalf of the MRC, to work towards a 100 percent submission rate on the MRC Effectiveness Survey of the Board of Trustees.

Personnel Certification Governance Committee

Jake Burger, chair, highlighted items from the committee's written report to the board (**Exhibit Q**).

Standards Committee

Allen Mosher, chair, referred to the highlighted items from the committee's written report to the board (**Exhibit R**).

Compliance and Certification Committee

Chair Clay Smith provided the Compliance and Certification Committee (CCC) report highlighting key activities. Mr. Smith also reviewed and recommended acceptance of the CCC 2012 Work Plan (**Exhibit S**), as well as the 2011 Stakeholder Perception Survey (**Exhibit T**).

On motion of Gerry Cauley the board accepted the 2012 action plan of the NERC Compliance and Certification Committee and deferred action on the stakeholder survey submitted by the Committee.

Electricity Sub-Sector Coordinating Council

Stuart Brindley, consultant to NERC, presented a report to the board on the ESCC Coordinated Action Plan covering the background of the plan, where the committee is with the plan today, and what is on the horizon. The presentation is attached as (**Exhibit U**).

Forum and Group Reports**North American Energy Standards Board (NAESB)**

Mr. Michael Desselle presented a statement on behalf of NAESB:

"I want to note a milestone in our relationship: ten years ago we entered into a MOU with NERC and soon after that we collectively agreed to a MOU between our organizations and the newly formed ISO/RTO Council (also celebrating their tenth year of existence). That MOU created the Joint Interface Committee and as the trust developed between our organizations we modified our coordination processes over the years.

There was a lot of speculation at the time that this would be a rocky relationship. That never really happened because of the commitment of our Boards and the leadership of staff and participants scattered around the room here today to make this marriage work.

It continues today with the transition of the TSIN registry and efforts currently underway for the field tests on parallel Flow Visualization TLR standards.

And we are being asked to continue the collaboration on an issue critical to both our organizations. Much like the formation of the wholesale electric Quadrant with NAESB, the topic has the tendency to be highly politicized and divisive. Gerry raised it this morning as a priority for the organization and Janet discussed what NERC staff has been doing on the topic on the legislative and regulatory front and Jeffrey talked about what the Planning Committee has on its plate

It is the interdependence of the gas and electric industries and how to harmonize them.

It is a market transformative issue with implications for reliability, especially as:

- EPA regulations will limit coal as fuel source for electric generation;
- As Shale gas becomes more abundant;
- As natural gas prices continue to fall;
- As the Smart Grid comes into being; and,
- As other variable generating resources become more viable.

A year ago following the Texas cold snap and New Mexico gas freeze-offs we were advised to consider what NAESB could or should do with respect to standards on gas/electric interdependence. And subsequently within the year no less than 10 reports on the subject were issued. So we formed a Board Committee and identified 18 specific areas that may need to be reviewed. They can be characterized as falling into three buckets:

- Transparency/communication and data interdependence;
- Coordination of timelines and market functions; and,
- The identification of bottlenecks or other services.

We expect the recommendations of the Board Committee to yield:

- Decisions where NAESB should consider modifying or creating new standards; or,
- Identification of policy or other industry actions necessary before NAESB could go further (much the same as we did following the 2004 New England cold snap); or,
- Decisions that NAESB should not develop standards (that others standards organizations should or that market services should be developed).

Just as we did with the coordination of standards amongst our own organizations we are counting on the continued Board of Trustee support to provide the appropriate leadership of NERC staff and industry participation as we collectively address the implications for reliability.”

North American Transmission Forum

Tom Galloway, referred to the Forum's written report to the board (**Exhibit V**). Mr. Galloway did note that the Forum has hired one new staff member since the November 2011 board meeting and look to hire an additional five in the near future.

North American Generator Forum

Mark Bennett reviewed his report highlighting a key item: the shift to non-profit status. The new structure will consist of tiers aligning nominal dues to each tier. The proposed tiers are \$500, \$1,000 and \$2,000. Mr. Bennett acknowledged the overwhelming support during their annual meeting from attending members, as well as through the electronic vote submissions. An additional highlight, the new structure will provide necessary funds to hire a part-time administrative associate. In conclusion, Mr. Bennett noted that during the annual meeting the Forum also spent time discussing the Generator/Transmission Operator issue.

Board Committee Reports

Corporate Governance and Human Resources

Chair Janice Case provided a summary report of the Corporate Governance and Human Resources Committee (CGHRC) open meeting. Chair Case reviewed and requested board approval of the board committee assignments for 2012 and the Defined Contribution Plan.

On motion of Janice Case, the board approved the following board committee assignments for 2012:

Finance and Audit Committee

Fred Gorbet, Chair
Janice Case
Dave Goulding
Roy Thilly

Compliance Committee

Bruce Scherr, Chair
Vicky Bailey
Ken Peterson
Jan Schori
Roy Thilly

Corporate Governance & Human Resources Committee

Janice Case, Chair
Vicky Bailey
Tom Berry
Jan Schori

Standards Oversight & Technology Committee

Ken Peterson, Chair
Paul Barber
Tom Berry
Dave Goulding
Bruce Scherr

Nominating Committee

Jan Schori, Chair
Paul Barber
Janice Case
Fred Gorbet

Ken Peterson
Bruce Scherr
Roy Thilly
5 MRC Representatives

Ex officio to all: John Q. Anderson

Chairman Anderson announced he was appointing Paul Barber to be the NERC independent trustee member of the Electricity Sub-Sector Coordinating Council.

Defined Contribution Plan

On the motion of Janice Case, the board adopted the following resolution:

RESOLVED, that on recommendation of the Corporate Governance and Human Resources Committee, the board authorizes the 2011 contribution equal to 10% of eligible compensation (salary and bonus) to the defined contribution plan for all eligible employees for the plan year ending December 31, 2011.

On motion of Chair Case, the board approved the following resolutions:

WHEREAS, the Corporate Governance and Human Resources Committee has recommended that the North American Electric Reliability Corporation (the "Company") establish a deferred compensation plan under section 457(b) of the Internal Revenue Code of 1986, as amended;

WHEREAS, NERC management, working with Employee Fiduciary Corporation, has developed a proposed North American Electric Reliability Corporation 457(b) Deferred Compensation Plan (the "Plan")(Attachment 1 to this resolution);

WHEREAS, the Board of Trustees finds that it is appropriate to establish the Plan;

THEREFORE, the Board of Trustees adopts the following resolutions:

RESOLVED, that the Plan be adopted in the form attached hereto, which Plan is hereby adopted and approved;

FURTHER RESOLVED, that the appropriate officers of the Company be, and they hereby are, authorized and directed to execute the Plan on behalf of the Company;

FURTHER RESOLVED, that the officers of the Company be, and they hereby are, authorized and directed to take any and all actions and execute and deliver such documents as they may deem necessary, appropriate or convenient to effect the foregoing resolutions including, without limitation, causing to be prepared and filed such reports, documents or other information as may be required under applicable law.

Compliance Committee

Chair Bruce Scherr provided a brief summary of the Compliance Open meeting from the previous day highlighting the committee reviewed its self-assessment results and have committed to review the mandate for changes with respect to those results; that NERC staff provided an update on the Compliance Enforcement Initiative, including Find, Fix, Track, and Report, and NERC staff provided an update on the filing of the six-month report. Mr. Scherr also noted that Mr. Stanley Kopman with NPCC provided an informative presentation on the Regional perspective on the FFT initiative.

Finance and Audit Committee

Chair Fred Gorbet reported that the committee met in closed session on January 30 with the external auditors to review the proposed audit plans for the audit of the financial statements, retirement savings plan, and the Form 990. The committee accepted the audit plans and approved the fees which remain the same as the previous year. The committee also met in open session on February 3 and completed review of the committee's self-assessment results and they audited year-end results. A couple highlights from the year-end results included NERC and the Regional Entities combined were under budget by a little less than four percent and that all Regional Entities individually were under budget. A key driver noted for the under budget result for the Regional Entities was their inability to acquire staff as quickly as budgeted. NERC was over budget by five percent but aligned with the Regions in that NERC was under budget on the personnel side. Additionally, during the February 3 session the committee discussed the upcoming budget process and implementing a working capital policy.

Following discussion, Chair Gorbet moved that the board accept the Unaudited Year-End 2011 Financial Statements of NERC and the eight Regional Entities; the board agreed to accept those statements. **(Exhibit W)**

Standards Oversight and Technology Committee

Chair Peterson provided a brief review of the actions of the committee the day prior.

Closing

Chair Anderson thanked the industry for their attendance and their continued support. He reconfirmed that the policy input is beneficial to the board and requests that the industry members continue to submit their comments.

Adjournment

There being no further business, Chair Anderson terminated the meeting at 11:55 a.m.

Submitted by,



David N. Cook
Corporate Secretary

Personnel Certification Governance Committee Nominations

Action

Appoint Mr. Don Oatman of the Electric Reliability Council of Texas (ERCOT) as a committee member to the Personnel Certification Governance Committee (PCGC). Mr. Oatman will be replacing Kelly Blackmer, the ERCOT representative on the PCGC.

Compliance and Certification Committee Nominations

Action

Approve the NERC Compliance and Certification Committee (CCC) Nominating Subcommittee request to the NERC Board of Trustees of the following Committee Officer appointments, membership appointments and re-appointments:

- CCC Officers for a two-year term starting July 1, 2012
 - **For the position of CCC Chair:** Mr. Terry Bilke of Midwest ISO, Inc.
 - **For the position of CCC Vice-Chair:** Ms. Patricia Metro of National Rural Electric Cooperative Association
- New membership appointments for three-year terms effective on the date of NERC Board of Trustees approval:
 - Mr. David Roth of Vandolah Power Company representing the Merchant Electricity Generator Sector
 - Mr. Darrell Piatt of FERC representing US Federal Government (non-voting)
- Membership re-appointments for three-year terms effective on the date of NERC Board of Trustees approval:
 - Mr. Clay Smith of Georgia Systems Operations Corporation representing the Cooperative Sector
 - Mr. Terry Bilke of Midwest ISO, Inc. representing RE-MRO
 - Mr. Chuck Manning of Electric Reliability Council of Texas, Inc. representing RE-TRE
 - Mr. Gregory Pierce of Entergy Corporation representing RE-SERC
 - Mr. Howard Rulf of WE Energies representing the Investor Owned Utility Sector

Agenda Item 6a – FAC-003-3 – Transmission Vegetation Management Program

Action

Adopt the following standards documents and direct staff to file with applicable regulatory authorities:

- **Reliability Standard FAC-003-3 – Transmission Vegetation Management** effective consistent with the Implementation Plan for FAC-003-3
[\[FAC-003-3–clean\]](#) [\[FAC-003-3 redline to last approval\]](#)
- **Implementation Plan for FAC-003-3 – Transmission Vegetation Management:**
[\[Implementation Plan\]](#)

There are two effective dates associated with FAC-003-3. The first gives Generator Owners (GOs) one year, as detailed in the implementation plan, to develop documented vegetation maintenance strategies, procedures, processes, or specifications as outlined in Requirement R3. The second effective date allows GOs two years, as detailed in the implementation plan, to comply with Requirements R1, R2, R4, R5, R6, and R7. This second effective date gives GOs sufficient time to begin executing the maintenance strategies, procedures, processes, or specifications documented in the first year.

These effective dates take into consideration that GOs were not previously required to comply with the vegetation management standard, and should be afforded adequate time, up to two years, to do so.

There are three scenarios that could occur regarding the approval of FAC-003-2 (approved by the NERC Board of Trustees on November 3, 2011) that would affect the implementation of FAC-003-3. These are addressed in the FAC-003-3 implementation plan.

Retirements

Retire the following standard midnight of the day immediately prior to the effective date of FAC-003-3.

- FAC-003-2 – Transmission Vegetation Management

Background

Building on the work of the Ad Hoc Group for Generator Requirements at the Transmission Interface (“Ad Hoc Group”), FAC-003-3 includes modifications that help ensure that responsibility for generator interconnection Facilities is appropriately assigned in NERC’s Reliability Standards. The changes proposed by the drafting team for Project 2010-07 offer a focused approach whereby sole-use interconnection Facilities (at or above 100 kV) that are owned and operated by generating entities will be included in a small set of standards and requirements previously only applicable to Transmission Owners (TOs). These generating entities, GOs and Generator Operators (GOPs), do not own or operate Facilities that are part of

the interconnected system; rather, they own and operate sole-use Facilities that are connected to the boundary of the interconnected system and, as such, may have a limited role in providing reliability compared to those entities that operate in a networked fashion beyond the point of interconnection.

In the past, certain GOs and GOPs with generator interconnection Facilities have been registered as TOs and Transmission Operators (TOPs). However, such action may not be necessary to provide an appropriate level of reliability for the Bulk Electric System. GOs and GOPs do not need, and in some cases may be prohibited from having, a wide-area view and responsibility for the integrated transmission system. Requiring GOs and GOPs to have such responsibilities would require significant training, require substantially more data, and increase modeling responsibilities. These responsibilities would also detract from the entities' primary functions: to operate their generation equipment—including interconnection Facilities—in a reliable manner.

The drafting team for Project 2010-07 proposed making FAC-003 applicable to certain qualifying GOs. FAC-003-3 requires a GO with qualifying interconnection Facilities to perform vegetation management. Previously, GOs with overhead lines were not required to perform vegetation management on those lines, thereby posing a reliability risk. For longer lines, the risk of outages from vegetation located on a right-of-way is similar to the risk for TOs.

FAC-003-3 includes exception language that excludes Facilities shorter than one mile with clear line of sight from the fenced area of the generating station switchyard to the point of interconnection. In many cases, generation Facilities are staffed and the overhead portion is within line of sight or over a paved surface.

Related changes to FAC-001-1—Facility Connection Requirements and PRC-004-2.1a—Analysis and Mitigation of Transmission and Generation Protection System Misoperations were adopted by NERC's Board of Trustees at its February 9, 2012 meeting, and PRC-005-1.1b—Transmission and Generation Protection System Maintenance and Testing is being presented this month alongside FAC-003-3.

Standard Development Process

FAC-003-3 progressed through four postings for stakeholder comment (one informal and three formal) over a 14-month period, an initial ballot in November 2011, a successive ballot in March 2012, and a recirculation ballot beginning in April 2012. The changes made between comment periods improved the clarity of the applicability changes.

A now voided recirculation ballot for FAC-003-X and FAC-003-3 took place in December 2011.

On January 20, 2012, an entity submitted an appeal that contended that the Standard Processes Manual was violated in that the transition from initial ballot to recirculation ballot incorporated changes made by the Standards Drafting Team (SDT) that were substantive.

NERC's Vice President and Director of Standards and Training determined the Standard Processes Manual was not adhered to, and referred the issue to the Standards Committee for handling. The Standards Committee Executive Committee directed NERC staff to void the FAC-003-X and FAC-003-3 recirculation ballot results of December 2011 and "remand the work to the drafting team with direction to take into account the issues raised in the Exelon appeal submitted in response to the recirculation ballot previously conducted and either: modify the language added following the initial ballot and then re-post the standard for a successive ballot, or remove the language added following the initial ballot and go directly to recirculation ballot."

The Project 2010-07 Standard Drafting Team (SDT) considered Exelon's appeal in the context of other stakeholder comments and continues to believe that a reference to line of sight is clarifying and makes explicit the SDT's implicit intent.

The ballots have not been completed at the time of submittal of this background material. The outcome will be reported at the BOT meeting

Unresolved Minority Issues

In comment periods, some entities maintained that FAC-003-3 should not include an exception for generator interconnection facilities of a certain length, because there are no exceptions made for TO facilities of different lengths.

The SDT still contends, as did the original Ad Hoc Report, that there is a very low risk from vegetation within the line of sight on a generator interconnection Facility, and thus the formal steps in FAC-003-3 are not necessary to ensure reliability of these lines. In many cases, generation Facilities are staffed and the overhead portion is within a line of sight or over a paved surface. Requiring GOs with Facilities like these to perform vegetation management would impose a burden with no reliability benefit.

Summary

The proposed changes to FAC-003-3 ensure that GOs that own generator interconnection Facilities with a reasonable risk of vegetation-related outages – those Facilities longer than one mile or without clear line of sight from the fenced area of the generating switchyard – are required to perform vegetation management, closing an identified reliability gap.

The Violation Risk Factors (VRFs), Time Horizons, and Violation Severity Levels (VSLs) for the standard were not modified to change all references from "Transmission Owner" to "responsible entity." Other administrative modifications were made to the compliance elements of the standard to conform to current guidelines.

A link to the project history and files is included here for reference:

http://www.nerc.com/filez/standards/Project2010-07_GOTO_Project.html

If trustees have questions or need additional information, they may contact Herb Schrayshuen, vice president and director of standards and training, at herb.schrayshuen@nerc.net.

Agenda Item 6b –PRC-005-1.1b – Transmission and Generation Protection System Maintenance and Testing

Action

Adopt the following standards documents and direct staff to file with applicable regulatory authorities:

- **Reliability Standard PRC-005-1.1b – Transmission and Generation Protection System Maintenance and Testing** effective consistent with the Implementation Plan for PRC-005-1.1a:
[\[PRC-005-1.1b–clean\]](#) [\[PRC-005-1.1b redline to last approval\]](#)
- **Implementation Plan for PRC-005-1.1b – Transmission and Generation Protection System Maintenance and Testing:**
[\[Implementation Plan\]](#)

The proposed changes to Requirements R1 and R2 are minor clarifying changes that make clear that generator interconnection Facilities are also part of GOs’ responsibility in the context of this standard. Because the changes are merely clarifying, no additional time for compliance is needed and all requirements become effective upon approval. In those jurisdictions where no regulatory approval is required, all requirements become effective upon Board of Trustees’ adoption.

Retirements

Retire the following standard midnight of the day immediately prior to the effective date of PRC-005-1.1b.

- PRC-005-1b – Transmission and Generation Protection System Maintenance and Testing

Background

Building on the work of the Ad Hoc Group for Generator Requirements at the Transmission Interface (“Ad Hoc Group”), PRC-005-1.1b includes modifications that help ensure that responsibility for generator interconnection Facilities is appropriately assigned in NERC’s Reliability Standards. The changes proposed by the drafting team for Project 2010-07 offer a focused approach whereby sole-use interconnection Facilities (at or above 100 kV) that are owned and operated by generating entities will be included in a small set of standards and requirements previously only applicable to TOs. These generating entities, GOs and GOPs, do not own or operate Facilities that are part of the interconnected system; rather, they own and operate sole-use Facilities that are connected to the boundary of the interconnected system, and as such, may have a limited role in providing reliability compared to those entities that operate in a networked fashion beyond the point of interconnection.

In the past, certain GOs and GOPs with generator interconnection Facilities have been registered as TOPs. However, such action may not be necessary to provide an appropriate level of reliability for the Bulk Electric System. GOs and GOPs do not need and, in some cases, may be prohibited from having, a wide-area view and responsibility for the integrated transmission system. Requiring GOs and GOPs to have such responsibilities would require significant training, require substantially more data, and increase modeling responsibilities. These responsibilities would also detract from the entities' primary functions: to operate their generation equipment—including interconnection Facilities—in a reliable manner.

In PRC-005-1.1b, certain language in Requirements R1 and R2 (“...that owns a generation Protection System...”) could lead to some confusion about whether an interconnection Facility is included. The phrase “and generator interconnection Facility” was added in these requirements as shown in the redlined version of the standard. Because there is no change in applicability, this change is considered a minor change employed only to add clarity.

Related changes to FAC-001-1 – Facility Connection Requirements and PRC-004-2.1a – Analysis and Mitigation of Transmission and Generation Protection System Misoperations were adopted by NERC’s Board of Trustees at its February 9, 2012 meeting, and FAC-003-3 – Transmission Vegetation Management is being presented this month alongside PRC-005-1.1b.

Standard Development Process

PRC-005-1.1b progressed through the normal standards development process, which included one formal comment period that began in March 2012, and will include an initial and recirculation ballot in April 2012. These ballots have not been completed at the time of submittal of this background material. The outcomes will be reported at the BOT meeting.

Summary

The proposed change to Requirement R1 and R2 of PRC-005-1.1b are clarifying (errata) changes that make clear that generator interconnection Facilities are also part of GOs’ responsibility in the context of this standard. Thus, no changes were proposed for the VRFs or VSLs for PRC-005-1.1b. Other administrative modifications were made to the compliance elements of the standard to bring it into conformance with current guidelines.

A link to the project history and files is included here for reference:

http://www.nerc.com/filez/standards/Project2010-07_GOTO_Project.html

If trustees have questions or need additional information, they may contact Herb Schrayshuen, vice president and director of standards and training, at herb.schrayshuen@nerc.net.

Agenda Item 6c — TOP-001-2-Transmission Operations; TOP-002-3-Operations Planning; and TOP-003-2-Operational Reliability Data—Real-Time Operations

Action

Adopt the following standards documents and direct staff to file with applicable regulatory authorities upon Board of Trustees approval of the remaining work products associated with this project:

- Reliability Standard TOP-001-2 Transmission Operations, effective consistent with the Implementation Plan for Project 2007-03
[\[TOP-001-2 -clean\]](#) [\[TOP-001-2 -redline to last approval\]](#)
- Reliability Standard TOP-002-3 Operations Planning, effective consistent with the Implementation Plan for Project 2007-03
[\[TOP-002-3 -clean\]](#) [\[TOP-002-3 -redline to last approval\]](#)
- Reliability Standard TOP-003-2 Operational Reliability Data, effective consistent with the Implementation Plan for Project 2007-03
[\[TOP-003-2 -clean\]](#) [\[TOP-003-2 -redline to last approval\]](#)
- Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for TOP-001-2, TOP-002-3, and TOP-003-2
[\[VRFs and VSLs\]](#)
- Implementation Plan for Project 2007-03
[\[Implementation Plan\]](#)

Background

On March 15, 2007, NERC received, and the Standards Committee accepted, a Standards Authorization Request (SAR) for Project 2007-03: Real-time Operations. The SAR was approved by the Standards Committee for standard development on November 1, 2007 with the following scope:

- Clarify requirements for Real-time operations of the Bulk Electric System (BES)
- Consider stakeholder comments received during the initial development of the Version 0 standards
- Respond to directives in FERC Order 693:
 - Add measures and levels of non-compliance
 - Clarify emergency conditions
 - Establish communication protocols for removing equipment from service
 - Address confidentiality of data issues
 - Require next-day analysis of IROLs and voltages
 - Require analysis to match actual field conditions
 - Clarify deliverability of power to load
 - Determine an appropriate lead time for outage notification

- Restore the system to proven limits in a defined timeframe
- Respect multiple contingencies in defined situations
- Assure that all needed data is provided in a timely fashion

During the course of the project, the SDT had to contend with several issues. Two key issues were as follows:

- The proper handling of Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs)

In the course of their deliberations, the SDT began to look closely at the requirements revolving around SOLs and IROLs to make certain that they accurately reflected what was needed for the reliability of the bulk power system.

SOLs are defined in the NERC Glossary as the value (such as MW, MVar, Amperes, Frequency, or Volts) that satisfies the most limiting of the prescribed operating criteria for a specified System configuration to ensure operation within acceptable reliability criteria. SOLs are based upon certain operating criteria. These include, but are not limited to:

- Facility Ratings (Applicable pre- and post-Contingency equipment or Facility Ratings)
- Transient Stability Ratings (Applicable pre- and post-Contingency Stability Limits)
- Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability Limits)
- System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits)

IROLs are defined as a SOL that, if violated, could lead to instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the BES. An IROL violation occurs when the IROL limit is exceeded continuously for greater than T_v . An IROL is exceeded, but not violated, if the IROL limit is exceeded for less than T_v . This is an important concept to understand as the terms “exceedance” and “violation” are often used interchangeably even though they have two distinctly separate meanings where an IROL violation has compliance violation implications and an IROL exceedance does not.

The problem confronting the SDT was to determine if the current standards adequately addressed the handling of these limits. In particular, the SDT was concerned that the transition from Operating Policies and Guidelines to the Version 0 standards had resulted in an incorrect emphasis on non-IROL SOLs versus IROLs. The pertinent existing standards where these limits were addressed are:

- TOP-002-2a, R10: Each Balancing Authority (BA) and Transmission Operator (TOP) shall plan to meet all System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs)
- TOP-004-2, R1: Each TOP shall operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs)

- TOP-007-0, R2: Following a Contingency or other event that results in an IROL violation, the TOP shall return its transmission system to within IROL as soon as possible, but not longer than 30 minutes

The SDT became concerned due to the apparent discrepancy between the three requirements. In the first two requirements, the applicable entities were told to plan and operate to meet all SOLs and IROLs while in the third requirement, they were only instructed to take action for IROLs. In this particular case, why were there requirements to plan and operate for non-IROL SOLs while actions were only required to be taken for IROLs? This led the SDT to perform historical research into the transition from Operating Policies and Guidelines to the Version 0 standards.

Operating Policy 2 clearly stated that the dangers to the reliability of the bulk power system (BPS) resulted from violations of IROLs. This policy clearly laid out the requirements for operating within IROLs and their respective T_v . It does not mention operating within non-IROL SOLs. This led the SDT to believe that the translation to Version 0 standards did not accurately reflect what the operating policies stated. The SDT contained members from all of the major interconnections in North America—California ISO, Electric Reliability Council of Texas, PJM Interconnection, Midwest ISO, and Northeast Power Coordinating Council. All of the members unanimously supported the position espoused in the revised standards.

With all of this in mind, non-IROL SOLs are important. Applicable entities must be aware of non-IROL SOLs and must consider whether exceeding an individual non-IROL SOL or multiple non-IROL SOLs would or could become a BPS reliability issue. However, the true risk to the System exists when the System is operating in conditions such that an IROL limit is exceeded for a time exceeding T_v . T_v represents the maximum time allowable to operate at the level of risk represented by exceeding an IROL.

As a result, the SDT revised the requirements on operating within limits. The SDT believes that this stance moves the standards to where the Operating Policies intended them to be and that the reliability of the Interconnected System will be maintained by this position and even enhanced because System Operators will not become distracted from true reliability problems by local system issues. Indeed, the revised standards actually further enhance the reliability of the BPS by tying actions to T_v . This mandates a tighter time standard for action and will improve the reliability of the BPS beyond an Adequate Level of Reliability.

The SDT further notes that, while non-IROL SOLs are similar to IROLs in that non-IROL SOLs must respect the ratings of equipment associated with the facilities to which the non-IROL SOL applies, there is no specific requirement established for a time of exceedance similar to the T_v of an IROL. The SDT recognizes that ratings have a wide range of acceptable operating practices and may have differing associated timeframes.

For example, large power transformers may have a significant thermal inertia which will allow for them to operate in excess of their rating for a number of hours. Transmission lines may have many different ratings relevant to them, including continuous ratings (may operate at the level continuously), emergency ratings (may operate at an increased level for a shorter duration of time, usually in terms of a few (2 to 4) hours), or even short-term ratings expressed in terms of a magnitude and a duration of a few (typically 5 to 30) minutes.

The notable difference between non-IROL SOLs and IROLs is expressed in the difference between the consequences to the System (or impact to reliability) should unplanned perturbations of the System occur when the limit is being exceeded. For an IROL, the consequences are described as Cascading, uncontrolled separation, or instability. For a non-IROL SOL, the consequences are typically thought of in terms of equipment damage or loss of life and are restricted to a limited, or local, area. By definition, the impact of exceeding a non-IROL SOL will not result in an Adverse Reliability Impact as defined in the NERC Glossary of Terms. That definition is repeated here:

- Adverse Reliability Impact:

The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection.

The SDT received valuable feedback from the open comment periods. While the majority of commenters agreed with the SDT position, there were a few concerns regarding non-IROL SOLs becoming IROLs in Real-time operations due to changes in System conditions. In response to those comments, the SDT included a requirement for identifying a sub-set of non-IROL SOLs that were identified as important for local areas and to monitor and report exceeding those non-IROL SOLs to the Reliability Coordinators (RCs). This requirement will allow for any RC, TOP, or BA to ensure that any non-IROL SOLs about which it is concerned, to be established and monitored to ensure local consequences are managed. Those entities may also identify and communicate to the RC any of the non-IROL SOLs that are believed or anticipated to have potential to develop into IROLs and, thus, to ensure that they, too, are monitored and managed. While the SDT does not feel that all non-IROL SOLs are necessary to be monitored and managed in a manner equal to that of IROLs, this provision will enable such operating practices where they are considered to be necessary.

- Handling deliverability issues in operations planning:

Power must always be deliverable to Load. There was some confusion in the past on how this deliverability was being handled in operations planning. The SDT clarified this issue by tying the operations planning process to a defined activity, Operational Planning Analysis (OPA), which requires an entity to consider Contingencies and to observe all applicable limits. When all power inputs and Loads are represented in the OPA, with all applicable limits observed, deliverability of power to Load is guaranteed.

Standard Development Process

The standards were processed through the full standards development process, including postings for seven formal comment periods, an Initial Ballot, two Successive Ballots, and a Recirculation Ballot.

Recirculation Ballot

The standards were posted for comment in October of 2008, April of 2009, August of 2009, and August of 2010 before moving to Initial Ballot.

The proposed standards were posted for public comment from April 26, 2011, through June 9, 2011, with an Initial Ballot occurring from May 31, 2011 through June 9, 2011. The set of standards achieved a quorum of 88.47 percent and an approval of 48.64 percent.

Subsequently, the standards were subjected to individual Successive Ballots. This was done to put more focus on individual standards and determine where the energies of the drafting team would best be focused. A public comment period was held from December 14, 2011, through January 12, 2012, with a Successive Ballot held from January 3, 2012, through January 12, 2012. The Successive Ballot results were as follows:

- TOP-001-2 achieved a quorum of 82.04 percent and a weighted segment approval of 59.93 percent.
- TOP-002-3 achieved a quorum of 82.04 percent and a weighted segment approval of 77.08 percent.
- TOP-003-2 achieved a quorum of 82.04 percent and a weighted segment approval of 78.95 percent.

The standards were put through a public comment period from March 22, 2012 to April 20, 2012, with Successive Ballots held from April 11, 2012 through April 20, 2012. These ballots have not been completed at the time of submittal of this background material. The outcomes will be reported at the BOT meeting

VRFs and VSLs

Initially, the VRFs and VSLs were subject of a non-binding poll of all the VRFs and VSLs associated with the standards for this project. That poll occurred from May 31, 2011 through June 9, 2011, and achieved a quorum of 84.18 percent and an approval of 41 percent.

Subsequently, another non-binding poll was taken, this time focusing on each standard individually. The second set of polls occurred from January 9, 2012 through January 18/19, 2012 (TOP-002 completed on the 18th, while TOP-001 and -003 completed on the 19th), and achieved quorums, with the following results:

- For TOP-001-2, 81.5 percent of those who registered to participate provided an opinion, and 67.61 percent of those who provided an opinion indicated support for the VRFs and VSLs that were proposed.
- For TOP-002-3, 76.41 percent of those who registered to participate provided an opinion, and 71.42 percent of those who provided an opinion indicated support for the VRFs and VSLs that were proposed.
- For TOP-003-2, 81.5 percent of those who registered to participate provided an opinion, and 70.28 percent of those who provided an opinion indicated support for the VRFs and VSLs that were proposed.

NERC standards staff has reviewed the VRFs and VSLs and recommends them for adoption.

Minority Issues

- Some commenters objected to the use of an unapproved definition, “Reliability Directive,” in TOP-001-2, stating it presented coordination problems and could cause a change to the standard if the definition is changed during its balloting. The SDT explained that it was working closely with Project 2006-06 which is developing the definition, and that the need to coordinate filing of projects 2006-06 and 2007-03 has been forwarded to NERC management.
- There is still some debate as to what is meant by the term “internal area reliability.” Some commenters asked for a formal definition of this term. The SDT believes that TOPs should have some degree of freedom in this determination and that they are best suited to determine what affects its internal area. Therefore, the best approach is believed to be to leave the concept as is and not to constrain the TOP to a hard and fast definition. This way, each situation can be determined on its own merits and the responsibility rests solely with the individual TOP. However, to provide additional clarity to the concept and to better show the intent of the SDT, the term was changed to “reliability internal to its Transmission Operator Area.”
- There was concern about possible double jeopardy with TOP-003-2, Requirements R1/R3 and R2/R4. The SDT explained that double jeopardy should not be a concern, as the two requirements represent two different actions: one to create the specification and one to distribute it. The two separate and distinct actions mean that there are two distinct reliability outcomes and that two separate requirements are needed.

A link to the project history and files is included here for reference:

[http://www.nerc.com/filez/standards/Real-time Operations Project 2007-03.html](http://www.nerc.com/filez/standards/Real-time_Operations_Project_2007-03.html)

If trustees have questions or need additional information, they may contact Herb Schrayshuen, vice president and director of standards and training, at herb.schrayshuen@nerc.net.

Agenda Item 6d —Interpretation 2010-05 of CIP-002-1 for Duke Energy

Action

Adopt the interpretation of Requirement R3 of CIP-002-1 (Cyber Security – Critical Cyber Asset Identification) for Duke Energy and direct staff to file with applicable regulatory authorities.

- Interpretation of CIP-002-1 — The referenced clean standard below provides the interpretation being approved as an appendix.

[\[CIP-002-1a Clean\]](#)

Background

On January 31, 2010, Duke Energy requested a formal interpretation of CIP-002-1 Cyber Security – Critical Cyber Asset Identification, Requirement R3, asking the following questions:

- Is the phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be assessed for inclusion in the list of Critical Cyber Assets using an entity’s critical cyber asset methodology?
- What does the phrase "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"?

An interpretation was developed and posted for a 30-day public comment period from September 8, 2010 through October 8, 2010. There were 39 sets of comments, including comments from more than 85 different people from approximately 75 companies representing 9 of the 10 NERC Industry Segments. However, work on the interpretation was delayed based on reprioritization of the total standards workload and then further delayed until the Standards Committee developed more formal processes for addressing interpretations in support of the board’s November 2009 guidance.

In April 2011, the Standards Committee approved and issued the NERC Guidelines for Interpretation Drafting Teams and directed that work resume on the interpretation. Nominations were solicited for a dedicated Critical Infrastructure Protection (CIP) Interpretation Drafting Team. A CIP Interpretation Drafting Team was appointed, and members of the team reviewed the comments received from the 2010 comment period.

The interpretation was modified based on the feedback received, and posted for a 45-day public comment period from February 8, 2012, through March 23, 2012; with an Initial Ballot occurring on the last 10 days of the comment period. The ballot achieved a 94.71 percent approval, with a quorum of 89.63 percent. A Recirculation Ballot was conducted from April 20, 2012, through April 30, 2012, and was approved by stakeholders, achieving a 94.71 percent approval with a quorum of 89.63 percent.

Summary

The Interpretation provides the following answers to the requestor:

The phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” is illustrative, not prescriptive. It simply provides examples of the types of Cyber Assets that should be considered. It does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types.

The word “essential” is not defined in the Glossary of Terms used in NERC Reliability Standards, but the well-understood meaning and ordinary usage of the word “essential” implies “inherent to” or “necessary.” The phrase “essential to the operation of the Critical Asset” means inherent to or necessary for the operation of the Critical Asset. A Cyber Asset that “may” be used, but is not “required” (i.e., without which a Critical Asset cannot function as intended), for the operation of a Critical Asset is not “essential to the operation of the Critical Asset” for purposes of Requirement R3. Similarly, a Cyber Asset that is merely “valuable to” the operation of a Critical Asset, but is not necessary for or inherent to the operation of that Critical Asset, is not “essential to the operation” of the Critical Asset.

A link to the project history and files is included here for reference:

http://www.nerc.com/filez/standards/2010-INT-05_ Interpretation_CIP-002-1_Duke.html

If trustees have questions or need additional information, they may contact Herb Schrayshuen, vice president and director of standards and training, at herb.schrayshuen@nerc.net.

Agenda Item 6e — ReliabilityFirst Corporation Regional Standards Development Procedure

Action

Approve the following standards document and direct staff to file with applicable regulatory authorities:

- **Version 4 of ReliabilityFirst Corporation Regional Standards Development Procedure**

Background

At the May 10, 2011 NERC Board of Trustees meeting, Version 3 of ReliabilityFirst Corporation (RFC) Regional Standards Development Procedure was approved. For that version, NERC publicly noticed and requested comments on RFC's proposed changes for a 45-day comment period, from March 1, 2011 to April 15, 2011. NERC received nine sets of comments. The principal issue raised in the comments was the addition of the language with respect to the effective date of standards for Members of RFC. Commenters objected to inclusion of this additional language, stating that standards cannot be made mandatory and enforceable under section 215 until they have been approved by NERC and the FERC. The provision regarding the enforceability on RFC Members was not a new concept. The provision has been part of the Bylaws of RFC since its inception. The only thing that was new was the language in the standards procedure that clarified the issue. The NERC Board of Trustees action included an understanding that the RFC President would discuss possible changes to the RFC Bylaws to address industry concern regarding enforcement of non FERC-approved standards on Members.

Summary

Subsequent to the May 10, 2011 NERC Board of Trustees action, RFC's Membership approved an amended definition of "Regional Reliability Standard" contained within the amended Bylaws and Certificate of Incorporation. Based on this action, the RFC Standards Committee made a conforming minor change to Version 4 of the RFC Reliability Standards Development Procedure. This minor change was made to ensure that the RFC Reliability Standards Development Procedure defines and utilizes the term "Regional Reliability Standard" in a manner consistent with the Member-approved amended definition. During the December 1, 2011 RFC Board of Directors' meeting, the Board concurred with the minor change in Version 4 of the RFC Reliability Standards Development Procedure.

The proposed amended definition of "Regional Reliability Standard" specifically states that a Regional Reliability Standard is not binding upon any Member or Registered Entity, nor is it effective or enforceable, until the Regional Reliability Standard has been adopted by NERC and approved by the Commission.

A link to the project history and files is included here for reference:

<https://rsvp.rfirst.org/SDP501RFC03/default.aspx>

If trustees have questions or need additional information, they may contact Herb Schrayshuen, vice president and director of standards and training, at herb.schrayshuen@nerc.net.

Agenda Item 6f – Western Electricity Coordinating Council Regional Variance

Action

Adopt the following standards documents and direct staff to file with applicable regulatory authorities:

- WECC Variance to Reliability Standard VAR-001-3 – Voltage and Reactive Control
[\[VAR-001-3 – Clean\]](#) [\[VAR-001-3 – Redline to VAR-001-2\]](#)
- Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the WECC variance to VAR-001-3
[VRFs and VSLs are available in the Standard above]
- Implementation Plan for VAR-001-3

The effective date for WECC variance to VAR-001-3 is the first day of the first calendar quarter six months after applicable regulatory approval, or in those jurisdictions where no regulatory approval is required, the first day of the first calendar quarter six months after NERC Board of Trustees' approval.

Background

The purpose of this regional variance to the existing NERC Standard VAR-001-2 is to ensure that voltage levels are within limits in real time to protect equipment and the reliable operation of the Western Interconnection. Analysis of disturbances in the Western Interconnection have demonstrated that during and immediately following a disturbance, the generator's Automatic Voltage Regulator (AVR) – operating in automatic voltage control mode – is needed to stabilize the Bulk Electric System's (BES) voltage. TOPs are responsible for determining the voltage levels required to maintain reliable operation of the Interconnection and convey the required voltage level information to GOPs.

Summary

Existing VAR-001-2 Requirement R3 allows TOPs the option of specifying criteria that exempt generators from compliance with the requirements defined in NERC Standard VAR-001-2 Requirement 4 and Requirement 6.1. The WECC SDT and WECC stakeholders determined that permitting such exemptions in the Western Interconnection would reduce the amount of voltage support available when generation and transmission outages occur, adversely impacting the reliability of the Western Interconnection.

Existing VAR-001-2 Requirement R4 allows TOPs the option of providing reactive power schedules rather than voltage schedules; however, operating against a reactive power schedule in the Western Interconnection will not ensure that generators provide the proper voltage support when generation and transmission outages occur. This conclusion was based on the fact that generator operators that are provided reactive schedules under NERC VAR-001-2 are required to maintain the reactive output defined in the schedule at all times. This would require generator operators to modify the AVR set point as system conditions change to maintain the specified reactive output of the schedule.

This variance to the NERC Standard restricts the TOP to providing only a voltage schedule, but allows the schedule to be conveyed through a reactive power level, provided that the reactive power level is converted to a voltage level for the AVR's automatic voltage control mode setting.

In the Western Interconnection, SOLs for transmission paths in the BES assume that the AVRs are in service to control voltage to support the transfer capabilities. As noted below, previous approvals and rulings regarding VAR-002-WECC-1 have directed GOPs to operate AVRs in voltage control mode to support transfer capabilities in the Western Interconnection.

- April 16, 2008 – The WECC Board of Directors approved VAR-002-WECC-1 to ensure that the AVRs are in service and controlling voltage so that generators provide the proper voltage support when generation and transmission outages occur
- October 29, 2008 – The NERC Board of Trustees approved VAR-002-WECC-1
- April 21, 2011 – FERC issued an Order approving VAR-002-WECC-1

During the development of WECC Regional Standard VAR-002-WECC-1, industry comments noted that not all WECC TOPs provide voltage schedules to their GOPs. Providing reactive power schedules (instead of specific voltage levels) forces GOPs to manually adjust their AVR voltage setting to a setting that will provide the exact amount of reactive power in the schedule.

It is recognized that during the course of a day, system dynamics may result in changes in reactive output such that the generator will no longer produce the amount of reactive power specified by the TOP's reactive power schedule. If the GOP alters the amount of reactive power provided by the generator to return it to the schedule, there is higher risk that such action will result in the generator doing the exact opposite of what is needed to maintain system reliability: ensuring that generators provide the proper voltage support when generation and transmission outages occur.

The WECC Variance to VAR-001-2 is an alternative approach to meeting the same reliability objective as the NERC VAR-001-2 Reliability Standard. The proposed regional variance in Section E contains requirements that are more stringent than the continent-wide Requirements R3 and R4 of VAR-001-2 or provides a specific alternative approach to meeting the same reliability objective.

Standards Staff View of VRFs and VSLs

The non-binding poll of VRFs and VSLs was conducted during the regional ballot of the associated standard. NERC standards staff is not recommending any modifications be made to the VRFs and VSLs that were posted for the nonbinding poll.

Minority Issues

There were several minority issues raised during the development process:

- **Issue:** Why would the drafting team want to assume the GOP has the expertise to convert a Reactive Power schedule to a voltage set point-especially when the wrong steps could be taken by a GOP during an incident that would be perfectly correct under normal operating conditions?

Response: The drafting team believes that GOPs have a better understanding of the operation and control of a generator than the TOPs. The conversion process is developed in advance and used to translate the TOP's schedule to an AVR set point during normal operating conditions, and there is no specific action taken by the GOP at the time of a system event. The requirement to have the AVR in voltage control mode is so that the unit(s) will respond appropriately and automatically during a system event.

- **Issue:** The WECC Variance inappropriately mimics NERC VAR-002-1.1b for GOPs.

Response: In the WECC Variance, the GOP has an integral part in establishing the schedule at the generator terminal. If the requirements in the WECC Variance were split between VAR-001-2 and VAR-002-1.1b, there would more confusion than combining the requirements into a WECC Variance. The drafting team clarified the communication of schedules and the GOP's response to those schedules.

- **Issue:** There are no physical differences in the BES in WECC to justify the generator specific requirements in the WECC Variance.

Response: The requirements in the WECC Variance are designed to make the Interconnection more reliable because there are physical differences that require AVRs to control voltage. In the Western Interconnection this physical difference and need for keeping AVRs in service controlling voltage was recognized when one of the causes of the 1996 disturbances was identified as insufficient supply of reactive power from generators, including AVRs that were not operating in voltage control mode. As a result of this experience, WECC determined there should be only very limited circumstances where a GOP should remove its unit from AVR operation (see VAR-002-WECC-1).

Furthermore, the analyses of many disturbances in the Western Interconnection have demonstrated the need to stabilize system voltage by using AVR response. The development the WECC Variance further supports the need for voltage support during system disturbances by:

- Requiring that TOPs provide voltage rather than reactive schedules to GOPs
- Allowing TOPs to provide voltage schedules through reactive power terms
- Requiring the conversion of voltage schedules into voltage settings for the AVRs

A link to the project history and files is included here for reference:

<http://www.wecc.biz/Standards/Development/WECC0046/default.aspx>

If trustees have questions or need additional information, they may contact Herb Schrayshuen, vice president and director of standards and training, at herb.schrayshuen@nerc.net.

Agenda Item 6g — Update on Frequency Response (Project 2007-12)

Action

Discussion

Executive Summary

The Frequency Response Project will not be able to deliver a standard responsive to FERC's previous directives within the mandatory time frame established. NERC is continuing to work with the SDT to develop a quality standard that meets the directive and has requested FERC to grant relief from the filing deadline.

Background

Frequency Response is a measure of an Interconnection's ability to stabilize frequency immediately following the sudden loss of generation or load. It is a critical component to the reliable operation of the BPS, particularly during disturbances and restoration. There is evidence of continuing decline in Frequency Response over the past 10 years, but no confirmed reason for the apparent decline.

NERC began work on addressing ongoing concerns with Frequency Response as far back as 2005. Following various edits and modifications to a SAR, initial work on the standard began in 2007, with more extensive efforts commencing in 2008 focusing on a standard that would require mandatory data reporting for further analysis. In 2009, work was stopped, and then restarted in 2010 to be more focused on actual BA performance, rather than just data submittal. Due to the complexity of the subject matter, a first draft of the standard was not posted until February 4, 2011; a second draft was posted for comment and Initial Ballot on October 23, 2011. At that time, the standard achieved only a limited amount of success, with a weighted segment vote of 30.82 percent.

Discussion

Stakeholders have identified a number of concerns regarding this standard, which are leading to a reduced amount of ballot support.

- Assignment of responsibility to the BA, without assigning responsibility to the GO. Several entities have indicated that a BA cannot currently compel a generator to deliver frequency response. As such, holding the BA accountable for delivery of Frequency Response absent a generator performance standard of some kind is unacceptable to them.
- Some stakeholders have identified concerns that the Frequency Response Obligation being established by the standard is too low, and will not adequately protect reliability.
- Need for a market-based solution because frequency response is a resource "requiring activity".

FERC staff has identified what they perceive to be several shortcomings in the standards. Specifically:

- The use of an annual measure of central tendency to determine a BA's performance (based on a representative sample of events), rather than a discrete per-event determination. The SDT believes that due to the significant number of variables involved in determining performance, it is difficult or impossible to accurately measure performance during individual events. FERC staff believes we have not exhausted all options here, nor provided sufficient support of our claim.
- The use of a sample set of events, as selected by the ERO, based on specific exclusion criteria rather than using all events that meet certain criteria. The SDT feels that given the variables involved in determining performance, they must exclude certain kinds of events. However, FERC staff is concerned that excluding these events may result in excluding events where Frequency Response is of particular importance.
- The use of the mathematical "median" to measure central tendency. The SDT believes this will eliminate outliers in the sample set. While this is true, FERC staff has expressed concerns that it will simply eliminate all values being considered from the sample except the median value, and there is no analysis of the other samples or the magnitude of their deviation from the median.
- The use of a 25 percent reliability margin, of which FERC staff has questioned the technical merit. NERC staff has also identified potential concerns with this value.
- The lack of a requirement to sustain frequency response until a secondary response replaces it. The SDT feels that there is no way to accurately measure performance during the extended time between when an event starts and when secondary response takes over; however FERC staff believes that technology upgrades might support such analysis. The SDT agrees that technology upgrades could support such analysis but feels that these upgrades would be extremely costly and would not receive the support of the industry.

At this time, NERC believes the best course of action is to continue working, perform any needed research to validate or disprove hypotheses regarding how to measure Frequency Responsive Reserve performance, and develop a technically accurate and defensible standard. Accordingly, NERC has requested that FERC grant additional time to continue its work. Although the decline of Frequency Response is of concern, the decline is not at this point acute to where reliability is under threat, and it is believed that such a threshold point will not be crossed for some years.

A link to the project history and files is included here for reference:

http://www.nerc.com/filez/standards/Frequency_Response.html

If trustees have questions or need additional information, they may contact Herb Schrayshuen, vice president and director of standards and training, at herb.schrayshuen@nerc.net, or Mark Lauby, vice president and director reliability assessment and performance analysis at mark.lauby@nerc.net.

Request to Shorten Comment Period for Proposed Data Request Under Section 1606 of the NERC Rules of Procedure

Action

Approve shortening the time period normally required to issue a request for data or information in accordance with Section 1600 of the NERC Rules of Procedure. Section 1606 of the Rules allows for a shortened time period to issue a request for data or information if the data or information must be obtained in order to evaluate a threat to the reliability or security of the bulk power system or to comply with a directive in an order issued by the Commission or by another governmental authority.

Background

On April 19, 2012, the Federal Energy Regulatory Commission (“FERC” or the “Commission”) issued Order No. 762 remanding NERC’s proposed Transmission Planning (TPL) Reliability Standard TPL-002-2b (“Remand Order”).

The TPL-002-2b standard includes a provision that allows for planned load shed in a single contingency provided that the plan is documented and alternatives are considered and vetted in an open and transparent stakeholder process. The Commission determined that the proposed footnote is vague, unenforceable, and not responsive to the Commission directives. The Commission therefore remanded the proposed TPL-002-2b standard as unjust, unreasonable, unduly discriminatory or preferential, and not in the public interest.

In the Remand Order, the Commission noted that several entities stated that the interruption of Firm Demand is rarely needed, but no support was provided for this conclusion. Accordingly, FERC directed NERC to identify the specific instances of any planned interruptions of Firm Demand under footnote b and determine how frequently the provision has been used. FERC directed NERC to gather this data using Section 1600 of its Rules of Procedure. FERC also directed NERC to deploy its Expedited Reliability Standards Development Process to quickly respond to the remand.

Given FERC’s directive to respond to the Remand Order quickly, which must also include a discussion on how frequently the footnote b provision has been used, NERC needs to send a Section 1600 data request to registered entities to collect information requested by the Commission. The results of this data request will be analyzed by the standard drafting team to help respond to the FERC directives in the Remand Order.

NERC is working to respond to the Remand Order and present a revised footnote b by the November 2012 Board of Trustees meeting. However, in order to meet this aggressive schedule, NERC must proceed on an expedited schedule for issuing the proposed data request in order to obtain results quickly so they can be used in the development of a revised footnote.

Section 1600 of NERC's Rules of Procedure normally require a twenty-one (21) day review period by FERC's Office of Electric Reliability and a subsequent forty-five (45) day industry comment period before a request for data or information can be sent to the industry. With NERC Board of Trustees approval, these procedures can be shortened. NERC management recommends shortening the time for public comment to twenty-one (21) days. NERC has discussed an expedited review with FERC staff as well. This schedule will enable NERC to present the proposed data request to the Board of Trustees for approval in June and allow us to collect data for use by the standards drafting team in its development of a revised footnote b.

If trustees have questions or need additional information, they may contact Herb Schrayshuen, Vice President of Standards and Training, at herb.schrayshuen@nerc.net.

Proposed Amendments to Delegation Agreement with Midwest Reliability Organization (MRO) – Amended Exhibit B (MRO Bylaws)

Action

Approve proposed amendments to NERC's Delegation Agreement with MRO, consisting of amended MRO Bylaws (Exhibit B to Delegation Agreement).

Background

MRO has requested that the Board approve, and direct NERC staff to file with FERC for approval, amendments to the Delegation Agreement between NERC and MRO, consisting of amendments to Exhibit B – the MRO Bylaws. **Attachment 1** is a letter from MRO requesting Board of Trustees (Board) approval of the amendments to the FRCC Bylaws and explaining the purposes of the proposed amendments. **Attachment 2** is a redlined version of Exhibit B to the MRO Delegation Agreement (MRO Bylaws), marked to show the proposed amendments. The Board is requested to approve the proposed amendments in substantially the form shown on **Attachment 2**.

There are no proposed revisions to any other portions of the MRO Delegation Agreement, and therefore only the redlined version of Exhibit B is being provided with this agenda item.

Board approval of the amendments to Exhibit B of the MRO Delegation Agreement will also constitute approval of the amendments to the MRO Bylaws as a "Regional Entity rule." The proposed amendments to Exhibit B have received the necessary approvals from the MRO Board of Directors and membership. NERC staff worked with MRO during this process to ensure that the amended MRO Bylaws continue to meet the governance criteria stated in Exhibit B to the Delegation Agreement.

The following discussion summarizes the principal components of the amendments.

Discussion of Amendments to Delegation Agreement Exhibit B (MRO Bylaws)

There are three significant areas of amendment to the MRO Bylaws. First, the "Large End Use Electricity Sector" and the "Small End Use Electricity Sector" are eliminated from the Industry Sectors of MRO Membership (§1.14 and deleted §§1.13 and 1.22). Correspondingly, the two director positions on the MRO board representing these Sectors are eliminated (§7.3). MRO states that the eliminated Sectors have historically had very low, or no, membership, and a lack of participation.

Second, two Independent Directors are added to the MRO board, thereby making the board a hybrid board rather than solely a stakeholder board. Addition of the two Independent Directors coupled with elimination of the director positions for the two eliminated Sectors results in the overall MRO board membership continuing to be 19 directors (§7.3). The Independent Directors will be nominated by the board and elected by the members (§7.3). "Independent Director" is defined in new §1.13 as follows:

"Independent Director" means an individual who is not (1) an officer or employee of the Corporation; (2) a member, director, officer or employee of a Member or Adjunct Member of the Corporation; (3) a director, officer or employee of any Registered Entity on the NERC registry; or (4) reasonably

perceived as having a direct financial interest in the outcome of a decision by the board of directors and who (a) does not have any other relationship that would interfere with the exercise of independent judgment in carrying out the responsibilities of a director and (b) meets any additional requirements of independence established by the board of directors.

This definition is comparable to the definition of “independent trustee” in Article III, section 3 of the NERC Bylaws. Additionally, amended §7.3 states that “Independent Directors shall have relevant senior management expertise and experience to the reliable operation of the bulk power system in North America.” Section 7.4 is amended to provide that while all directors shall generally serve three-year, staggered terms, the initial term for one of the Independent Directors shall be two years. Section 7.4 is also amended to provide that a director elected by an Industry Sector may be removed by affirmative vote of two-thirds of the Members of that Industry Sector, and an Independent Director may be removed by affirmative vote of two-thirds of the remaining directors. Further, §7.5 is amended to provide that the board may set reasonable compensation for the service provided by Independent Directors, but that directors elected by an Industry Sector shall not receive compensation.

Third, a new, non-voting class of members, referred to as Adjunct Members, is added to the Membership of MRO (§5.1). “Adjunct Member” is defined as:

an entity that: (1) is not eligible to belong to an Industry Sector; (2) has a material interest in reliability issues in the Corporation’s Region and (3) becomes an Adjunct Member of the Corporation. (§1.1)

Additionally, §16.1, Regulatory Participants, is amended to state that “All Regulatory Participants shall be entitled to be Adjunct Members.” (“Regulatory Participant” is defined in §1.23 to include state and provincial regulatory agencies in the MRO Region, representatives of FERC, regional advisory bodies established by FERC, and representatives of any federal regulator or agency.) MRO states that adding the Adjunct Members class will provide an opportunity to participate for people and entities that are not part of an Industry Sector but nevertheless have a material interest in reliability issues in the MRO Region, including any entities that would have been members in the Large-End Use Electricity Customer Sector or Small End-Use Electricity Customer Sector. For example, Adjunct Members can attend the Annual Meeting and Special Meetings of Members (§6.1 and §6.2.1); and may inspect the books and records of the Corporation (§11.1).

Because the Membership of MRO will now consist of the two classes, [Industry Sector] Members and Adjunct Members, there are numerous amendments to the Bylaws to identify the rights of Adjunct Members, to distinguish between the rights of [Industry Sector] Members and Adjunct Members, and to identify the actions in which only [Industry Sector] Members can participate. See, e.g., §5.3 (Admission of Members and Adjunct Members); §5.4 (Voting Rights); §5.5 (Transfer of Membership); §6.1 (Annual Meeting of Members); §6.2.1 (Special Meetings of Members – Who May Call); §6.5 (Right to Vote; Act of Members (providing that only Industry Sector Members may vote)); §6.6 (Quorum (basing the quorum requirement solely on attendance by Industry Sector Members)); §6.7 (Action by Written Ballot); §6.8 (Action by

Electronic Communication); §11.1 (Books and Records; Financial Statements); and §15.2 (Limitations on Liability).

Due to the revised compositions of the MRO Membership, Industry Sectors and board, it was necessary to ensure that the MRO governance under its Bylaws continues to satisfy the Exhibit B governance criteria that no two Industry Sectors can control any action and no one Industry Sector can veto any action. This was accomplished by adding the following text in §6.5, Right to Vote; Act of Members, and §7.9, Board Action:

§6.5: “. . . in no event will an action of the Members be valid where the action was passed solely by the vote of Members from two Industry Sectors or defeated solely by the vote of Members in a single Industry Sector.”

§7.9: “. . . in no event will an action of the Directors be valid where the action was passed solely by the vote of Directors from two Industry Sectors or defeated solely by the vote of Directors in a single Industry Sector.”

Finally, a number of sections of the Bylaws have been amended to add section titles, as in the current Bylaws some sections have titles and other sections do not. See, e.g., the sections in Articles 16, 17 and 19.

ATTACHMENT 1

**MIDWEST RELIABILITY ORGANIZATION LETTER
REQUESTING APPROVAL OF AMENDMENTS
TO MRO BYLAWS**



April 3, 2012

Mr. David N. Cook, Vice President and General Counsel
Ms. Rebecca J. Michael, Assistant General Counsel
North American Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005

Re: Midwest Reliability Organization's Bylaw Changes

Dear Mr. Cook and Ms. Michael:

Midwest Reliability Organization (MRO) is submitting proposed changes to its bylaws for consideration by the North American Reliability Corporation Board of Trustees (NERC BOT).

The MRO board of directors began considering a change from a stakeholder board to a hybrid board in 2010. This change, as well as others, was discussed at the MRO Governance and Personnel Committee and board meetings throughout 2011. At its annual strategy session in October, the board decided to move forward with changes to the bylaws.

On December 15, 2011, the board of directors unanimously approved the proposed changes which were submitted to the membership for approval during February and March 2012. On March 14, 2012, the members of MRO approved the changes.¹ Attached are redlined and clean copies of the proposed changes to the MRO Bylaws which have been approved.

There are three significant changes to the bylaws. First, two independent directors are added. Second, the Large End-Use Electricity Customers Sector and the Small End-Use Electricity Customer's Sector are eliminated. Finally, a non-voting Adjunct Member class is added. Additional changes to the bylaws were made to simplify language or correct errors.

The board believes that the addition of two independent directors is consistent with good governance corporate practices and trends. Additionally, several Regional Entity boards have added independent directors recently. Independent directors will bring additional and different perspectives, providing a dimension of independence not provided in a balanced stakeholder

¹ Following the membership approval and pursuant to the board's authority in Article 19, the board unanimously approved additions to the bylaws to make explicit MRO's obligations under law and the delegation agreement, namely, that no action by the members or the board was valid if the action was passed solely by the vote from two sectors or was defeated solely by the vote of a single sector.





MRO Bylaw Changes

April 3, 2012

Page 2 of 3

board. Independent directors were defined in Section 1.13 of the proposed MRO Bylaws as:

Independent Director. “Independent Director” means an individual who is not (1) an officer or employee of the Corporation; (2) a member, director, officer or employee of a Member or Adjunct Member of the Corporation; (3) a director, officer or employee of any Registered Entity on the NERC registry; or (4) reasonably perceived as having a direct financial interest in the outcome of a decision by the board of directors and who (a) does not have any other relationship that would interfere with the exercise of independent judgment in carrying out the responsibilities of a director and (b) meets any additional the requirements of independence established by the board of directors.

Changes were made to the bylaws to allow, but not require, the board to compensate the independent directors for their time.

The Large End-Use Electricity Customers Sector and the Small End-Use Electricity Customers Sector were eliminated due to the historic lack of participation by these sectors. The Large End-Use Electricity Customers Sector consists of three members. It has never elected a member to the board of directors. The Small End-Use Electricity Customers Sector did not have any members until 2011 and to date has not elected a member to the board of directors.

Of interest are the votes of these two sectors on the proposed bylaw changes. None of the three members in the Large End-Use Electricity Customers Sector voted, which is consistent with past practice of the members of this sector; the Small End-Use Electricity Customers Sector voted unanimously for the proposal.

The third change was to add a non-voting adjunct class of members to provide an opportunity to participate for people and entities that are not part of an industry sector but nevertheless have a material interest in reliability issues in the MRO Region. MRO believes this will allow those formerly in the Large End-Use Electricity Customers Sector and the Small End-Use Electricity Customers Sector to participate as well as entities such as Planning Authorities and state regulators.

Midwest Reliability Organization respectfully requests that the North American Reliability Corporation (NERC) Board of Trustees approve these changes to its bylaws, amend the delegation agreement between MRO and NERC accordingly, and direct NERC staff to seek approval of these changes from the Federal Energy Regulatory Commission.





MRO Bylaw Changes

April 3, 2012

Page 3 of 3

We appreciate your consideration and assistance with these important changes.

Very truly yours,

Miggie E. Cramblit
General Counsel and Director of External Affairs

cc: Mr. Dan Skaar, President
Mr. Jeffrey J. Gust, Chairman of the Board
Mr. Ed Tymofichuk, former Chairman of the Board

Note: Effective April 30th, 2012, our mailing address will be
380 St. Peter Street, Suite 800, St. Paul, MN 55102



ATTACHMENT 2

**REDLINED VERSION OF
MIDWEST RELIABILITY ORGANIZATION BYLAWS,
SHOWING AMENDMENTS**

**BYLAWS OF THE
MIDWEST RELIABILITY ORGANIZATION, INC.**

As amended through ~~December~~ March 29~~21~~5xx, 201-210

TABLE OF CONTENTS

ARTICLE 1	DEFINITIONS	1
	<u>Section 1.1</u> <u>Adjunct Member.....</u>	<u>1</u>
	Section 1.2 Affiliate.....	1
	Section 1.3 Bulk-Power System.....	1
	Section 1.4 Bulk-Power System Users	1
	Section 1.5 Canadian Utilities.....	1
	<u>Section 1.6</u> <u>Corporation.....</u>	<u>1</u>
	Section 1.67 Cooperative.....	1
	Section 1.78 Corporate Region.....	21
	Section 1.82 FERC.....	21
	Section 1.910 Federal Power Marketing Agencies	2
	Section 1.110 Generators and Power Marketers.....	2
	Section 1.124 Good Utility Practice	2
	<u>Section 1.132</u> <u>Independent Director</u>	
	Section 1.143 Industry Sector(s).....	2
	Section 1.154 Investor Owned Utility	23
	Section 1.13 Large End Use Electricity Customers	2
	Section 1.165 Member	32
	<u>Section 1.167</u> <u>Membership</u>	
	Section 1.187 Municipal Utilities.....	23
	Section 1.198 NERC	32
	Section 1.2019 	Person 32
	Section 1.210 Public Utility District.....	32
	Section 1.214 Regional Entity.....	3
	Section 1.232 Regulatory Participant	3
	Section 1.243 Reliability Standards	43
	Section 1.22 Small End Use Electricity Customers.....	3
	Section 1.254 Transmission System	43
	Section 1.24 Regional Planning Entity	3
ARTICLE 2	PURPOSE.....	4
	Section 2.1 Purpose.....	4
	Section 2.2 Activities.....	4
	Section 2.3 Not-for-Profit Corporation	4
ARTICLE 3	POWERS	4
	Section 3.1 Powers	4
ARTICLE 4	OFFICES	4
	Section 4.1 Offices.....	4

Formatted: Normal

Formatted: Normal

Formatted: Font: 12 pt, Bold

ARTICLE 5 MEMBERS	5
Section 5.1 Classes of Members.....	5
Section 5.2 Qualifications of Members	5
Section 5.3 Admission of Members	5
Section 5.4 Voting Rights.....	5
Section 5.5 Transfer of Membership	5
Section 5.6 Obligations of Members	5
Section 5.7 Withdrawal.....	5
Section 5.8 Budget and Fees	6
ARTICLE 6 MEETING OF MEMBERS	6
Section 6.1 Annual Meeting of Members	6
Section 6.2 Special Meetings of Members	6
6.2.1 Who May Call.	6
6.2.2 Notice of Meeting.	7
6.2.3 Time and Place of Special Meetings.....	7
6.2.4 Notice Requirements; Business Limited.	7
Section 6.3 Notice Requirements.....	7
6.3.1 To Whom Given.	7
6.3.2 When Given; Contents.	7
6.3.3 Waiver of Notice; Objections.....	7
Section 6.4 Record Date; Determining Members Entitled to Notice and Vote.....	8
Section 6.5 Right to Vote; Act of Members.....	8
6.5.1 Special Voting Requirements.....	8
6.5.2 Change of Dues Structure.	8
6.5.3 Fractional Voting Alternative.....	8
Section 6.6 Quorum.....	8
Section 6.7 Action by Written Ballot	9
Section 6.8 Action by Electronic Communication.....	9
Section 6.9 Member Representatives; Proxies.....	9
6.9.1 Designation of Representative.	9
6.9.2 Authorization.....	9
6.9.3 Effective Period.	9
6.9.4 Revocation.	9
Section 6.10 Reimbursement of Member Expenses	10
ARTICLE 7 BOARD OF DIRECTORS	10
Section 7.1 Management of Corporation	10
Section 7.2 Voting.....	10
Section 7.3 Composition of the Board of Directors	10
Section 7.4 Terms of Directors	11
Section 7.5 Compensation and Reimbursement	11
Section 7.6 Vacancies	11
Section 7.7 Meetings; Notice.....	11
Section 7.8 Quorum.....	12

Section 7.9	Board Action.....	12
Section 7.10	Action Without a Meeting.....	12
Section 7.11	Action by Electronic Communication.....	12
ARTICLE 8	ORGANIZATIONAL GROUPS.....	12
Section 8.1	Establishment of Organizational Groups.....	12
Section 8.2	Reimbursement.....	13
ARTICLE 9	OFFICERS.....	13
Section 9.1	Officers.....	13
Section 9.2	Election and Term of Office.....	13
Section 9.3	Removal.....	13
Section 9.4	Vacancies.....	13
Section 9.5	President.....	13
Section 9.6	Secretary.....	14
Section 9.7	Treasurer.....	14
ARTICLE 10	CERTIFICATES OF MEMBERSHIP.....	14
Section 10.1	Certificates of Membership.....	14
ARTICLE 11	BOOKS AND RECORDS.....	15
Section 11.1	Books and Records; Financial Statements.....	15
ARTICLE 12	FISCAL YEAR.....	15
Section 12.1	Fiscal Year.....	15
ARTICLE 13	TRANSFER OF ASSETS.....	15
Section 13.1	Member Approval Not Required.....	15
Section 13.2	Member approval; when required.....	15
ARTICLE 14	CONTRACTS, CHECKS, DEPOSITS, AND GIFTS.....	15
Section 14.1	Contracts.....	15
Section 14.2	Checks, Drafts, or Orders.....	16
Section 14.3	Deposits.....	16
Section 14.4	Gifts.....	16
ARTICLE 15	INSURANCE, LIABILITY, AND INDEMNIFICATION.....	16
Section 15.1	Insurance.....	16
Section 15.2	Limitations on Liability.....	16
Section 15.3	Indemnification.....	16
ARTICLE 16	PARTICIPATION BY REGULATORY PARTICIPANTS.....	18
Section 16.1	Regulatory Participants.....	18
ARTICLE 17	PARTICIPATION BY FEDERAL POWER MARKETING ADMINISTRATIONS ¹⁸	
Section 17.1	<u>Power Marketing Administrations Participation</u>	18
Section 17.2	<u>Failure of Congress to Make Appropriations</u>	18

Section 17.3	<u>Inapplicability of Bylaws to Congressional Members and Delegates</u>	19
Section 17.4	<u>No Solicitation of Power Marketing Administration Participation</u>	19
Section 17.5	<u>Provisions Applicable to the Corporation</u>	19
17.5.1.	<u>No Discrimination</u>	19
17.5.2.	<u>Contract Work Hours and Safety Standards Act</u>	19
17.5.3.	<u>Imprisonment</u>	19
ARTICLE 18 HEARINGS AND DISPUTE RESOLUTION		19
Section 18.1	<u>Hearings</u>	19
Section 18.2	<u>Disputes</u>	20
ARTICLE 19 AMENDMENT OF BYLAWS		20
Section 19.1	<u>Changes to Bylaws</u>	20

**BYLAWS
OF THE
MIDWEST RELIABILITY ORGANIZATION, INC.**
a Delaware nonprofit corporation
(the “Corporation”)

ARTICLE 1
DEFINITIONS

Section 1.1 Adjunct Member. “Adjunct Member” means an entity that: (1) is not eligible to belong to an Industry Sector; (2) has a material interest in reliability issues in the Corporation’s Region and (3) becomes an Adjunct Member of the Corporation.

Formatted: Font: Not Bold, No underline

Section 1.2 Affiliate. “Affiliate” means with respect to any entity, any other entity that, directly or indirectly, through one or more intermediaries, controls, or is controlled by, or is under common control with, such entity, as determined in the sole discretion of the board of directors of the Corporation. For this purpose, “control” may be presumed by the direct or indirect ownership of 50 percent or more of the outstanding voting capital stock or other equity interests having ordinary voting power. A member of, or owner of an interest in, a transmission company that FERC has found meets the independence requirements for a regional transmission organization shall not be deemed to be an affiliate of such transmission company.

~~Section 1.1~~

Section 1.3 Bulk-Power System. “Bulk-Power System” means (1) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (2) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in local distribution of electric energy. The term Bulk-Power System shall be interpreted consistently with any definition given by NERC.

Section 1.4 Bulk-Power System Users. “Bulk-Power System Users” means any entity that sells, purchases, or transmits electric power over the Bulk-Power System, or that owns, operates or maintains facilities or control systems that are part of the Bulk-Power System.

Section 1.5 Canadian Utilities. “Canadian Utilities” means any government-owned utility serving in Canada within the Corporate Region.

Formatted: List Paragraph

Section 1.6 Corporation. “Corporation” means Midwest Reliability Organization, Inc.

Section 1.7 Cooperative. “Cooperative” means an entity serving within the Corporate Region which generally has the following characteristics: (1) private independent electric utility; (2) incorporated under the laws of ~~the a~~ states in which they operate; (3) established to provide electric service to its members; (4) owned by the

consumers they serve; and (5) governed by a board of directors elected from the membership. This sector includes Generation and Transmission Cooperatives and Public Utility Districts.

~~Section 1.6~~**Section 1.8 Corporate Region.** “Corporate Region” means the geographic area boundaries of the Bulk-Power Systems as designated by the then current delegation agreement, each of the Members.

~~Section 1.7~~**Section 1.9 FERC.** “FERC” means the Federal Energy Regulatory Commission.

~~Section 1.8~~**Section 1.10 Federal Power Marketing Agencies.** “Federal Power Marketing Agencies” means agencies of the federal government created to market power within the Corporate Region.

~~Section 1.9~~**Section 1.11 Generators and Power Marketers.** “Generators and Power Marketers” means any entity that owns or operates more than 50 MW of generation in the Corporate Region, or is a power marketer doing business in the Corporate Region, and that does not qualify also to participate in the Investor-Owned Utility, Cooperative, Municipal Utility, Federal Power Marketing Agency or Canadian Utilities Sector.

Section 1.12 Good Utility Practice. “Good Utility Practice” means any of the practices, methods and acts engaged in or approved by a significant portion of the electric utility industry during the relevant time period, or any of the practices, methods and acts which, in the exercise of reasonable judgment in light of the facts known at the time the decision was made, could have been expected to accomplish the desired result at a reasonable cost consistent with good business practices, reliability, safety and expedition. Good Utility Practice is not intended to be limited to the optimum practice, method, or act to the exclusion of all others, but rather to be acceptable practices, methods, or acts generally accepted in the Corporate Region.

~~Section 1.10~~**Section 1.13 Independent Director.** “Independent Director” means an individual who is not (1) an officer or employee of the Corporation; (2) a member, director, officer or employee of a Member or Adjunct Member of the Corporation; (3) a director, officer or employee of any Registered Entity on the NERC registry; or (4) reasonably perceived as having a direct financial interest in the outcome of a decision by the board of directors and who (a) does not have any other relationship that would interfere with the exercise of independent judgment in carrying out the responsibilities of a director and (b) meets any additional requirements of independence established by the board of directors.

~~Section 1.11~~**Section 1.14 Industry Sector(s).** “Industry Sector or Sector(s)” means a group of Bulk-Power System Users in the Corporate Region with substantially similar reliability interests, as determined by these Bylaws. The Industry Sectors shall include the following: (1) Transmission System Operators; (2) Generators and Power Marketers; (3) Investor Owned Utilities (4) Cooperatives; (5) Municipal Utilities (6) Federal Power Marketing Agencies; and (7) Canadian Utilities; ~~(8) Large End Use Electricity Customers; and (9) Small End Use Load Electricity Customers.~~

Formatted: List Paragraph

~~Section 1.12~~**Section 1.15 Investor Owned Utility.** “Investor Owned Utility” means any for-profit entity that owns and operates a distribution system and serves end-use load within the Corporate Region pursuant to an obligation to serve under state, federal or provincial law, including a default service obligation, or pursuant to a tariff by which the entity offers service to the general public.

~~Section 1.13~~ ~~**Large End-Use Electricity Customers.**~~ “~~Large End-Use Electricity Customers~~” means ~~any entity in North America with: (1) at least one service delivery taken at 50 kV or higher (radial supply or facilities dedicated to serve customers) that is not purchased for resale; or (2) any single end use customer with an average aggregated service load (not purchased for resale) of at least 50,000 MWh annually, excluding cogeneration or other back feed to the serving utility. This sector also includes organizations are represent the interest of such entities.~~

Formatted: Indent: Left: 0.75", No bullets or numbering

Section 1.16 Member. “Member” means any entity eligible to belong to an Industry Sector(s) that becomes a Member of the Corporation, ~~a member of the Corporation.~~

~~Section 1.14~~**Section 1.17 Membership.** “Membership” includes Adjunct Members and Members of the Corporation. Membership in the Corporation is voluntary and does not affect NERC registration.

Formatted: Font: Not Bold, No underline

~~Section 1.15~~**Section 1.18 Municipal Utilities.** “Municipal Utilities” means any electric utility that is owned by a state or municipality, or group of municipalities, including a joint action agency, which serves within the Corporate Region.

~~Section 1.16~~**Section 1.19 NERC.** “NERC” means the North American Electric Reliability Corporation or a successor entity.

~~Section 1.17~~**Section 1.20 Person.** “Person” means any natural person, corporation, Cooperative, partnership, association, or other private or public entity.

~~Section 1.18~~**Section 1.21 Public Utility District.** “Public Utility District” means an entity that is a state political or governmental subdivision which owns electric generation, transmission and distribution facilities and that was created and organized under state statutes that are different than those that Municipal Utilities in the same state are created and organized under.

~~Section 1.19~~**Section 1.22 Regional Entity.** “Regional Entity” means an entity having authority pursuant to a delegation agreement with NERC and pursuant to any agreements or laws relating to the Corporation’s functions in Canada.

~~Section 1.20~~**Section 1.23 Regulatory Participant.** “Regulatory Participant” means any state or provincial regulatory agencies in the Corporate Region exercising authority over the rates, terms or conditions of electric service of an entity other than itself within the Corporate Region, or the planning, siting, construction or operation of electric facilities of an entity other than itself within the Corporate Region, as well as any representatives of FERC, regional advisory bodies that may be established by FERC, or representatives of any federal regulator or agency.

~~Section 1.21~~ **Section 1.24 Reliability Standard.** “Reliability Standard” means a NERC reliability standard, duly in effect, under the rules, regulations and laws governing such standards, to provide for reliable operation of the Bulk-Power System.

~~Section 1.22~~ **~~Small End-Use Electricity Customers.~~** ~~“Small End-Use Electricity Customers” means: (1) any person or entity within North America that takes service below 50 kV; or (2) any single end-use customer with an average aggregated service load (not purchased for resale) of less than 50,000 MWh annually, excluding cogeneration or other back-feed to the serving utility. This sector also includes organizations (including state consumer advocates) that represent the interests of such entities.~~

Formatted: Indent: Left: 0.25", No bullets or numbering

~~Section 1.23~~ **Section 1.25 Transmission System Operator.** “Transmission System Operator” means an entity that operates or controls operation of high voltage transmission facilities within the Corporate Region (more than 300 miles of transmission at 100 kV or greater) that does not also own, operate or control generation within the Corporate Region, except to the limited extent permitted by FERC for independent transmission organizations with respect to ancillary service obligations. Transmission System Operators include: (1) regional transmission organizations; (2) independent transmission providers; (3) independent system operators; (4) and transmission-only companies.

~~Section 1.24~~ **~~Regional Planning Entity.~~** ~~“Regional Planning Entity” means an entity which is subject to Reliability Standards in the MRO Region and shall be eligible for MRO membership.~~

Formatted: Indent: Left: 0.25", No bullets or numbering

ARTICLE 2 **PURPOSE**

Section 2.1 Purpose. The Corporation will be a Regional Entity within the NERC structure for the purpose of preserving and enhancing electric service reliability, adequacy and security in the Corporate Region and other interconnected regions for the benefit of all end-users of electricity and all entities engaged in providing electric services in the Corporate Region, ~~with due regard for safety, environmental protection and economy of service.~~

Section 2.2 Activities. In support and furtherance of its purpose, the Corporation’s responsibilities shall include, but not be limited to: (1) proposing Reliability Standards, including regional variances or regional Reliability Standards required to maintain and enhance electric service reliability, adequacy and security in the Corporate Region; (2) assessing compliance with and enforcing Reliability Standards, to the extent authorized by applicable agreements and/or law governing a Member’s membership in the Corporation; (3) conducting investigations and data analysis on disturbances, system events, and related matters; (4) conducting long-term assessments of reliability within the Corporate region; and (5) other related activities.

Section 2.3 Not-for-Profit Corporation. The Corporation is operated as a Delaware non-stock, nonprofit corporation and is organized pursuant to the general corporation law of the State of Delaware.

ARTICLE 3
POWERS

Section 3.1 Powers. The Corporation shall have the power to engage in any lawful act or activity for which corporations may be organized under the general corporation law of the State of Delaware, subject to any limitations provided in applicable federal, provincial or state law or in the Corporation's certificate of incorporation or these Bylaws.

ARTICLE 4
OFFICES

Section 4.1 Offices. The principal office of the Corporation shall be located initially within the Corporate Region, at such location as the board of directors may from time to time determine, giving consideration to the total cost to the Corporation and convenience of travel for staff, Members and Regulatory Participants. Once established, the principal office may remain in its location, even if outside the Corporate Region.

ARTICLE 5
MEMBERS

Section 5.1 Classes of Members. The Corporation shall have ~~one~~ two classes of ~~m~~Members, Adjunct Members and Members.

~~Section 5.1~~**Section 5.2 Affiliates.** Each Affiliate of a Member or Adjunct Member may separately be a Member or Adjunct Member, respectively.

~~Section 5.2~~ **Qualifications of Members.** ~~A Member may be any entity eligible to be a member of an Industry Sector.~~

Section 5.3 Admission of Members and Adjunct Members. New Members and Adjunct Members may join the Corporation upon submittal of an application, in a form approved by the president, and payment of the fees as established by the Corporation. An entity applying to be a ~~The~~ Member shall designate the Industry Sector to which it belongs. A Member may change its Industry Sector designation once each calendar year, by providing notice to the president at least sixty (60) days prior to the beginning of such year. The president shall review a membership application and may request demonstration by the applicant that it qualifies for membership in a particular Industry Sector or as an Adjunct Member. Any dispute with respect to a Member's or Adjunct Member's qualifications ~~for a particular Sector~~ shall be resolved by the board of directors. The president shall have authority to approve an application for membership, subject to review by the board of directors.

Section 5.4 Voting Rights. Each Member in good standing shall be entitled to one vote in the Industry Sector in which it is a Member, on matters submitted to a vote of Members. A Member delinquent in payment of its dues, fees or other obligations to the Corporation shall not be entitled to a vote.

Formatted: Indent: Left: 0.75", No bullets or numbering

Section 5.5 Transfer of Membership. ~~A Member of the Corporation may not transfer its membership~~ or a right arising from such membership may not be transferred except to any Person succeeding to all or substantially all of the assets of the Member or Adjunct Member. The president shall have authority to approve any such transfer, subject to review by the board of directors.

Section 5.6 Obligations of Members and Adjunct Members. By applying for Membership and becoming a Member of the Corporation, each the Member acknowledges applicant acknowledges that it is authorized and agrees to comply with, Reliability Standards to the extent such standards are applicable, and other obligations ~~of Members of the Corporation as~~ set forth in these Bylaws or duly adopted by the board of directors in order to achieve the purposes of the Corporation. Such obligations include but are not limited to requirements to provide data and information needed to perform the functions of the Corporation and the payment of dues and any authorized penalties, including penalties and other obligations resulting from violations of Reliability Standards assessed in accordance with NERC rules and subject to applicable regulatory approval-

Section 5.7 Withdrawal. ~~A Member may withdraw~~ from Membership participation in the Corporation is accomplished by providing written notice to the president of the Corporation of such intent to withdraw. Such notice shall specify a date, not earlier than thirty (30) days from the date of notice, on which the withdrawal shall become effective; provided however, that any such withdrawing Member or Adjunct Member shall remain liable to the Corporation for any fees, dues, sanctions or obligations to the Corporation incurred during the entity's Membership while it was a Member, as well as its share of any obligations of the Corporation for the current fiscal year. If notice is given after October 1 of the current calendar year, the entity Member will also be liable for any fees and dues included in the budget for the following fiscal year. ~~Section 5.7 does not apply to any fees, dues, or obligations associated with the Corporation responsibilities under delegated authority from NERC or applicable regulatory authorities.~~

Section 5.8 Budget and Fees. The board of directors shall propose to NERC a budget for delegated functions exercised by the Corporation pursuant to a delegation agreement with NERC and pursuant to any agreements or laws relating to the Corporation's functions in Canada. For those functions outside the scope of the Corporation's delegated functions, the board of directors may from time to time fix the amount of dues, assessments, or fees, if any, and determine the methods of collection, consistent with this Section, the regulations of applicable government authorities, and any resolutions duly adopted by the Members under Section 6.5.2 of these Bylaws.

ARTICLE 6 **MEETING OF MEMBERS**

Section 6.1 Annual Meeting of Members. The Members shall hold an annual meeting each calendar year ~~of each year~~. ~~The annual meeting of the Members shall be held in~~ December, or at such other time specified by the board of directors, in order for Members to review the proposed budget and operations of the Corporation. Adjunct Members may attend the annual meeting of Members. The Membership All Members shall be

entitled to at least thirty (30) days prior written notice of the annual meeting. At or before the annual meeting of Members: (1) each Industry Sector shall elect the successor(s), if any, for any director(s) from ~~their~~ its Industry Sector whose term will expire before the next annual meeting of the Members, provided however, that any Industry Sector may elect a successor director representing such Industry Sector prior to such annual meeting, in accordance with the provisions of this Article 6, in which case the election of such succeeding director(s) shall be reported to the Corporation at such annual meeting; (2) the Members will elect Independent Directors, if any; (3) the president and treasurer shall report on the activities and financial condition of the Corporation; and ~~(4)~~ the Members shall consider and act upon such other matters as may be raised, consistent with the notice of the annual meeting. The failure to hold an annual meeting in accordance with these Bylaws shall not affect the validity of a corporate action.

Section 6.2 Special Meetings of Members.

6.2.1 Who May Call. Special meetings of the Members may be called by six (6) members of the board of directors, by the president or if at least 10 percent of the Members sign, date, and deliver to the president one or more written demands for a special meeting describing the purpose for which it is to be held. Adjunct Members may attend special meetings of the Members.

6.2.2 Notice of Meeting. Within fifteen (15) days after receipt of a demand for a special meeting from Members, the president shall cause a special meeting to be called and held on notice to the Membership no later than forty-five (45) days after receipt of the demand. If the president fails to cause a special meeting to be called and held as required by this section, a Member making the demand may call the meeting by giving notice under Section 6.3. In either event, notice of the meeting and the costs of the meeting shall be at the expense of the Corporation.

6.2.3 Time and Place of Special Meetings. Special meetings of the Members shall be held at a location designated by the president or the board of directors. If a special meeting is demanded by the Members, the meeting must be held in a facility of appropriate size to accommodate the Membership and at a location within the Corporate Region.

6.2.4 Notice Requirements; Business Limited. The notice of a special meeting must contain a statement of the purposes of the meeting. The business transacted at a special meeting is limited to the purposes stated within the notice of the meeting. Business transacted at a special meeting that is not included in those stated purposes is voidable by or on behalf of the Corporation, unless 90 percent of the Members entitled to vote were present at such meeting or have waived notice of the meeting under Section 6.3.

Section 6.3 Notice Requirements.

6.3.1 To Whom Given. Notice of meetings of Members must be given to the Membership every Member as of the record date determined under Section 6.4. If the meeting is an adjourned meeting and the date, time and place of the meeting were

announced at the time of the adjournment, notice is not required unless a new record date for the adjourned meeting is or must be fixed.

6.3.2 When Given; Contents. In all cases where a specific minimum notice period has not been fixed by law or these Bylaws, the notice must be given at least five (5) days before the date of a meeting and not more than sixty (60) days before the date of a meeting. The notice must contain the date, time and place of the meeting, and an agenda of the matters upon which action may be taken at the meeting. A matter may be added to the agenda of a meeting at the meeting upon the affirmative vote of three-quarters (3/4) of the Sector votes cast on a motion to amend the agenda.

6.3.3 Waiver of Notice; Objections. A Member may waive notice of a meeting of Members. A waiver of notice by a Member entitled to notice is effective whether given before, at, or after the meeting, and whether given in writing, or by attendance. Attendance by a Member at a meeting is a waiver of notice of that meeting, unless the Member objects at the beginning of the meeting to the transaction of business because the meeting is not lawfully called or convened, or objects before a vote on an item of business because the item may not lawfully be considered at that meeting and does not participate in the consideration of the item at that meeting.

Section 6.4 Record Date; Determining Members Entitled to Notice and Vote.

The board of directors may fix a date not more than forty (40) days before the date of a meeting of Members as the date for the determination of the Members ~~hip~~ entitled to notice of ~~and entitled to vote at~~ the meeting and the Members entitled to vote at the meeting. When a date is so fixed, only ~~the Membership Members~~ on that date ~~is~~are entitled to notice and only the Members are entitled to vote at a ~~meeting of the Mmembers-membership meeting~~ unless the board of directors fixes a new date for determining the right to notice and to vote, which it must do if the meeting is adjourned to a date more than sixty (60) days after the record date for determining Members ~~hip~~ entitled to notice of the original meeting.

Section 6.5 Right to Vote; Act of Members. Voting of the Members shall be by Industry Sector, with each Industry Sector entitled to the same number of votes as it has directors on the board. If a quorum is present, except with respect to amendments of these Bylaws, modification of a budget approved by the board of directors or termination of the Corporation, the affirmative vote of the majority of the Industry Sector votes present and entitled to vote, which must also be a majority of the required quorum, is the act of the Members, however, in no event will an action of the Members be valid where the action was passed solely by the vote of Members from two Industry Sectors or defeated solely by the vote of Members in a single Industry Sector. Within an Industry Sector, each Member within the Industry Sector shall have one vote. If a quorum is present with respect to the Industry Sector, the affirmative vote of the majority of the Members within the Industry Sector present and entitled to vote, which must also be a majority of the required quorum, is the act of the Industry Sector. All of the Industry Sector's votes shall be cast consistent with the act of the Industry Sector unless the Industry Sector adopts a fractional voting alternative as described in Section 6.5.3.

6.5.1 Special Voting Requirements. In order to amend the Bylaws, except as provided in Article ~~20-19~~ with respect to the board of directors, two-thirds (2/3) of the Industry Sector votes cast shall be required to approve the proposed amendment. The substance of the proposed amendment must be contained in the notice of the meeting at which the vote will be taken; provided that, the Members may modify a proposed bylaw amendment at the meeting. Two-thirds (2/3) of the Industry Sector votes cast shall be required to approve any proposal to terminate the Corporation. To the extent practicable, all Member votes may be held electronically under such terms and conditions as are approved by the Board.

6.5.2 Change of Dues Structure. The Members may change the dues structure by resolution with an affirmative vote of two-thirds (2/3) of the Industry Sector votes cast.

6.5.3 Fractional Voting Alternative. An Industry Sector may adopt fractional voting. Member votes for and against are converted to percentages and multiplied by the applicable sector weight. Abstentions are not counted and do not impact the voting tabulation.

Section 6.6 Quorum. A quorum for a meeting of Members is a majority of the Industry Sector votes entitled to vote at the meeting. A quorum for a meeting of an Industry Sector is a majority of the Members of that Industry Sector present or voting electronically on matters before the meeting. A quorum is necessary for the transaction of business at a meeting of Members. If a quorum is not present, a meeting may be adjourned from time to time for that reason by the Industry Sectors or Members then represented or present.

Section 6.7 Action by Written Ballot. An action that may be taken at a regular or special meeting of Members may be taken without a meeting if the Corporation mails or delivers a written ballot to every Member entitled to vote on the matter. Whenever possible, voting by Industry Sectors for directors shall be by written ballot preceding the regular meeting of the Members.

Approval by written ballot is valid only when the number of votes cast by ballot equals or exceeds the quorum required to be present at a meeting authorizing the action, and the number of approvals equals or exceeds the number of votes that would be required to approve the matter at a meeting at which the total number of votes cast was the same as the number of votes cast by ballot.

Solicitations for votes by written ballot must: (1) indicate the number of responses needed to meet the quorum requirements; (2) state the percentage of approvals necessary to approve the matter; and (3) specify the time by which a ballot must be received by the Corporation in order to be counted. A written ballot may not be revoked.

Section 6.8 Action by Electronic Communication. Any vote of an Industry Sector to elect a board member or for any other purpose may be taken by electronic means without a meeting or during a meeting. In addition, a conference among Members by a means of communication through which the participants may simultaneously hear each other during the conference is a meeting of the Members, if the same notice is given of the

conference as would be required for a meeting and if the number of persons participating in the conference is a quorum. Participation in a meeting by this means is personal presence at the meeting. A Member may participate in a meeting of the Members by a means of communication through which the Member, other persons participating, and all persons physically present at the meeting may simultaneously communicate with each other during the meeting. Participation in a meeting by this means constitutes personal presence at the meeting.

Section 6.9 Member Representatives; Proxies.

6.9.1. Designation of Representative. Each year prior to the annual meeting of Members, each Member shall designate the individual authorized to vote on Corporation matters on behalf of the Member, in accordance with procedures approved by the board. A Member may change such designation at any time.

6.9.2 Authorization. The individual designated to vote by a Member may appoint a proxy to vote or otherwise act for the Member at any meeting or electronically by signing an appointment form either personally or by an attorney so designated by the Member.

6.9.3 Effective Period. An appointment of a proxy is effective when received by the secretary or other officer or agent authorized to tabulate votes. An appointment is valid for the next regular or specially scheduled meeting or electronic ballot. However, a proxy is not valid for more than sixty (60) days from its date of execution.

6.9.4 Revocation. An appointment of a proxy is revocable by the Member. Appointment of a proxy is revoked by the person appointing the proxy by signing and delivering to the secretary or other officer or agent authorized to tabulate proxy votes. This may be done either in a written statement that the appointment of the proxy is revoked or a subsequent appointment form.

Section 6.10 Reimbursement of Membership Meeting Expenses. The Corporation will be under no obligation to reimburse the Membership Members for expenses associated with their attendance at regular or special Member meetings.

ARTICLE 7
BOARD OF DIRECTORS

Section 7.1 Management of Corporation. Consistent with these Bylaws, the business and affairs of the Corporation shall be managed by or under the direction of a board of directors. The duties of the board will include, but will not be limited to the following: (1) govern the Corporation and oversee all of its activities; (2) establish and oversee all organizational groups; (3) oversee accomplishment of all functions set forth in any delegation or other agreement with NERC or any governmental entity related to development, monitoring and enforcement of Reliability Standards and related matters; (4) approve, revise and enforce Member data and information requirements and related confidentiality requirements; (5) establish and approve an annual budget; (6) represent the Corporation in legal and regulatory proceedings; (7) hire the president. The board of directors shall select a chair and a vice-chair

from among the members of the board. The board may establish board committees as appropriate.

Section 7.2 Voting. Each director shall have one vote with respect to decisions of the board.

Section 7.3 Composition of the Board of Directors. The board of directors shall consist of nineteen (19) board members, seventeen (17) of the board members are elected by the Industry Sectors as follows:

(a). Three (3) directors from the Transmission System Operators Sector;

(b). Two (2) directors from the Generators and Power Marketers Sector;

(c). Five (5) directors from the Investor Owned Utilities Sector;

(1). Two (2) directors must be from utilities with less than 3,000 megawatts of end-use load.

(2). Three (3) directors must be from utilities with 3,000 megawatts or greater of end-use load.

(d). Two (2) directors from the Cooperative Sector;

(e). Two (2) directors from the Municipal Utilities Sector;

(f). One (1) director from the Federal Power Marketing Agencies; and

(g). Two (2) directors from the Canadian Utilities Sector provided that both directors are not residents of the same Canadian province;

~~(h). One (1) director from the Large End-Use Electricity Customers Sector, and~~

~~(i);(h). One (1) director from the Small End Use Electricity Customers Sector.~~

Provided, however, that in choosing directors from an Industry -Sector, there shall not be more directors from a particular Industry Sector than there are actual Members of such Industry Sector.

Members shall endeavor to select directors from Industry Sectors among individuals holding senior management or officer positions in Member organizations, and with a view toward ensuring geographic representation of the Corporate Region on the board. No two directors elected from Industry Sectors may be employees of a single Member or employees of Members

that are affiliates. To the extent the Members of an Industry Sector do not select a director, that director position shall remain vacant until a director is selected by the Industry Sector.

Two (2) board members shall be Independent Directors nominated by the board of directors and elected by the members. Independent Directors shall have relevant senior management expertise and experience to the reliable operation of the bulk power system in North America.

Formatted: Font: (Default) Times New Roman, 12 pt

Section 7.4 Terms of Directors. ~~The~~All directors will serve three-year, staggered terms~~except—The~~ initial term for one of the s of the independent directors shall be two (2) years. initial directors will be selected by lot at the first meeting of the board of directors. Any director elected by an Industry Sector may be removed at any time by the affirmative vote of two-thirds (2/3) of the Members of the Industry Sector selecting such director. An Independent Director may be removed by the affirmative vote of two-thirds of the remaining directors. Any director may be removed by the board of directors for non-attendance of three consecutive board meetings.

Section 7.5 Compensation and Reimbursement. ~~All d~~Directors shall have the right to reimbursement by the Corporation of their actual reasonable travel expenses to board meetings or when specifically selected to represent the Corporation at a business meeting. The board of directors may set reasonable compensation for the service provided by Independent Directors; directors elected by an Industry Sector shall not receive compensation.

Section 7.6 Vacancies. If a director resigns, dies, changes corporate affiliation or is removed during the term of office for which elected, the directorship shall thereupon be vacant and shall be filled as soon as practicable and in accordance with the same procedures that the directorship had previously been by the Members of the respective Sector, by written or electronic ballot in accordance with the procedures and requirements set forth above. ~~The~~filled. The successor director elected by the Members of the Sector shall hold office for the unexpired term of the director replaced.

Section 7.7 Meetings; Notice. An annual meeting of the board of directors shall be held without notice immediately following the annual meeting of the Members to elect the chair and vice-chair of the board of directors for the next year. In addition, regular meetings may be held at such time or times as fixed by the board of directors. Schedules of regular meetings of the board of directors shall be published by the secretary and provided to the all Members~~hip~~. Special meetings of the board of directors may be called by the president or by three directors and shall be held at the principal office of the Corporation, or such other place within the Corporate Region as determined by the president after consultation with the board. Notice of the date, time, and place of a special meeting shall be given by the secretary not less than seven (7) days prior to the meeting by mail, telegram, or electronic communication to each director and the Member~~hip~~. Except as necessary to discuss personnel issues, litigation or similar sensitive or confidential matters, all meetings of the board of directors shall be open to Members~~hip~~ and other interested persons.

Section 7.8 Quorum. A majority of the directors currently holding office is a quorum for the transaction of business.

Section 7.9 Board Action. The act of a majority of the directors present at a meeting at which a quorum is present shall be the act of the board of directors, unless the act of a greater number is required by law or these Bylaws, however, in no event will an action of the Directors be valid where the action was passed solely by the vote of Directors from two Industry Sectors or defeated solely by the vote of Directors in an single Industry Sector.-

Section 7.10 Action Without a Meeting. An action required or permitted to be taken at a board of directors meeting may be taken by written action, including electronic communication, signed by all of the directors of the Corporation. The written action is effective when signed by the required number of directors, unless a different effective time is provided in the written action.

Section 7.11 Action by Electronic Communication. A conference among directors by a means of communication through which the directors may simultaneously hear each other during the conference is a board meeting if the same notice is given of the conference as would be required for a meeting and if the number of directors participating in the conference is a quorum. Participation in a meeting by this means constitutes personal presence at the meeting. A director may participate in a board meeting by any means of communication through which the director, other directors participating, and all directors physically present at the meeting may simultaneously communicate with each other during the meeting.

ARTICLE 8 **ORGANIZATIONAL GROUPS**

Section 8.1 Establishment of Organizational Groups. The board of directors shall establish such organizational groups, consisting of committees, sub-committees, task forces and working groups of Members, as are necessary and appropriate to accomplish the purposes of the Corporation in an efficient and cost-effective manner. All organizational groups shall be subject to the direction and control of the board. The membership of organizational groups shall be determined based upon experience, expertise and geographic diversity and to the extent practicable shall include balanced representation of the Sectors.

The board of directors shall establish policies and procedures governing the creation of organizational groups, how they are populated, how voting and related matters are conducted and how they may be reorganized. The board shall conduct a review of all organizational groups of the Corporation on a periodic basis to ensure that the business of the Corporation is conducted in an efficient, cost-effective manner and shall include a statement of its conclusions and resulting actions in the board's report to Members at the annual meeting.

Section 8.2 Reimbursement. Consistent with the annual budget of the Corporation, the Board may authorize reimbursement by the Corporation for members of organizational groups (other than committees of the whole) of reasonable travel, meals and lodging expenses for organizational group meetings or for representation of the Corporation

at other business meetings as authorized by the board. The board of directors may authorize reimbursement for persons acting on behalf of the Corporation, as necessary in the interests of the Corporation.

ARTICLE 9
OFFICERS

Section 9.1 Officers. The officers of the Corporation shall include a president, a secretary, a treasurer and any other officers as may be elected or appointed in accordance with the provisions of this Article. The board of directors may elect or appoint any additional officers that it deems desirable, such other officers to have the authority and perform the duties prescribed by the board of directors. The same individual may hold any number of offices, except that of president.

Section 9.2 Election and Term of Office. The officers of the Corporation shall be elected by the board of directors. Each officer shall hold office at the pleasure of the board. New officers may be created and the positions filled at any meeting of the board of directors. Each elected officer shall hold office until his or her successor has been duly elected and qualified.

Section 9.3 Removal. Any officer elected by the board of directors may be removed by the affirmative vote of two-thirds (2/3) of the board of directors whenever in its judgment the best interests of the Corporation would be served thereby, but such removal shall be without prejudice to the contract rights, if any, of the officer so removed. Election or appointment of an officer or agent shall not of itself create contract rights.

Section 9.4 Vacancies. A vacancy in any office because of death, resignation, removal, disqualification, or otherwise, may be filled by the board of directors for the unexpired portion of the term.

Section 9.5 President. The president shall be, in the discretion of the board of directors, either an employee of or contractor to the Corporation and shall:

- (a). be the ~~principal-chief~~ executive ~~and-operating~~ officer of the Corporation;
- (b). sign certificates of membership, and may sign any deeds, mortgages, deeds of trust, notes, bonds, contracts or other instruments authorized by the board of directors to be executed, except in cases in which the signing and execution thereof shall be expressly delegated by the board of directors or by these Bylaws to some other officer or agent of the Corporation; and
- (c). perform all duties incident to the office of president and chief executive officer, including hiring and directing staff, and such other duties as may be prescribed by the board of directors from time to time.

Section 9.6 Secretary. The secretary shall ensure that the following duties are carried out:

- (a). the minutes of the meetings of the Members and of the board of directors are recorded;
- (b). all required notices are duly given in accordance with these Bylaws and as required by law;
- (c). a register of the current names and addresses of the Membership ~~all Members~~ is maintained;
- (d). a complete copy of the ~~A~~articles of ~~I~~ncorporation and Bylaws of the Corporation containing all amendments thereto are kept on file at all times, which copies shall always be open to the inspection of ~~any~~the Membership; and
- (e). generally perform all duties incident to the office of secretary and such other duties as may be prescribed by the board of directors from time to time.

Section 9.7 Treasurer. The treasurer shall be responsible for the following activities:

- (a). maintain custody of all funds and securities of the Corporation;
- (b). receipt of and the issuance of receipts for all monies due and payable to the Corporation and for deposit of all such monies in the name of the Corporation in such bank or banks or financial institutions as shall be selected by the board of directors; and
- (c). generally perform all duties incident to the office of treasurer and such other duties as may be prescribed by the board of directors from time to time.

ARTICLE 10 **CERTIFICATES OF MEMBERSHIP**

Section 10.1 Certificates of Membership. The board of directors may provide for the issuance of certificates evidencing ~~m~~Membership in the Corporation, which certificates shall be in such form as may be determined by the board.

ARTICLE 11 **BOOKS AND RECORDS**

Section 11.1 Books and Records; Financial Statements. The Corporation shall keep at its registered office correct and complete copies of its ~~a~~Articles of Incorporation and Bylaws, accounting records, and minutes of meetings of Members, board of directors, and committees having any of the authority of the board of directors. A Member or Adjunct Member, or the agent or attorney of a Member or Adjunct Member, may inspect all books and records and voting agreements for any proper purpose at any reasonable time. Upon

request, the Corporation shall give the Member ~~or Adjunct Member~~ a statement showing the financial result of all operations and transactions affecting income and surplus during its last annual accounting period and a balance sheet containing a summary of its assets and liabilities as of the closing date of the accounting period.

ARTICLE 12
FISCAL YEAR

Section 12.1 Fiscal Year. The fiscal year of the Corporation shall be the calendar year.

ARTICLE 13
TRANSFER OF ASSETS

Section 13.1 Member Approval Not Required. The Corporation, by affirmative vote of the board of directors, may sell, lease, transfer, or dispose of its property and assets in the usual and regular course of its activities and grant a security interest in all or substantially all of its property and assets in the usual and regular course of its activities, upon those terms and conditions and for those considerations, which may be money, securities, or other instruments for the payment of money or other property, as the board of directors considers expedient, in which case no Member approval is required.

Section 13.2 Member Approval; When Required. The Corporation may sell, lease, transfer, or dispose of all or substantially all of its property and assets, including its good will, not in the usual and regular course of its activities, upon those terms and conditions and for those considerations, which may be money, securities, or other instruments for the payment of money or other property, as the board of directors considers expedient only when approved at a regular or special meeting of the Members by the affirmative vote of two-thirds (2/3) of all the Members. Notice of the meeting must be given to the Membership. The notice must state that a purpose of the meeting is to consider the sale, lease, transfer, or other disposition of all or substantially all of the property and assets of the Corporation.

ARTICLE 14
CONTRACTS, CHECKS, DEPOSITS, AND GIFTS

Section 14.1 Contracts. The board of directors may authorize any officer or officers or agent or agents of the Corporation, in addition to the officers so authorized by these Bylaws, to enter into any contract or execute and deliver any instrument in the name of and on behalf of the Corporation, and such authority may be general or may be confined to specific instances.

Section 14.2 Checks, Drafts, or Orders. All checks, drafts, or orders for the payment of money, notes, or other evidences of indebtedness issued in the name of the Corporation, shall be signed by such officer or officers or agent or agents of the Corporation, and in such manner as shall from time to time be determined by resolution of the board of directors.

Section 14.3 Deposits. All funds of the Corporation shall be deposited to the credit of the Corporation in such banks, trust companies, or other depositories as the board of directors may select.

Section 14.4 Gifts. The board of directors may accept on behalf of the Corporation any contribution, gift, bequest, or devise for any purpose of the Corporation.

ARTICLE 15 **INSURANCE, LIABILITY, AND INDEMNIFICATION**

Section 15.1 Insurance. The president is authorized to procure insurance to protect the Corporation against damages arising out of or related to any directive, order, procedure, action or requirement of the Corporation.

Section 15.2 Limitations on Liability. No director, officer, agent, employee or other representative of the Corporation, and no corporation or other business organization that employs a director of the Corporation, or any director, officer, agent or employee of such corporation or other business organization, shall be personally liable to the Corporation or any Member or Adjunct Member of the Corporation for any act or omission on the part of any such director, officer, agent, employee, or other representative of the Corporation, which was performed or omitted in good faith in his official capacity as a director, officer, agent, employee or other representative of the Corporation. However, this release of liability shall not operate to release such a director, officer, agent, employee or other representative of the Corporation from any personal liability resulting from willful acts or omissions knowingly or intentionally committed or omitted by him in breach of these Bylaws for improper personal benefit or in bad faith.

Section 15.3 Indemnification. It is the intent of the Corporation to indemnify its directors, officers, agents, employees, or other representatives to the maximum extent allowed by law consistent with these Bylaws. Each director, officer, agent, employee, or other representative of the Corporation shall be indemnified by the Corporation against all judgments, penalties, fines, settlements, and reasonable expenses, including legal fees, incurred by him as a result of, or in connection with, any threatened, pending or completed civil, criminal, administrative, or investigative proceedings to which he may be made a party by reason of his acting or having acted in his official capacity as a director, officer, agent, employee, or representative of the Corporation, or in any other capacity which he may hold at the request of the Corporation, as its representative in any other organization, subject to the following conditions:

(a). Such director, officer, agent, employee, or other representative must have conducted himself in good faith and, in the case of criminal proceedings, he must have had no reasonable cause to believe that his conduct was unlawful. When acting in his official capacity, he must have reasonably believed that his conduct was in the best interests of the Corporation, and, when acting in any other capacity, he must have reasonably believed that his conduct was at least not opposed to the best interests of the Corporation.

(b). If the proceeding was brought by or on behalf of the Corporation, however, indemnification shall be made only with respect to reasonable expenses referenced above. No indemnification of any kind shall be made in any such proceeding in which the director, officer, agent, employee, or other representative shall have been adjudged liable to the Corporation.

(c). In no event, however, will indemnification be made with respect to any described proceeding which charges or alleges improper personal benefit to a director, officer, agent, employee, or other representative and where liability is imposed upon him on the basis of the receipt of such improper personal benefit.

(d). In order for any director, officer, agent, employee, or other representative to receive indemnification under this provision, he shall vigorously assert and pursue any and all defenses to those claims, charges, or proceedings covered hereby which are reasonable and legally available and shall fully cooperate with the Corporation or any attorneys involved in the defense of any such claim, charges, or proceedings on behalf of the Corporation.

(e). No indemnification shall be made in any specific instance until it has been determined by the Corporation that indemnification is permissible in that specific case, under the standards set forth herein and that any expenses claimed or to be incurred are reasonable. These two (2) determinations shall be made by a majority vote of at least a quorum of the board consisting solely of directors who were not parties to the proceeding for which indemnification or reimbursement of expenses is claimed. If such a quorum cannot be obtained, a majority of at least a quorum of the full board, including directors who are parties to said proceeding, shall designate a special legal counsel who shall make said determinations on behalf of the Corporation. In making any such determinations, the termination of any proceeding by judgment, order, settlement, conviction, or upon plea of nolo contendere, or its equivalent, shall not, in and of itself, be conclusive that the person did not meet the standards set forth herein.

(f). Any reasonable expenses, as shall be determined above, that have been incurred by a director, officer, agent, employee, or other representative who has been made a party to a proceeding as defined herein, may be paid or reimbursed in advance upon a majority vote of a quorum of the full board, including those who may be a party to the same proceeding. However, such director, officer, agent, employee, or other representative shall have provided the Corporation with (i) a written affirmation under oath that he, in good faith, believes that he has met the conditions for indemnification herein, and (ii) a written undertaking that he shall repay any amounts advanced, with interest accumulated at a reasonable rate, if it is ultimately determined that he has not met such conditions. In addition to the indemnification and reimbursement of expenses provided herein, the president shall purchase insurance that would protect the Corporation, its directors, officers, agents, employees, or other representatives against reasonably expected liabilities and expenses arising out of the performance of their duties for the Corporation.

ARTICLE 16
PARTICIPATION BY REGULATORY PARTICIPANTS

Section 16.1 Regulatory Participants. All Regulatory Participants shall be entitled to ~~be Adjunct Members, and be provided with the same rights to notice of and participation in meetings or other activities of the Corporation as are provided to Members, but shall not have the right to vote.~~

Formatted: Font: Bold

ARTICLE 17
PARTICIPATION BY FEDERAL POWER MARKETING ADMINISTRATIONS

Section 17.1 Power Marketing Administrations Participation. The participation by the United States through Federal power marketing administrations (PMA) in the Corporation is subject in all respects to acts of Congress and to regulations of the Secretary of Energy established thereunder. This reservation includes, but is not limited to, the statutory limitations upon the authority of the Secretary of Energy to submit disputes arising hereunder to arbitration. In the event of a conflict between this Article ~~187~~ and any other Article of these Bylaws, this Article ~~178~~ shall have precedence with respect to the application of these Bylaws to the United States.

Section 17.2 Failure of Congress to Make Appropriations. Where activities provided for herein extend beyond the current fiscal year, continued expenditures by the United States are contingent upon Congress making the necessary appropriations required for the continued performance of the obligations of the PMA hereunder. In case such appropriations are not made, the Corporation and its Members hereby release the PMA from its contractual obligations under these Bylaws and from all liability due to the failure of Congress to make such appropriation.

Section 17.3 Inapplicability of Bylaws to Congressional Members and Delegates. No member of or delegate to Congress shall be admitted to any share or part of, or to any benefit that may have arisen from, these Bylaws, but this restriction shall not be construed to extend to these Bylaws if made with a corporation or company for its general benefit.

Section 17.4 No Solicitation of Power Marketing Administration Participation. The Corporation and its Members ~~hip~~ warrant that no Person or selling agency has been employed or retained to solicit or secure participation by a PMA in the Corporation upon an agreement or understanding for a commission, percentage, brokerage or contingent fee, excepting *bona fide* employees or *bona fide* established commercial or selling agencies maintained by the Members ~~hip~~ for the purpose of securing business. For breach or violation of this warranty, a PMA shall have the right to annul its participation in the Corporation without liability or, in its discretion, to deduct from its dues or fees the full amount of such commission, percentage, brokerage, or contingent fee.

Section 17.5 Provisions Applicable to the Corporation. For the purpose of this Section ~~187.5~~ the term "Contract" shall mean these Bylaws and the term "Contractor" shall

mean the Corporation. During the performance of this Contract, the Contractor agrees to the following provisions.

17.5.1. No Discrimination. Section 202 of the Executive Order No. 11246, 30 Fed. Reg. 12319 (1965), as amended by Executive Order No. 12086, 43 Fed. Reg. 46501 (1978), which provides, among other things, that the Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, or national origin, is incorporated by reference in the Contract.

17.5.2. Contract Work Hours and Safety Standards Act. The Contract, to the extent that it is of a character specified in Section 103 of the Contract Work Hours and Safety Standards Act, 40 U.S.C. § 329 (1986) (the “Act”), is subject to the provisions of the Act, 40 U.S.C. §§ 327-333 (1986), and to regulations promulgated by the Secretary of Labor pursuant to the Act.

17.5.3. Imprisonment. The Contractor agrees not to employ any person undergoing sentence of imprisonment in performing the Contract except as provided by 18 U.S.C. § 4082(c)(2) and Executive Order 11755, 39 Fed. Reg. 779 (1973).

ARTICLE 18
HEARINGS AND DISPUTE RESOLUTION

Section 18.1 Hearings. Except as otherwise provided in applicable agreements and/or law governing ~~a Member's m~~Membership in the Corporation, the Corporation shall be responsible for making final determinations regarding whether a Registered Entity has violated a Reliability Standard in accordance with the NERC Rules of Procedure.

Section 18.2 Disputes. Dispute resolution procedures will be established by the board of directors for disputes between Members, or between a Member and the Corporation, for issues arising under these Bylaws. Determinations related to violations of Reliability Standards will be resolved in accordance with the NERC Rules of Procedure. Except as otherwise provided in applicable agreements and/or law governing a Member’s membership in the corporation.

ARTICLE 19
AMENDMENT OF BYLAWS

Section 19.1 Changes to Bylaws. The power to adopt, amend or repeal these Bylaws is vested in the Members as set forth in Section 6.5 of these Bylaws; provided however, upon the passage of any federal reliability legislation and/or the adoption of related requirements and procedures by NERC or any regulatory agency with jurisdiction, the board or directors shall have authority upon a two-thirds (2/3) vote to amend these Bylaws as necessary and appropriate to comply with such law and related requirements.

**Proposed Renewal Agreement Between
SERC Reliability Corporation and Florida Reliability Coordinating Council
And Between
SERC Reliability Corporation and Southwest Power Pool, Inc.
For SERC to Act as Compliance Enforcement Authority for the
FRCC and SPP Registered Functions**

Action

(1) Approve proposed renewal agreements between SERC and FRCC and between SERC and SPP for SERC to continue to act as the Compliance Enforcement Authority (CEA) for the FRCC Registered Functions and the SPP Registered Functions, respectively. (2) Approve conforming amendments to Exhibit A to NERC-FRCC Delegation Agreement and Exhibit A to the NERC-SPP Delegation Agreement, respectively, to reference the SERC-FRCC and SERC-SPP renewal CEA Agreements.

Background

In 2010, the Board and FERC approved agreements between SERC and FRCC and between SERC and SPP pursuant to which SERC would act as the CEA for the FRCC and SPP Registered Functions. FRCC, through its Member Services Division, is registered as the Reliability Coordinator (RC) and the Planning Authority (PA) in the FRCC Region. SPP is registered as an RC, PA, Interchange Authority (IA), Reserve Sharing Group (RSG), Transmission Planner (TP) and Transmission Service Provider (TSP) in the SPP Regional Entity (SPP RE) Region. The current CEA Agreements went into effect in July 2010 and expire December 31, 2012. In approving the CEA Agreements, FERC required that they not renew automatically at the end of the initial term, but rather that SERC-FRCC and SERC-SPP be required to request approval from NERC and FERC to renew the CEA Agreements if they wanted the Agreements to continue beyond December 31, 2012.

SERC-FRCC and SERC-SPP have now requested approval from NERC to renew the CEA Agreements, and have submitted proposed renewal agreements that contain a number of revisions from the current CEA Agreements. Significant revisions (and non-revisions) in the proposed renewal Agreements are described below. Attachments 1 and 2 are, respectively, clean and redlined (against the current Agreement) versions of the proposed SERC-FRCC renewal CEA Agreement. Attachments 3 and 4 are, respectively, clean and redlined (against the current Agreement) versions of the proposed SERC-SPP renewal CEA Agreement. As discussed below, NERC staff recommends approval of the proposed SERC-FRCC and SERC-SPP renewal CEA Agreements.

Consideration of renewal of the CEA Agreements requires review of whether the Agreements are working as intended to provide effective compliance monitoring and enforcement services with respect to FRCC's and SPP's compliance with the Reliability Standards applicable to their respective Registered Functions. SERC conducted an on-site audit of the FRCC RC and PA functions for compliance with applicable operating/planning standard, and an on-site audit of the FRCC RC function for compliance with applicable CIP standards, in January and February 2012. SERC has also requested and received from FRCC periodic self-certifications and periodic data submittals concerning compliance with Reliability Standards applicable to the FRCC Registered Functions, in accordance with posted schedules. With respect to SPP, SERC conducted an onsite compliance audit in September 2010 of the IA, PA, RC, RSG, TP and TSP functions, covering 78 requirements of Reliability

Standards. SERC has also requested and received from SPP periodic self-certifications and periodic data submittals concerning compliance with Reliability Standards applicable to the SPP Registered Functions, in accordance with posted schedules. SERC is processing open enforcement actions involving the Registered Functions that were identified before SERC became the CEA, as well as any compliance items that have arisen since July 2010. NERC Compliance Operations has monitored SERC's performance as the CEA for the FRCC and SPP Registered Functions and believes that SERC has been providing appropriate coverage for its CEA responsibilities. NERC staff recommends renewal of the SERC-FRCC and SERC-SPP CEA arrangements.

Discussion of Terms of Proposed SERC-FRCC and SERC-SPP renewal CEA Agreements

SERC, FRCC and SPP have proposed renewal CEA Agreements that are revised in a number of respects from the current Agreements. Among other things, the revisions eliminate some provisions that are no longer needed, and they modify other provisions based on the Parties' experience. NERC staff reviewed drafts of the proposed renewal Agreements and recommended several changes that have been incorporated in the Agreements being presented to the Board for approval. Therefore, NERC staff recommends approval of the proposed renewal CEA Agreements. The following discussion describes principal revisions from the current Agreements, as well as key provisions of the current Agreements that are not substantively revised. The two proposed renewal Agreements are substantially identical, and therefore the following discussion applies to both renewal Agreements.

- Section 1, "Responsibilities of SERC," has not been substantively revised. This Section sets forth SERC's responsibilities under the Agreement as CEA.
- Section 4 of the current Agreement, which concerned the transfer of CEA responsibilities to SERC at the time the current Agreement went into effect in July 2010, is deleted as no longer needed.
- Section 4 (Section 5 in the current Agreement), concerning Compensation to SERC, has been revised to reflect a more simplified billing arrangement to which the Parties have agreed. Under the current Agreements, an estimated cost for the year is determined as part of the business plan and budget process and then billed by SERC to FRCC or SPP in four quarterly installments during the year, with a reconciliation of payments to actual costs incurred by SERC during the year taking place within 90 days following the end of the year and any true-up amounts being reflected in the Parties' budgets and assessments for the second following year. Under the renewal Agreements, SERC will continue to prepare, as part of the business plan and budget process, estimates of the costs (including an appropriate allocation of SERC's general and administrative (G&A) costs) it will incur during the upcoming year to act as CEA for the FRCC and SPP Registered Functions. These estimated costs will be excluded from SERC's assessments to Load-Serving Entities (LSEs) in the SERC Region and will be included in FRCC's and SPP's assessments to LSEs in their respective Regions. However, under the renewal Agreements, SERC will bill FRCC and SPP on a monthly basis for the costs actually incurred in the preceding month (including an appropriate allocation of SERC's G&A costs) in acting as the CEA for the FRCC and SPP Registered Functions. Therefore, no year-end reconciliation and true-up of billed amounts to actual costs incurred will be needed, and the provisions relating to the year-end reconciliation are deleted in the renewal Agreements.
- However, to ensure a reconciliation of budgeted to actual costs is provided for purposes of reporting to FERC in the required annual true-up filings, a new Section 4(c) is added in the renewal Agreements, specifying that the Parties shall record their costs and revenues associated with performance of the Agreement at the same level

of line-item detail as is used for their budgets that are submitted to NERC, and that each party shall include in its annual true-up report submitted to NERC a separate section showing the Party's actual and budgeted costs and revenues associated with performance of the Agreement, with an explanation of variances.

- Section 5 concerning Term and renewals provides that the renewal Agreement shall have a term from the Effective Date (expected to be January 1, 2013, subject to NERC and FERC approvals) to December 1, 2017, i.e., 5 years. The Agreement shall renew automatically for a Renewal Term of 5 years unless either Party gives written notice of termination at least 12 months prior to the end of the Term ending December 31, 2017. Additionally, during a Renewal Term, either Party may terminate the Agreement on 12 months written notice.
- Further, Section 5 provides that the Agreement shall not automatically renew if NERC gives written notice to the Parties, at least 12 months prior to the end of the Term or any Renewal Term, that the Parties should request NERC's approval to renew the Agreement, in which case the Parties shall submit a request to renew the Agreement to NERC at least nine 9 months prior to the end of such Term or Renewal Term. Thus, while obtaining NERC approval is not automatically required for all renewals of the Agreement, this provision gives NERC the ability to step in, by notice given at least 12 months prior to automatic renewal, and require the Parties to make a submission to NERC justifying renewal.

Conforming Agreements to NERC-FRCC and NERC-SPP Delegation Agreements

Exhibit A to each of the current NERC-FRCC and NERC-SPP Delegation Agreements state that SERC performs certain CEA services within the FRCC Region and SPP RE Region, respectively, and references the current SERC-FRCC and SERC-SPP CEA Agreements, respectively. Conforming amendments will need to be made to these provisions in the NERC-FRCC and NERC-SPP Delegation Agreements to reference the renewal CEA Agreements, by date.

**AGREEMENT BETWEEN
SERC RELIABILITY CORPORATION AND
FLORIDA RELIABILITY COORDINATING COUNCIL, INC.
CONCERNING COMPLIANCE MONITORING AND ENFORCEMENT
OF FRCC REGISTERED FUNCTIONS**

THIS AGREEMENT (“Agreement”) made effective as of January 1, 2013 (the “Effective Date”), is entered into between the SERC Reliability Corporation (“SERC”), an organization established to develop and enforce Reliability Standards, and Florida Reliability Coordinating Council, Inc. (“FRCC”), an organization established to develop and enforce Reliability Standards within the geographic boundaries identified on **Exhibit A** to the Amended and Restated Delegation Agreement between the North American Electric Reliability Corporation (“NERC”) and FRCC (referred to herein as the “FRCC Region”), and for other purposes. SERC and FRCC may be individually referred to herein as “Party” or collectively as “Parties.”

RECITALS

I. SERC is a party to a certain Amended and Restated Delegation Agreement with NERC (the “NERC-SERC Delegation Agreement”), which has been approved by the Federal Energy Regulatory Commission (“Commission”) and which states in Section 6 thereof, in pertinent part, that SERC shall enforce Reliability Standards (including Regional Reliability Standards) through a compliance monitoring and enforcement program set forth in Exhibit D to the NERC-SERC Delegation Agreement.

II. FRCC is a party to a certain Amended and Restated Delegation Agreement with NERC (the “NERC-FRCC Delegation Agreement”), which has been approved by the Commission and which states in Section 6 thereof, in pertinent part, that FRCC shall enforce Reliability Standards (including Regional Reliability Standards) within the FRCC Region through a compliance monitoring and enforcement program set forth in Exhibit D to the NERC-FRCC Delegation Agreement.

III. FRCC, through its Member Services Division (“FRCC Member Services Division”), currently performs the Reliability Coordinator (“RC”) and Planning Authority (“PA”)

functions (as “Reliability Coordinator” and “Planning Authority” are defined in the NERC *Glossary of Terms Used in Reliability Standards*) for the FRCC Region, and is registered on the NERC *Compliance Registry* as the RC and a PA for the FRCC Region. In this Agreement, the RC and PA functions are sometimes referred to as the “FRCC Registered Functions,” and FRCC Member Services Division is referred to as the “Registered Entity” with respect to its performance of the FRCC Registered Functions.

IV. To avoid any appearance of a lack of independence in compliance monitoring and enforcement for FRCC Registered Functions, SERC and FRCC hereby agree, subject to approval by NERC and the Commission, that SERC should assume responsibility for the Compliance Monitoring and Enforcement Program (“CMEP”) with respect to the FRCC Registered Functions within the FRCC Region, and that the terms on which responsibility for the CMEP with respect to the FRCC Registered Functions within the FRCC Region shall be performed by SERC should be memorialized in this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants and agreements contained herein, the Parties, intending to be bound, agree as follows:

1. Responsibilities of SERC.

(a) Beginning on the Effective Date, SERC will perform all responsibilities of the Compliance Enforcement Authority (“CEA”) as specified in the NERC uniform CMEP, Appendix 4C to the NERC Rules of Procedure (“ROP”), as amended from time to time (the “NERC Uniform CMEP”), within the FRCC Region with respect to the FRCC Registered Functions.

(b) Without limiting the scope of SERC’s responsibilities as stated in subsection 1(a) of this Agreement, SERC agrees to perform the following activities:

(1) Administer all compliance processes in Section 3.0 of the NERC Uniform CMEP with respect to the FRCC Registered Functions, in accordance with the NERC

Annual CMEP Implementation Plan required by Section 4.1 of the NERC Uniform CMEP for each year. If at any time the FRCC Registered Functions change, SERC will monitor the Registered Functions in effect at that time.

(2) Lead all compliance audits and compliance investigations (“CI”) of the FRCC Registered Functions.

(i) SERC shall conduct a scheduled compliance audit of the FRCC Registered Functions in accordance with the frequency established by NERC in the CMEP. As FRCC is currently registered, SERC will audit the RC function at least once every three (3) years and shall conduct a scheduled compliance audit of the PA function at least once every six (6) years.

(ii) Scheduled compliance audits of the FRCC Registered Functions shall be in accordance with the NERC Annual CMEP Implementation Plan.

(iii) As required by the NERC ROP, all compliance audits of the FRCC RC function shall be conducted on site. Spot checks or other compliance monitoring methods may be completed off site.

(3) Determine if Notice of Possible Violations and Notices of Alleged Violations, as those terms are defined in the CMEP, and proposed penalties or sanctions should be issued to FRCC Member Services Division with respect to the FRCC Registered Functions, and calculate or determine any proposed penalties or sanctions in accordance with the NERC *Sanction Guidelines*.

(4) Administer processes as specified in Section 5.0 of the NERC Uniform CMEP with respect to any Alleged Violations, as that term is defined in the CMEP, and proposed penalties or sanctions issued with respect to the FRCC Registered Functions.

(5) Review and approve proposed Mitigation Plans submitted by a FRCC Registered Function, and monitor implementation and completion of approved Mitigation Plans, in accordance with Section 6.0 of the NERC Uniform CMEP.

(6) Determine if Remedial Action Directives should be issued to FRCC Member Services Division with respect to a FRCC Registered Function, and issue such Remedial Action Directives if determined to be necessary, in accordance with Section 7.0 of the NERC Uniform CMEP.

(7) Conduct settlement negotiations for any violations of Reliability Standards discovered by SERC per this agreement, if requested by FRCC Member Services Division, in accordance with Section 5.4 of the NERC Uniform CMEP.

(8) Provide due process hearings for the FRCC Registered Functions with respect to notices of Alleged Violations, proposed penalties and sanctions, disputed Mitigation Plans, and disputed Remedial Action Directives, as requested by FRCC Member Services Division, in accordance with Attachment 2, Hearing Procedures, to the NERC Uniform CMEP.

(c) Compliance audit teams, CI teams, and review teams for self-certifications, spot check responses, periodic data submittals, self-reports, exception reports and complaints submitted by or relating to a FRCC Registered Function shall not include any employees of FRCC, but may include employees of other Regional Entities, NERC and Commission staff members. Provided, that in accordance with Section 2(c) of this Agreement, SERC may request and obtain technical advice and assistance from FRCC employees, acting in a consulting or advisory capacity, who are not employed in a FRCC Registered Function.

2. Responsibilities of FRCC.

(a) FRCC Member Services Division shall establish and designate to SERC a

primary compliance contact for each FRCC Registered Function, in accordance with Section 2.0 of the NERC Uniform CMEP.

(b) FRCC Member Services Division shall timely respond to and comply with all notices, requests for information and schedules issued by SERC as the CEA pursuant to the NERC Uniform CMEP.

(c) FRCC shall provide subject-matter experts (“SMEs”) as requested by SERC to provide technical advice and assistance to SERC, in SERC’s discretion, in carrying out the CMEP with respect to the FRCC Registered Functions. A SME provided by FRCC may be an employee of FRCC or an industry volunteer, provided, that no SME provided by FRCC may be employed by FRCC in a FRCC Registered Function. The Parties agree that SMEs provided by FRCC shall only be used by SERC in a consulting or advisory capacity to provide expertise and advice on technical matters pertaining to the FRCC Registered Functions, shall have no decision-making responsibilities with respect to any compliance processes or compliance enforcement matters, and shall not be a member of any compliance audit team, CI team, or review team for self-certifications, spot check responses, periodic data submittals, self-reports, exception reports or complaints submitted by or relating to a FRCC Registered Function.

(d) FRCC Regional Entity Division shall reimburse SERC the actual, reasonable costs of SERC’s performance of the CMEP with respect to the FRCC Registered Functions, including an appropriate allocation of SERC’s general and administrative costs, in accordance with Section 4 of this Agreement.

(e) Except as provided in this Agreement, FRCC Regional Entity Division shall continue to perform all CMEP responsibilities in the FRCC Region in accordance with the NERC-FRCC Delegation Agreement.

3. Disposition of Penalties Paid by FRCC with respect to a FRCC Registered Function.

Any penalties to be paid by FRCC Member Services Division for violations of Reliability Standards by a FRCC Registered Function shall be transmitted to NERC, to be used by NERC as a general offset to NERC's budget for its activities as the Electric Reliability Organization under the Federal Power Act for the following year, in accordance with the *NERC Accounting, Financial Statement and Budgetary Treatment of Penalties Imposed and Received for Violations of Reliability Standards*.

4. Compensation to SERC for Performance of CMEP With Respect to the FRCC Registered Functions.

(a) Compensation, In its annual Business Plans and Budgets submitted to NERC and the Commission for years within the term of this Agreement, SERC shall identify a portion of its CMEP budget (the "FRCC Registered Functions CMEP Budget"), including an appropriate allocation of SERC's general and administrative costs, that is attributable to the performance of the CMEP with respect to the FRCC Registered Functions. SERC's allocation of resources to the performance of its obligations under this Agreement and the corresponding budgeted amount shall be subject to approval by NERC and by the Commission as part of their overall approval of SERC's business plan and budget. The amount of SERC's proposed FRCC Registered Functions CMEP Budget shall also be included in FRCC's business plan and budget that is submitted to NERC and to the Commission for approval. The amount of the FRCC Registered Functions CMEP Budget for each year, as approved by the Commission, shall (i) be excluded from the calculation of SERC's assessments to Load-Serving Entities ("LSEs") in the SERC Region for each such year, and (ii) be included in the calculation of FRCC's assessments to LSEs in the FRCC Region for each such year.

(b) Billing SERC will submit an itemized invoice to FRCC on or before the twentieth (20th) day of each month for actual costs (including an appropriate allocation of

SERC's general and administrative costs) incurred during the previous month for work undertaken pursuant to this Agreement. FRCC shall pay SERC within sixty (60) days for the expenses SERC has incurred and for which it has submitted an invoice. SERC shall track the actual costs of the work as it is performed, and should actual costs be on track to exceed budgeted amounts, SERC shall notify the FRCC of this at the next billing cycle.

(c) True-up Reports. The Parties shall record their costs and revenues associated with the performance of this Agreement at the same level of line-item detail as is used for their budgets that are submitted to NERC for approval by NERC and by the Commission. Each Party shall include in its annual true-up report submitted to NERC a separate section showing the Party's actual and budgeted amounts of costs and revenues associated with performance of this Agreement for the year with explanations of variances.

5. Term, Renewal Term, Termination and Early Termination.

(a) Term. The Term of this Agreement shall be from the Effective Date of this Agreement to December 31, 2017.

(b) Renewal Terms. This Agreement shall automatically renew without notice or other action by either Party at the end of the Term specified in (a) or any Renewal Term for a Renewal Term of five (5) years; provided, however, that either Party may give written notice to the other Party at least twelve months prior to the end of the Term specified in (a) of an intent not to renew this Agreement; and provided, further, that during a Renewal Term either Party may terminate this Agreement by providing a written notice to the other Party at least twelve months prior to the desired termination date. Additionally, this Agreement shall not automatically renew if NERC gives written notice to the Parties, at least twelve (12) months prior to the end of the Term or Renewal Term, that the Parties should request NERC's approval to renew the Agreement, in which case the Parties shall submit a request to renew the Agreement to NERC at least nine (9) months prior to the end of such Term or Renewal Term.

In the event of a termination of this Agreement SERC shall continue to perform the CMEP role with respect to the FRCC Registered Functions within the FRCC Region in accordance with the terms of this Agreement and the NERC Uniform CMEP until another entity acceptable to NERC and the Commission is selected to take, and takes, responsibility for performance of the CMEP role with respect to the FRCC Registered Functions. In the event of termination of the Agreement, SERC will work with FRCC to transfer responsibility for any compliance activities in progress to the entity that will be the CEA for the FRCC Member Services Division.

(c) Early Termination. Notwithstanding the provisions of subsections 5(a) and 5(b) of this Agreement, Early Termination of this Agreement shall occur in the following events:

(i) If FRCC or SERC ceases to be a Regional Entity, this Agreement shall terminate as of the end of the calendar year that FRCC or SERC ceases to be a Regional Entity.

(ii) If FRCC ceases to be a Registered Entity in the FRCC Region, this Agreement shall terminate as of the last date that FRCC ceases to be a Registered Entity for any FRCC Registered Function.

(iii) If both Parties agree in writing to terminate this Agreement at any time.

(iv) If any provision of this Agreement, or the application thereof to any person, entity or circumstance, is held by a court or regulatory authority of competent jurisdiction to be invalid, void, or unenforceable, or if a modification or condition to this Agreement is imposed by the Commission, the Parties shall endeavor in good faith to negotiate such amendment or amendments to this Agreement as will restore the relative benefits and obligations of the signatories under this Agreement immediately prior to such holding, modification or condition. If either Party finds such holding, modification or condition unacceptable and the Parties are unable to renegotiate a mutually acceptable

resolution, either Party may unilaterally terminate this Agreement. Such termination shall be effective as of one (1) year following written notice by either Party to the other Party, or at such other time as may be mutually agreed by SERC and FRCC.

(vi) In the event of the Early Termination of this Agreement, SERC will transfer responsibility for completion of all CMEP processes that are in progress as of the date of Early Termination, or within a reasonable time thereafter as mutually agreed to by the Parties, to the entity that will be the CEA for FRCC Member Services Division.

(d) In the event of termination or Early Termination of this Agreement, the costs associated with the wind-down of this Agreement and transfer of any compliance processes in progress to the new CEA are payable by FRCC to SERC in accordance with Section 4 of this Agreement.

6. Representations of the Parties.

(a) Representations of FRCC. FRCC represents and warrants to SERC that (i) FRCC is and shall remain during the term of this Agreement validly existing and in good standing pursuant to all applicable laws relative to this Agreement, (ii) no applicable law, contract or other legal obligation prevents FRCC from executing this Agreement and fulfilling its obligations hereunder, (iii) entry into this Agreement by FRCC is duly authorized under its governing corporate documents, and (iv) the person or persons executing this Agreement on behalf of FRCC are duly authorized to do so.

(b) Representations of SERC. SERC represents and warrants to FRCC that (i) SERC is and shall remain during the term of this Agreement validly existing and in good standing pursuant to all applicable laws relative to this Agreement, (ii) no applicable law, contract or other legal obligation prevents SERC from executing this Agreement and fulfilling its obligations hereunder, (iii) entry into this Agreement by SERC is duly authorized under its

governing corporate documents, and (iv) the person or persons executing this Agreement on behalf of SERC are duly authorized to do so.

7. Limitation of Liability.

SERC and FRCC agree not to sue each other or their directors, officers, employees, and persons serving on their committees and subgroups based on any act or omission of any of the foregoing in the performance of duties pursuant to this Agreement or in conducting activities under the authority of Section 215 of the Federal Power Act, other than seeking a review of such action or inaction by the Commission. SERC and FRCC shall not be liable to one another for any damages whatsoever, other than for non-payment of or failure to remit compensation due pursuant to Section 4 of this Agreement, including without limitation, direct, indirect, incidental, special, multiple, consequential (including attorneys' fees and litigation costs), exemplary, or punitive damages arising out of or resulting from any act or omission associated with the performance of SERC's or FRCC's responsibilities under this Agreement or in conducting activities under the authority of Section 215 of the Federal Power Act, except to the extent that SERC or FRCC is found liable for gross negligence or intentional misconduct, in which case SERC or FRCC shall not be liable for any indirect, incidental, special, multiple, consequential (including without limitation attorneys' fees and litigation costs), exemplary, or punitive damages.

8. No Third Party Beneficiaries.

Nothing in this Agreement shall be construed to create any duty to, any standard of care with reference to, or any liability to any third party.

9. Confidentiality.

During the course of the Parties' performance under this Agreement, a Party may receive Confidential Information, as defined in Section 1500 of the NERC ROP. Except as set forth herein, the Parties agree to keep in confidence and not to copy, disclose, or distribute any

Confidential Information or any part thereof, without the prior written permission of the issuing Party, unless disclosure is required by subpoena, law, or other directive of a court, administrative agency, or arbitration panel, in which event the recipient hereby agrees to provide the Party that provided the Confidential Information with prompt notice of such request or requirement in order to enable such issuing Party to (a) seek an appropriate protective order or other remedy, (b) consult with the recipient with respect to taking steps to resist or narrow the scope of such request or legal process, or (c) waive compliance, in whole or in part, with the terms of this Section 9. In the event a protective order or other remedy is not obtained or the issuing Party waives compliance with the provisions, the recipient agrees to furnish only that portion of the Confidential Information which the recipient's counsel advises is legally required and to exercise best efforts to obtain assurance that confidential treatment will be accorded to such Confidential Information. In addition, each Party shall ensure that its officers, trustees, directors, employees, subcontractors and subcontractors' employees, and agents to whom Confidential Information is exposed are under obligations of confidentiality that are at least as restrictive as those contained herein. This confidentiality provision does not prohibit reporting and disclosure by SERC, as the CEA with respect to the FRCC Registered Functions, in accordance with Section 8.0 and other provisions of the NERC Uniform CMEP.

10. Amendment.

Neither this Agreement nor any of the terms hereof, may be amended unless such amendment is made in writing and signed by the Parties.

11. Dispute Resolution.

In the event a dispute arises under this Agreement between SERC and FRCC, representatives of the Parties with authority to settle the dispute shall meet and confer in good faith in an effort to resolve the dispute in a timely manner. In the event the designated representatives are unable to resolve the dispute within thirty (30) days or such other period as

the Parties may agree upon, each Party shall have all rights to pursue all remedies, except as expressly limited by the terms of this Agreement. Neither Party shall have the right to pursue other remedies until the Dispute Resolution procedures of this Section 11 have been exhausted. This Section 11 shall not apply to enforcement actions or Remedial Action Directives by SERC, as the CEA, against a FRCC Registered Function, or hearings conducted at the request of FRCC as the Registered Entity for a FRCC Registered Function, pursuant to the NERC Uniform CMEP.

12. Notices.

Whether expressly so stated or not, all notices, demands, requests, and other communications required or permitted by or provided for in this Agreement shall be given in writing to a Party at the address set forth below, or at such other address as a Party shall designate for itself in writing in accordance with this Section, and shall be delivered by hand or reputable overnight courier:

If to SERC:

SERC Reliability Corporation
2815 Coliseum Centre Drive
Suite 500
Charlotte, NC 28217

Attn: Marisa Sifontes
Facsimile: 704-357-7914

If to FRCC:

Florida Reliability Coordinating Council
1408 N Westshore Blvd
Suite 1002
Tampa, FL 33607

Attn: Reva Maskewitz
Facsimile: 813-289-5646

Provided, that the foregoing notice provision shall not be applicable to notices and other communications between SERC, as the CEA, and FRCC as the Registered Entity for a FRCC Registered Function, which notices and other communications shall instead be provided or transmitted in accordance with the NERC Uniform CMEP.

13. Governing Law.

When not in conflict with or preempted by federal law, this Agreement will be governed

by and construed in accordance with the laws of Delaware without giving effect to the conflict of law principles thereof. The Parties recognize and agree not to contest the exclusive or primary jurisdiction of the Commission to interpret and apply this Agreement; provided however, that if the Commission declines to exercise or is precluded from exercising jurisdiction of any action arising out of or concerning this Agreement, such action shall be brought in any state or federal court of competent jurisdiction in Delaware. All Parties hereby consent to the jurisdiction of any state or federal court of competent jurisdiction in Delaware for the purpose of hearing and determining any action not heard and determined by the Commission.

14. Headings.

The headings and captions in this Agreement are for convenience of reference only and shall not define, limit, or otherwise affect any of the terms or provisions hereof.

15. Entire Agreement.

This Agreement constitutes the entire agreement, and supersedes all prior agreements and understandings, both written and oral, among the Parties with respect to the subject matter of this Agreement.

16. Execution of Counterparts.

This Agreement may be executed in counterparts and each counterpart shall have the same force and effect as the original.

NOW, THEREFORE, the Parties have caused this Agreement to be executed by their duly authorized representatives, to be effective as of the Effective Date.

SERC RELIABILITY CORPORATION

FLORIDA RELIABILITY
COORDINATING COUNCIL

By: _____ By: _____

Name: R. Scott Henry

Name: Sarah Rogers

Title: President and CEO

Title: President and CEO

Date: _____ Date: _____

**AGREEMENT BETWEEN
SERC RELIABILITY CORPORATION ~~and~~AND
FLORIDA RELIABILITY COORDINATING COUNCIL , INC.
CONCERNING COMPLIANCE MONITORING AND ENFORCEMENT
OF FRCC REGISTERED FUNCTIONS**

THIS AGREEMENT ("Agreement") made effective as of ~~July 12, 2010~~ January 1, 2013 (the "Effective Date"), is entered into between the SERC Reliability Corporation ("SERC"), an organization established to develop and enforce Reliability Standards, and Florida Reliability Coordinating Council , Inc. ("FRCC"), an organization established to develop and enforce Reliability Standards within the geographic boundaries identified on **Exhibit A** to the "Amended and Restated Delegation Agreement ~~B~~etween the North American Electric Reliability Corporation ("NERC") and FRCC ~~Florida Reliability Coordinating Council, Inc."~~ (referred to herein as the "FRCC Region"), and for other purposes. SERC and FRCC may be individually referred to herein as "Party" or collectively as "Parties."

RECITALS

I. SERC is a party to a certain "Amended and Restated Delegation Agreement ~~Between the North American Electric Reliability Corporation~~ with NERC ~~and SERC Reliability Corporation"~~ (the "NERC-SERC Delegation Agreement"), which has been approved by the Federal Energy Regulatory Commission ("Commission") and which states in Section 6 thereof, in pertinent part, that SERC shall enforce Reliability Standards (including Regional Reliability Standards) through a compliance monitoring and enforcement program set forth in Exhibit D to the NERC-SERC Delegation Agreement.

II. FRCC is a party to a certain "Amended and Restated Delegation Agreement ~~Between~~ with NERC ~~the North American Electric Reliability Corporation and Florida Reliability Coordinating Council, Inc."~~ (the "NERC-FRCC Delegation Agreement"), which has been approved by the Commission and which states in Section 6 thereof, in pertinent part, that FRCC shall enforce Reliability Standards (including Regional Reliability Standards) within the FRCC Region through a compliance monitoring and enforcement program set forth in Exhibit D to

the NERC-FRCC Delegation Agreement.

III. FRCC, through its Member Services Division (“FRCC Member Services Division”), currently performs the Reliability Coordinator (“RC”) and Planning Authority (“PA”) functions (as “Reliability Coordinator” and “Planning Authority” are defined in the NERC *Glossary of Terms Used in Reliability Standards*) for the FRCC Region, and is registered on the NERC *Compliance Registry* as the RC and a PA for the FRCC Region. In this Agreement, the RC and PA functions are sometimes referred to as the “FRCC Registered Functions,” and FRCC Member Services Division is referred to as the “Registered Entity” with respect to its performance of the FRCC Registered Functions.

~~IV. To avoid any appearance of a lack of independence in compliance monitoring and enforcement for FRCC Registered Functions, SERC and FRCC hereby Notwithstanding the provisions of Section 6 of the NERC-FRCC Delegation Agreement, the Commission has ruled that FRCC’s performance of compliance monitoring and enforcement functions with respect to compliance with Reliability Standards by FRCC’s registered reliability functions results in a lack of independence in compliance monitoring and enforcement for FRCC operational functions. The Commission therefore directed NERC and FRCC to remedy this deficiency. In light of the Commission’s directive, SERC and FRCC agree, subject to approval by NERC and the Commission, that SERC should assume responsibility for the Compliance Monitoring and Enforcement Program (“CMEP”) with respect to the FRCC Registered Functions within the FRCC Region, and that the terms on which responsibility for the CMEP with respect to the FRCC Registered Functions within the FRCC Region shall be ~~transferred to and~~ performed by SERC should be memorialized in this Agreement.~~

NOW, THEREFORE, in consideration of the mutual covenants and agreements contained herein, the Parties, intending to be bound, agree as follows:

1. Responsibilities of SERC.

(a) Beginning on the Effective Date, SERC will perform all responsibilities of the Compliance Enforcement Authority (“CEA”) as specified in the NERC uniform CMEP, Appendix 4C to the NERC Rules of Procedure (“ROP”), as amended from time to time (the “NERC Uniform CMEP”), within the FRCC Region with respect to the FRCC Registered Functions.

(b) Without limiting the scope of SERC’s responsibilities as stated in ~~S~~subsection 1(a) of this Agreement, SERC agrees to perform the following activities:

(1) Administer all compliance processes in Section 3.0 of the NERC Uniform CMEP with respect to the FRCC Registered Functions, in accordance with the NERC Annual CMEP Implementation Plan required by Section 4.1 of the NERC Uniform CMEP for each year. ~~If at any time, the FRCC’s registration status~~ Registered Functions changes, SERC will monitor ~~the~~ Registered Functions in effect at that time.

(2) Lead all compliance audits and compliance ~~violation~~ investigations (“CVI”) of the FRCC Registered Functions.

(i) SERC shall conduct a scheduled compliance audit of the FRCC Registered Functions in accordance with the frequency established by NERC in the CMEP. As FRCC is currently registered, SERC will audit the RC function at least once every three (3) years and shall conduct a scheduled compliance audit of the PA function, at least once every six (6) years.

(ii) Scheduled compliance audits of the FRCC Registered Functions ~~shall be~~ ~~shall include all actively-monitored standards~~ in accordance with the NERC Annual CMEP Implementation Plan.

(iii) As required by the NERC ROP, all compliance audits of the FRCC RC function shall be conducted on site. ~~Spot checks or other compliance monitoring methods may be completed off site.~~

(3) Determine if Notice of Possible Violations and ~~n~~Notices of Alleged Violations, as those terms are defined in the CMEP, and proposed penalties or

sanctions should be issued to FRCC Member Services Division with respect to the FRCC Registered Functions, and calculate or determine any proposed penalties or sanctions in accordance with the NERC *Sanction Guidelines*.

(4) Administer processes as specified in Section 5.0 of the NERC Uniform CMEP with respect to any ~~notices of~~ Alleged Violations, [as that term is defined in the CMEP](#), and proposed penalties or sanctions issued with respect to the FRCC Registered Functions.

(5) Review and approve proposed Mitigation Plans submitted by a FRCC Registered Function, and monitor implementation and completion of approved Mitigation Plans, in accordance with Section 6.0 of the NERC Uniform CMEP.

(6) Determine if Remedial Action Directives should be issued to FRCC Member Services Division with respect to a FRCC Registered Function, and issue such Remedial Action Directives if determined to be necessary, in accordance with Section 7.0 of the NERC Uniform CMEP.

(7) Conduct settlement negotiations for any violations of Reliability Standards discovered by SERC per this agreement, if requested by FRCC Member Services Division, in accordance with Section 5.4 of the NERC Uniform CMEP.

(8) Provide due process hearings for the FRCC Registered Functions with respect to notices of Alleged Violations, proposed penalties and sanctions, disputed Mitigation Plans, and disputed Remedial Action Directives, as requested by FRCC Member Services Division, in accordance with Attachment 2, Hearing Procedures, to the NERC Uniform CMEP.

(c) Compliance audit teams, ~~CVICI~~ teams, and review teams for self-certifications, spot_check responses, periodic data submittals, self-reports, exception reports and complaints_submitted by or relating to a FRCC Registered Function shall not include any employees of FRCC, but may include employees of other Regional Entities, NERC and Commission staff_members. Provided, that in accordance with Section 2(c) of this

Agreement, SERC may request and obtain technical advice and assistance from FRCC employees, acting in a consulting or advisory capacity, who are not employed in a FRCC Registered Function.

2. Responsibilities of FRCC.

(a) ~~As the Registered Entity for the FRCC Registered Functions,~~ FRCC Member Services Division shall establish and designate to SERC a primary compliance contact for each FRCC Registered Function, in accordance with Section 2.0 of the NERC Uniform CMEP.

(b) ~~As the Registered Entity for the FRCC Registered Functions,~~ FRCC Member Services Division shall timely respond to and comply with all notices, requests for information and schedules issued by SERC as the CEA pursuant to the NERC Uniform CMEP.

(c) FRCC shall provide subject-matter experts (“SMEs”) as requested by SERC to provide technical advice and assistance to SERC, in SERC’s discretion, in carrying out the CMEP with respect to the FRCC Registered Functions. A SME provided by FRCC may be an employee of FRCC or an industry volunteer, provided, that no SME provided by FRCC may be employed by FRCC in a FRCC Registered Function. The Parties agree that SMEs provided by FRCC shall only be used by SERC in a consulting or advisory capacity to provide expertise and advice on technical matters pertaining to the FRCC Registered Functions, shall have no decision-making responsibilities with respect to any compliance processes or compliance enforcement matters, and shall not be a member of any compliance audit team, ~~CVI~~ team, or review team for self-certifications, spot check responses, periodic data submittals, self-reports, exception reports or complaints submitted by or relating to a FRCC Registered Function.

(d) FRCC Regional Entity Division shall reimburse SERC the actual, reasonable costs of SERC’s performance of the CMEP with respect to the FRCC Registered Functions, including an appropriate allocation of SERC’s ~~G~~general and ~~A~~administrative costs, in

accordance with Section 54 of this Agreement.

(e) Except as provided in this Agreement, FRCC Regional Entity Division shall continue to perform all CMEP responsibilities in the FRCC Region in accordance with the NERC-FRCC Delegation Agreement.

3. Disposition of Penalties Paid by FRCC with respect to a FRCC Registered Function.

Any penalties to be paid by FRCC Member Services Division for violations of Reliability Standards by a FRCC Registered Function, shall be transmitted to NERC, to be used by NERC as a general offset to NERC's budget for its activities as the Electric Reliability Organization under the Federal Power Act for the following year, in accordance with the *NERC Accounting, Financial Statement and Budgetary Treatment of Penalties Imposed and Received for Violations of Reliability Standards*.

~~**4. Transfer of Responsibilities for CMEP Activities With Respect To FRCC Registered Functions That Are In Progress on the Effective Date.**~~

~~SERC shall assume full responsibility, as the CEA, for completion of all compliance processes with respect to the FRCC Registered Functions that are in progress as of the Effective Date, including without limiting the foregoing, (i) completion and issuance of reports of compliance audits and CVI of the FRCC Registered Functions, (ii) completion of review of, and issuance of any findings or reports concerning, any self-certifications, spot-checks, periodic data submittals, self-reports, exception reports or complaints, submitted by or pertaining to a FRCC Registered Function, (iii) determination of whether any notice of Alleged Violations and/or proposed penalties or sanctions should be issued to a FRCC Registered Function as a result of any such compliance processes, (iv) processing of any notices of Alleged Violations and/or proposed penalties or sanctions that were issued before the Effective Date, or are issued after the Effective Date as the result of compliance processes conducted before the Effective Date,~~

~~and (v) review, approval and monitoring of implementation and completion of any Mitigation Plans required of a FRCC Registered Function as the result of compliance processes conducted before the Effective Date.~~

~~4.~~ **5. Compensation to SERC for Performance of CMEP With Respect to the FRCC Registered Functions.**

~~_____ Compensation for 2010.~~

~~For the period between the Effective Date of this Agreement and December 31, 2010, SERC shall invoice FRCC the amount of \$5000 per quarter (pro-rated for any partial quarter) on or about the first day of each calendar quarter. The first invoice shall also include the amount for the partial quarter, if any between the Effective Date and the date of the first invoice. FRCC shall remit to SERC the amount of each invoice by check or electronic funds transfer to SERC within twenty (20) business days following the date of each invoice.~~

~~(a) Compensation for Years Subsequent to 2010.~~

~~(a) _____ Compensation. (f)~~—In its annual Business Plans and Budgets submitted to NERC and the Commission for ~~the year 2011 and subsequent~~ years within the term of this Agreement, SERC shall identify a portion of its CMEP budget (the “FRCC Registered Functions CMEP Budget”), including an appropriate allocation of SERC’s General and Aadministrative Ccosts ~~the “FRCC Registered Functions CMEP Budget”~~, that is attributable to the performance of the CMEP with respect to the FRCC Registered Functions. SERC’s allocation of resources to the performance of its obligations under this Agreement and the corresponding budgeted amount shall be subject to approval by NERC and by the Commission as part of their overall approval of SERC’s business plan and budget. The amount of SERC’s proposed FRCC Registered Functions CMEP Budget shall also be included in FRCC’s business plan and budget that is submitted to NERC and to the Commission for approval. The amount of

the FRCC Registered Functions CMEP Budget for each year, as approved by the Commission, ~~shall~~ (i) ~~shall~~ be excluded from the calculation of SERC's assessments to Load-Serving Entities ("LSEs") in the SERC Region for each such year, and (ii) ~~shall~~ be included in the calculation of FRCC's assessments to LSEs in the FRCC Region for each such year.

~~(b) Billing. SERC shall invoice FRCC Regional Entity Division for the amount of the FRCC Registered Functions CMEP Budget in four equal quarterly amounts during each year, with the invoices to be issued by SERC to FRCC on or about January 1, April 1, July 1 and October 1 and to be paid by FRCC by check or electronic funds transfer to SERC within twenty (20) business days following the date of the invoice.~~

~~(c) Reconciliation of Costs.~~

~~No later than 90 days after the end of a budget year, SERC shall provide to FRCC a statement of actual expenses incurred by SERC in the fulfillment of SERC's responsibilities under this agreement for that budget year. The statement shall disclose the actual costs of labor, travel and meetings, and all other direct costs, as well as SERC's allocation of its actual General and Administrative Costs. The statement shall summarize the reasons for any variances as compared to the budget amount. SERC shall provide supporting documentation for the final statement upon request by FRCC. The total variance for the concluded budget year shall be incorporated as a compensating adjustment in both the SERC and FRCC budgets in the second year following the budget year and, as approved by NERC and the Commission, reflected in the quarterly invoices from SERC to FRCC and quarterly payments by FRCC to SERC in such year.~~

~~(d) Supplemental Invoice.~~

~~If during any budget year, including 2010, the actual cost of performing SERC's responsibilities under this agreement exceeds the budgeted funding by more than ten (10)~~

~~percent of SERC's budgeted cash reserve (for example as may be necessitated by the conduct of a compliance violation investigation or hearing), SERC shall have the right to issue supplemental invoices to FRCC to recover in full all actual costs incurred above the budgeted funding. Upon receipt of such a supplemental invoice, FRCC shall pay the full amount of the invoice by check or electronic funds transfer to SERC within sixty (60) days. SERC will submit an itemized invoice to FRCC on or before the twentieth (20th) day of each month for actual costs (including an appropriate allocation of SERC's general and administrative costs) incurred during the previous month for work undertaken pursuant to this Agreement. FRCC shall pay SERC within sixty (60) days for the expenses SERC has incurred and for which it has submitted an invoice. SERC shall track the actual costs of the work as it is performed, and should actual costs be on track to exceed budgeted amounts, SERC shall notify the FRCC of this at the next billing cycle.~~

(c) True-up Reports. The Parties shall record their costs and revenues associated with the performance of this Agreement at the same level of line-item detail as is used for their budgets that are submitted to NERC for approval by NERC and by the Commission. Each Party shall include in its annual true-up report submitted to NERC a separate section showing the Party's actual and budgeted amounts of costs and revenues associated with performance of this Agreement for the year with explanations of variances.

6.5. Term, Renewal Term, Termination and Early Termination.

(a) ~~Initial Term.~~ The ~~Initial~~ Term of this Agreement shall be from the Effective Date of this Agreement to December 31, 2017~~2~~.

(b) Renewal Terms. This Agreement shall ~~not automatically~~ renew without notice or other action by either Party at the end of the ~~Initial~~ Term specified in (a) or any Renewal Term for a Renewal Term of five (5) years; provided, however, that either Party may give written notice to the other Party at least twelve months prior to the end of the Term specified in (a) of an intent not to renew this Agreement; and provided, further, that during a

Renewal Term either Party may terminate this Agreement by providing a written notice to the other Party at least twelve months prior to the desired termination date. Additionally, this Agreement shall not automatically renew if NERC gives written notice to the Parties, at least twelve (12) months prior to the end of the Term or Renewal Term, that the Parties should request NERC's approval to renew the Agreement, in which case the Parties shall submit a request to renew the Agreement to NERC at least nine (9) months prior to the end of such Term or Renewal Term. In the event of a termination of this Agreement SERC shall continue to perform the CMEP role with respect to the FRCC Registered Functions within the FRCC Region in accordance with the terms of this Agreement and the NERC Uniform CMEP until another entity acceptable to NERC and the Commission is selected to take, and takes, responsibility for performance of the CMEP role with respect to the FRCC Registered Functions, ~~without the express approval of NERC and the Commission. If either Party does not plan to seek approval for renewal of the agreement, that Party must give written notice to the other Party and NERC, at least one (1) year prior to the end of the Initial Term. In the event the Parties intend to renew the Agreement, they shall make a joint filing to NERC not later than April 1, 2012 requesting approval of the renewal.~~ In the event of termination of the Agreement, SERC will work with FRCC to transfer responsibility for any compliance activities in progress to the entity that will be the CEA for the FRCC Member Services Division.

(c) Early Termination. Notwithstanding the provisions of subsections ~~65~~(a) and ~~65~~(b) of this Agreement, Early Termination of this Agreement shall occur in the following events:

(i) If FRCC or SERC ceases to be a Regional Entity, this Agreement shall terminate as of the end of the calendar year that FRCC or SERC ceases to be a Regional Entity.

(ii) If FRCC ceases to be a Registered Entity in the FRCC Region, this Agreement shall terminate as of the last date that FRCC ceases to be a Registered

Entity for any FRCC Registered Function.

(iii) If both ~~p~~Parties agree in writing to terminate this Agreement at any time.

(iv) If any provision of this Agreement, or the application thereof to any person, entity or circumstance, is held by a court or regulatory authority of competent jurisdiction to be invalid, void, or unenforceable, or if a modification or condition to this Agreement is imposed by the Commission, the Parties shall endeavor in good faith to negotiate such amendment or amendments to this Agreement as will restore the relative benefits and obligations of the signatories under this Agreement immediately prior to such holding, modification or condition. If either Party finds such holding, modification or condition unacceptable and the Parties are unable to renegotiate a mutually acceptable resolution, either Party may unilaterally terminate this Agreement. Such termination shall be effective as of one (1) year following written notice by either Party to the other Party, or at such other time as may be mutually agreed by SERC and FRCC.

(vi) ~~_____ Provided, that i~~n the event of the Early termination of this Agreement, SERC will transfer responsibility for completion of all CMEP compliance processes that are in progress as of the date of Early Termination, or within a reasonable time thereafter as mutually agreed to by the ~~p~~Parties, to the entity that will be the CEA for FRCC Member Services Division.

(d) In the event of termination or Early Termination of this Agreement, the costs associated with the wind-down of this Agreement and transfer of any compliance processes in progress to the new CEA are payable by FRCC to SERC in accordance with Section 4~~5~~ of this Agreement.

~~6.~~ **7. Representations of the Parties.**

(a) Representations of FRCC. FRCC represents and warrants to SERC that (i) FRCC is and shall remain during the term of this Agreement validly existing and in good standing pursuant to all applicable laws relative to this Agreement, (ii) no applicable law, contract or other legal obligation prevents FRCC from executing this Agreement and fulfilling its obligations hereunder, (iii) entry into this Agreement by FRCC is duly authorized under its governing corporate documents, and (iv) the person or persons executing this Agreement on behalf of FRCC are duly authorized to do so.

(b) Representations of SERC. SERC represents and warrants to FRCC that (i) SERC is and shall remain during the term of this Agreement validly existing and in good standing pursuant to all applicable laws relative to this Agreement, (ii) no applicable law, contract or other legal obligation prevents SERC from executing this Agreement and fulfilling its obligations hereunder, (iii) entry into this Agreement by SERC is duly authorized under its governing corporate documents, and (iv) the person or persons executing this Agreement on behalf of SERC are duly authorized to do so.

~~8.7.~~ **Limitation of Liability.**

SERC and FRCC agree not to sue each other or their directors, officers, employees, and persons serving on their committees and subgroups based on any act or omission of any of the foregoing in the performance of duties pursuant to this Agreement or in conducting activities under the authority of Section 215 of the Federal Power Act, other than seeking a review of such action or inaction by the Commission. SERC and FRCC shall not be liable to one another for any damages whatsoever, other than for non-payment of or failure to remit compensation due pursuant to Section ~~45~~ of this Agreement, including without limitation, direct, indirect, incidental, special, multiple, consequential (including attorneys' fees and litigation

costs), exemplary, or punitive damages arising out of or resulting from any act or omission associated with the performance of SERC's or FRCC's responsibilities under this Agreement or in conducting activities under the authority of Section 215 of the [Federal Power Act](#), except to the extent that SERC or FRCC is found liable for gross negligence or intentional misconduct, in which case SERC or FRCC shall not be liable for any indirect, incidental, special, multiple, consequential (including without limitation attorneys' fees and litigation costs), exemplary, or punitive damages.

9-8. No Third Party Beneficiaries.

Nothing in this Agreement shall be construed to create any duty to, any standard of care with reference to, or any liability to any third party.

10-9. Confidentiality.

During the course of the Parties' performance under this Agreement, a Party may receive Confidential Information, as defined in Section 1500 of the NERC ROP. Except as set forth herein, the Parties agree to keep in confidence and not to copy, disclose, or distribute any Confidential Information or any part thereof, without the prior written permission of the issuing Party, unless disclosure is required by subpoena, law, or other directive of a court, administrative agency, or arbitration panel, in which event the recipient hereby agrees to provide the Party that provided the Confidential Information with prompt notice of such request or requirement in order to enable such issuing Party to (a) seek an appropriate protective order or other remedy, (b) consult with the recipient with respect to taking steps to resist or narrow the scope of such request or legal process, or (c) waive compliance, in whole or in part, with the terms of this Section 910. In the event a protective order or other remedy is not obtained or the issuing Party waives compliance with the provisions, the recipient agrees to furnish only that portion of the Confidential Information which the recipient's counsel advises is legally required

and to exercise best efforts to obtain assurance that confidential treatment will be accorded to such Confidential Information. In addition, each Party shall ensure that its officers, trustees, directors, employees, subcontractors and subcontractors' employees, and agents to whom Confidential Information is exposed are under obligations of confidentiality that are at least as restrictive as those contained herein. This confidentiality provision does not prohibit reporting and disclosure by SERC, as the CEA with respect to the FRCC Registered Functions, in accordance with Section 8.0 and other provisions of the NERC Uniform CMEP.

~~4.10.~~ 10. **Amendment.**

Neither this Agreement nor any of the terms hereof, may be amended unless such amendment is made in writing and signed by the Parties.

~~12.11.~~ 11. **Dispute Resolution.**

In the event a dispute arises under this Agreement between SERC and FRCC, representatives of the Parties with authority to settle the dispute shall meet and confer in good faith in an effort to resolve the dispute in a timely manner. In the event the designated representatives are unable to resolve the dispute within thirty (30) days or such other period as the Parties may agree upon, each Party shall have all rights to pursue all remedies, except as expressly limited by the terms of this Agreement. Neither Party shall have the right to pursue other remedies until the Dispute Resolution procedures of this Section ~~112~~ have been exhausted. This Section ~~112~~ shall not apply to enforcement actions or Remedial Action Directives by SERC, as the CEA, against a FRCC Registered Function, or hearings conducted at the request of FRCC as the Registered Entity for a FRCC Registered Function, pursuant to the NERC Uniform CMEP.

12. ~~13.~~ Notices.

Whether expressly so stated or not, all notices, demands, requests, and other communications required or permitted by or provided for in this Agreement shall be given in writing to a Party at the address set forth below, or at such other address as a Party shall designate for itself in writing in accordance with this Section, and shall be delivered by hand or reputable overnight courier:

If to SERC:

SERC Reliability Corporation
2815 Coliseum Centre Drive
Suite 500
Charlotte, NC 28217

Attn: Marisa Sifontes
Facsimile: 704-357-7914

If to FRCC:

Florida Reliability Coordinating Council
1408 N Westshore Blvd
Suite 1002
Tampa, FL 33607

Attn: Reva Maskewitz
Facsimile: 813-289-5646

Provided, that the foregoing notice provision shall not be applicable to notices and other communications between SERC, as the CEA, and FRCC as the Registered Entity for a FRCC Registered Function, which notices and other communications shall instead be provided or transmitted in accordance with the NERC Uniform CMEP.

14.13. Governing Law.

When not in conflict with or preempted by federal law, this Agreement will be governed by and construed in accordance with the laws of Delaware without giving effect to the conflict of law principles thereof. The Parties recognize and agree not to contest the exclusive or primary jurisdiction of the Commission to interpret and apply this Agreement; provided however, that if the Commission declines to exercise or is precluded from exercising jurisdiction of any action arising out of or concerning this Agreement, such action shall be brought in any state or federal court of competent jurisdiction in Delaware. All Parties hereby consent to the jurisdiction of any state or federal court of competent jurisdiction in Delaware for the purpose of hearing and

determining any action not heard and determined by the Commission.

15.14. Headings.

The headings and captions in this Agreement are for convenience of reference only and shall not define, limit, or otherwise affect any of the terms or provisions hereof.

16.15. Entire Agreement.

This Agreement constitutes the entire agreement, and supersedes all prior agreements and understandings, both written and oral, among the Parties with respect to the subject matter of this Agreement.

17.16. Execution of Counterparts.

This Agreement may be executed in counterparts and each counterpart shall have the same force and effect as the original.

NOW, THEREFORE, the Parties have caused this Agreement to be executed by their duly authorized representatives, to be effective as of the Effective Date.

SERC RELIABILITY CORPORATION

FLORIDA RELIABILITY
COORDINATING COUNCIL

By: _____

By: _____

Name: R. Scott Henry

Name: Sarah Rogers

Title: President and CEO

Title: President and CEO

Date: _____

Date: _____

**AGREEMENT BETWEEN
SERC RELIABILITY CORPORATION AND
SOUTHWEST POWER POOL REGIONAL ENTITY
CONCERNING COMPLIANCE MONITORING AND ENFORCEMENT
OF SOUTHWEST POWER POOL, INC. REGISTERED FUNCTIONS**

THIS AGREEMENT (“Agreement”) made effective as of _____ (the “Effective Date”), between the SERC Reliability Corporation (“SERC”), an organization established to develop and enforce Reliability Standards, and Southwest Power Pool Regional Entity (“SPP RE”) a division of Southwest Power Pool, Inc. (“SPP”), an organization established to develop and enforce Reliability Standards within the geographic boundaries identified on Exhibit A (referred to herein as the “SPP RE Region”) to the “Amended and Restated Delegation Agreement between the North American Electric Reliability Corporation (“NERC”) and “SPP”, and for other purposes. SERC and the SPP RE may be individually referred to herein as “Party” or collectively as “Parties”.

RECITALS

I. SERC is a party to a certain “Amended and Restated Delegation Agreement between NERC and SERC” (the “NERC-SERC Delegation Agreement”), which has been approved by the Federal Energy Regulatory Commission (“Commission”) and which states in Section 6 thereof, in pertinent part, that SERC shall enforce Reliability Standards (including Regional Reliability Standards) through a compliance monitoring and enforcement program set forth in Exhibit D to the NERC-SERC Delegation Agreement.

II. SPP is a party to a certain “Amended and Restated Delegation Agreement between NERC and SPP (the “NERC-SPP Delegation Agreement”), which has been approved by the Commission and which states in Section 6 thereof, in pertinent part, that the SPP RE shall enforce Reliability Standards (including Regional Reliability Standards) within the geographic boundaries set forth in Exhibit A to the NERC-SPP Delegation Agreement through a

compliance monitoring and enforcement program set forth in Exhibit D to the NERC-SPP Delegation Agreement.

III. SPP serves as a Regional Transmission Organization and is currently registered as an Interchange Authority (“IA”), Planning Authority (“PA”), Reliability Coordinator (“RC”), Reserve Sharing Group (“RSG”), Transmission Planner (“TP”), and Transmission Service Provider (“TSP”) in the SPP RE Region. In this Agreement, the IA, PA, RC, RSG, TP and TSP functions are sometimes referred to as the “SPP Registered Functions”, and SPP is referred to as the “Registered Entity” with respect to its performance of the SPP Registered Functions.

IV. To avoid any appearance of a lack of independence in compliance monitoring and enforcement for SPP Registered Functions, SERC and the SPP RE hereby agree, subject to approval by NERC and by the Commission, that SERC should assume responsibility for the Compliance Monitoring and Enforcement Program (“CMEP”) with respect to the SPP Registered Functions within the SPP RE Region, and that the terms on which responsibility for the CMEP with respect to the SPP Registered Functions within the SPP RE Region shall be performed by SERC should be memorialized in this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants and agreements contained herein, the Parties, intending to be bound, agree as follows:

1. Responsibilities of SERC.

(a) Beginning on the Effective Date, SERC will perform all responsibilities of the Compliance Enforcement Authority (“CEA”) as specified in the NERC uniform CMEP, Appendix 4C to the NERC Rules of Procedure (“ROP”), as amended from time to time (the “NERC Uniform CMEP”), within the SPP RE Region with respect to the SPP Registered Functions.

(b) Without limiting the scope of SERC’s responsibilities as stated in subsection 1(a) of this Agreement, SERC agrees to perform the following activities within the SPP RE Region:

(1) Administer all compliance processes in Section 3.0 of the NERC Uniform CMEP with respect to the SPP Registered Functions, in accordance with the NERC

Annual CMEP Implementation Plan required by Section 4.1 of the NERC Uniform CMEP for each year. If at any time SPP Registered Functions change, SERC will monitor the Registered Functions in effect at that time.

(2) Lead all compliance audits and compliance investigations (“CI”) of the SPP Registered Functions.

(i) SERC shall conduct a scheduled compliance audit of the SPP Registered Functions in accordance with the frequency established by NERC in the CMEP. As SPP is currently registered, SERC will audit the RC function at least once every three (3) years and shall conduct a scheduled compliance audit of the remaining functions at least once every six (6) years.

(ii) Scheduled compliance audits of the SPP Registered Functions shall be in accordance with the NERC Annual CMEP Implementation Plan.

(iii) As required by the NERC ROP, all compliance audits of the SPP RC function shall be conducted on site. Spot checks or other compliance monitoring methods may be completed off site.

(3) Determine if Notices of Possible Violations and Notices of Alleged Violations, as those terms are defined in the CMEP, and proposed penalties or sanctions should be issued to SPP with respect to the SPP Registered Functions, and calculate or determine any proposed penalties or sanctions in accordance with the NERC *Sanction Guidelines*.

(4) Administer processes as specified in Section 5.0 of the NERC Uniform CMEP with respect to any Alleged Violations, as that term is defined in the CMEP, and proposed penalties or sanctions issued with respect to the SPP Registered Functions.

(5) Review and approve proposed Mitigation Plans submitted by an SPP Registered Function, and monitor implementation and completion of approved Mitigation Plans, in accordance with Section 6.0 of the NERC Uniform CMEP.

(6) Determine if Remedial Action Directives should be issued to SPP with respect to an SPP Registered Function, and issue such Remedial Action Directives if determined to be necessary, in accordance with Section 7.0 of the NERC Uniform CMEP.

(7) Conduct settlement negotiations for any violations of Reliability Standards discovered by SERC per this agreement, if requested by SPP, in accordance with Section 5.4 of the NERC Uniform CMEP.

(8) Provide due process hearings for the SPP Registered Functions with respect to notices of Alleged Violations, proposed penalties and sanctions, disputed Mitigation Plans, and disputed Remedial Action Directives, as requested by SPP, in accordance with Attachment 2, Hearing Procedures, to the NERC Uniform CMEP.

(c) Compliance audit teams, CI teams, and review teams for self-certifications, spot check responses, periodic data submittals, self-reports, exception reports and complaints submitted by or relating to an SPP Registered Function shall not include any employees of SPP, but may include employees of other Regional Entities, NERC and Commission staff members. Provided, that in accordance with Section 2(c) of this Agreement, SERC may request and obtain technical advice and assistance from SPP employees, acting in a consulting or advisory capacity, who are not employed in an SPP Registered Function.

2. Responsibilities of SPP.

(a) SPP shall establish and designate to SERC a primary compliance contact for each SPP Registered Function, in accordance with Section 2.0 of the NERC Uniform CMEP.

(b) SPP shall timely respond to and comply with all notices, requests for information and schedules issued by SERC as the CEA pursuant to the NERC Uniform CMEP.

(c) The SPP RE shall provide subject-matter experts (“SMEs”) as requested by SERC to provide technical advice and assistance to SERC, in SERC’s discretion, in carrying out

the CMEP with respect to the SPP Registered Functions. A SME provided by the SPP RE may be an employee of SPP or an industry volunteer, provided, that no SME provided by the SPP RE may be employed by SPP in an SPP Registered Function. The Parties agree that SMEs provided by the SPP RE shall only be used by SERC in a consulting or advisory capacity to provide expertise and advice on technical matters pertaining to the SPP Registered Functions, shall have no decision-making responsibilities with respect to any compliance processes or compliance enforcement matters, and shall not be a member of any compliance audit team, CI team, or review team for self-certifications, spot check responses, periodic data submittals, self-reports, exception reports or complaints submitted by or relating to an SPP Registered Function.

(d) The SPP RE shall reimburse SERC the actual costs of SERC's performance of the CMEP with respect to the SPP Registered Functions, including an appropriate allocation of SERC's general and administrative costs, in accordance with Section 4 of this Agreement.

(e) Except as provided in this Agreement, the SPP RE shall continue to perform all CMEP responsibilities in the SPP RE Region in accordance with the NERC-SPP Delegation Agreement.

3. Disposition of Penalties Paid by SPP with respect to an SPP Registered Function.

Any penalties to be paid by SPP for violations of Reliability Standards by an SPP Registered Function shall be transmitted to NERC, to be used by NERC as a general offset to NERC's budget for its activities as the Electric Reliability Organization under the Federal Power Act for the following year, in accordance with the *NERC Accounting, Financial Statement and Budgetary Treatment of Penalties Imposed and Received for Violations of Reliability Standards*.

4. Compensation to SERC for Performance of CMEP With Respect to the SPP Registered Functions.

(a) Compensation.

In its annual Business Plans and Budgets submitted to NERC and the Commission for years within the term of this Agreement, SERC shall identify a portion of its CMEP budget (the

“SPP Registered Functions CMEP Budget”), including an appropriate allocation of SERC’s general and administrative costs that is attributable to the performance of the CMEP with respect to the SPP Registered Functions. SERC’s allocation of resources to the performance of its obligations under this Agreement and the corresponding budgeted amount shall be subject to approval by NERC and by the Commission as part of their overall approval of SERC’s business plan and budget. The amount of SERC’s SPP Registered Functions CMEP Budget shall also be included in the SPP RE’s business plan and budget that is submitted to NERC and to the Commission for approval. The amount of the SPP Registered Functions CMEP Budget for each year, as approved by the Commission, shall (i) be excluded from the calculation of SERC’s assessments to Load-Serving Entities (“LSEs”) in the SERC region for each such year, and (ii) be included in the calculation of the SPP RE’s assessments to LSEs in the SPP RE Region for each such year.

(b) Billing

SERC will submit an itemized invoice to the SPP RE, on or before the twentieth (20th) day of each month, for actual costs (including an appropriate allocation of SERC’s general and administrative costs) incurred during the previous month for work undertaken pursuant to this Agreement. The SPP RE shall pay SERC within sixty (60) days for the expenses SERC has incurred and for which it has submitted an invoice. SERC shall track the actual costs of the work as it is performed, and should actual costs be on track to exceed budgeted amounts, SERC shall notify the SPP RE of this at the next billing cycle.

(c) True-up Reports

The Parties shall record their costs and revenues associated with the performance of this Agreement at the same level of line-item detail as is used for their budgets that are submitted to NERC for approval by NERC and by the Commission. Each Party shall include in its annual true-up report submitted to NERC a separate section showing the

Party's actual and budgeted amounts of costs and revenues associated with performance of this Agreement for the year with explanations of variances.

5. Term, Renewal Term, Termination and Early Termination.

(a) Term. The Term of this Agreement shall be from the Effective Date through December 31, 2017.

(b) Renewal Terms. This Agreement shall automatically renew without notice or other action by either Party, at the end of the Term specified in (a) or any Renewal Term for a Renewal Term of five (5) years; provided, however, that either Party may give written notice to the other Party at least twelve (12) months prior to the end of the Term specified in (a) of an intent not to renew this Agreement; and provided, further, that during a Renewal Term either Party may terminate this Agreement by providing a written notice to the other Party at least twelve (12) months prior to the desired termination date. Additionally, this Agreement shall not automatically renew if NERC gives written notice to the Parties, at least twelve (12) months prior to the end of the Term or any Renewal Term, that the Parties should request NERC's approval to renew the Agreement, in which case the Parties shall submit a request to renew the Agreement to NERC at least nine (9) months prior to the end of such Term or Renewal Term. In the event of a termination of this Agreement, SERC shall continue to perform the CMEP role with respect to the SPP Registered Functions within the SPP RE Region, in accordance with the terms of this Agreement and the NERC Uniform CMEP until another entity acceptable to the Commission is selected to take, and takes, responsibility for performance of the CMEP with respect to the SPP Registered Functions.

(c) Early Termination. Notwithstanding the provisions of subsections 5(a) and 5(b) of this Agreement, Early Termination of this Agreement shall occur in the following events:

(i) If SPP or SERC ceases to be a Regional Entity, this Agreement shall terminate as of the end of the calendar year that SPP ceases to be a Regional Entity.

(ii) If SPP or SERC ceases to be a Registered Entity in the SPP RE Region, this Agreement shall terminate as of the last date that SPP or SERC ceases to be a Registered Entity for any SPP Registered Function.

(iii) If both parties agree in writing to terminate this Agreement at any time.

(iv) If any provision of this Agreement, or the application thereof to any person, entity or circumstance, is held by a court or regulatory authority of competent jurisdiction to be invalid, void, or unenforceable, or if a modification or condition to this Agreement is imposed by the Commission, the Parties shall endeavor in good faith to negotiate such amendment or amendments to this Agreement as will restore the relative benefits and obligations of the signatories under this Agreement immediately prior to such holding, modification or condition. If either Party finds such holding, modification or condition unacceptable and the Parties are unable to renegotiate a mutually acceptable resolution, either Party may unilaterally terminate this Agreement. Such termination shall be effective as of one (1) year following written notice by either Party to the other Party, or at such other time as may be mutually agreed by SERC and the SPP RE.

(v) In the event of the Early Termination of this Agreement, SERC will transfer responsibility for completion of all CMEP processes that are in progress as of the date of Early Termination, or within a reasonable time thereafter as mutually agreed to by the Parties, to the entity that will be the CEA for SPP.

(d) In the event of termination or Early Termination of this Agreement, the costs associated with the wind-down of this Agreement and transfer of any compliance processes in progress to the new CEA are payable by the SPP RE to SERC in accordance with Section 4 of this Agreement.

6. Representations of the Parties.

(a) **Representations of the SPP RE.** The SPP RE represents and warrants to SERC that: (i) the SPP RE is and shall remain during the term of this Agreement validly existing and in good standing pursuant to all applicable laws relative to this Agreement, (ii) no applicable law, contract or other legal obligation prevents the SPP RE from executing this Agreement and fulfilling its obligations hereunder, (iii) entry into this Agreement by the SPP RE is duly authorized under its governing corporate documents, and (iv) the person or persons executing this Agreement on behalf of the SPP RE are duly authorized to do so.

(b) **Representations of SERC.** SERC represents and warrants to SPP that: (i) SERC is and shall remain during the term of this Agreement validly existing and in good standing pursuant to all applicable laws relative to this Agreement, (ii) no applicable law, contract or other legal obligation prevents SERC from executing this Agreement and fulfilling its obligations hereunder, (iii) entry into this Agreement by SERC is duly authorized under its governing corporate documents, and (iv) the person or persons executing this Agreement on behalf of SERC are duly authorized to do so.

7. Limitation of Liability.

SERC and the SPP RE agree not to sue each other or their directors, trustees, officers, employees, and persons serving on their committees and subgroups based on any act or omission of any of the foregoing in the performance of duties pursuant to this Agreement or in conducting activities under the authority of Section 215 of the Federal Power Act, other than seeking a review of such action or inaction by the Commission. SERC and the SPP RE shall not be liable to one another for any damages whatsoever, other than for non-payment of or failure to remit compensation due pursuant to Section 4 of this Agreement, including without limitation, direct, indirect, incidental, special, multiple, consequential (including attorneys' fees and litigation costs), exemplary, or punitive damages arising out of or resulting from any act or omission associated with the performance of SERC's or the SPP RE's responsibilities under this Agreement or in conducting activities under the authority of Section 215 of the Federal Power Act, except to the extent that SERC or the SPP RE is found liable for gross negligence or intentional misconduct, in which case SERC or SPP RE shall not be liable for any indirect, incidental, special, multiple, consequential (including without limitation attorneys' fees and litigation costs), exemplary, or punitive damages.

8. No Third Party Beneficiaries.

Nothing in this Agreement shall be construed to create any duty to, any standard of care with reference to, or any liability to any third party.

9. Confidentiality.

During the course of the Parties' performance under this Agreement, a Party may receive Confidential Information, as defined in Section 1500 of the NERC ROP. Except as set forth herein, the Parties agree to keep in confidence and not to copy, disclose, or distribute any Confidential Information or any part thereof, without the prior written permission of the issuing Party, unless disclosure is required by subpoena, law, or other directive of a court,

administrative agency, or arbitration panel, in which event the recipient hereby agrees to provide the Party that provided the Confidential Information with prompt notice of such request or requirement in order to enable such issuing Party to (a) seek an appropriate protective order or other remedy, (b) consult with the recipient with respect to taking steps to resist or narrow the scope of such request or legal process, or (c) waive compliance, in whole or in part, with the terms of this Section 9. In the event a protective order or other remedy is not obtained or the issuing Party waives compliance with the provisions, the recipient agrees to furnish only that portion of the Confidential Information which the recipient's counsel advises is legally required and to exercise best efforts to obtain assurance that confidential treatment will be accorded to such Confidential Information. In addition, each Party shall ensure that its officers, trustees, directors, employees, subcontractors and subcontractors' employees, and agents to whom Confidential Information is exposed are under obligations of confidentiality that are at least as restrictive as those contained herein. This confidentiality provision does not prohibit reporting and disclosure by SERC, as the CEA with respect to the SPP Registered Functions, in accordance with Section 8.0 and other provisions of the NERC Uniform CMEP.

10. Amendment.

Neither this Agreement nor any of the terms hereof, may be amended unless such amendment is made in writing and signed by the Parties.

11. Dispute Resolution.

In the event a dispute arises under this Agreement between SERC and the SPP RE, representatives of the Parties with authority to settle the dispute shall meet and confer in good faith in an effort to resolve the dispute in a timely manner. In the event the designated representatives are unable to resolve the dispute within thirty (30) days or such other period as the Parties may agree upon, each Party shall have all rights to pursue all remedies, except as expressly limited by the terms of this Agreement. Neither Party shall have the right to pursue

other remedies until the Dispute Resolution procedures of this Section 11 have been exhausted. This Section 11 shall not apply to enforcement actions or Remedial Action Directives by SERC, as the CEA, against an SPP Registered Function, or hearings conducted at the request of SPP as the Registered Entity for an SPP Registered Function, pursuant to the NERC Uniform CMEP.

12. Notices.

Whether expressly so stated or not, all notices, demands, requests, and other communications required or permitted by or provided for in this Agreement shall be given in writing to a Party at the address set forth below, or at such other address as a Party shall designate for itself in writing in accordance with this Section, and shall be delivered by hand or reputable overnight courier:

If to SERC:

SERC Reliability Corporation
2815 Coliseum Centre Drive
Suite 500
Charlotte, NC 28217
Attn: Marisa Sifontes
Facsimile: 704-357-7914

If to the SPP RE:

Southwest Power Pool Regional Entity
415 North McKinley,
Suite 140
Little Rock, AR 72205
Attn: Stacy Dochoda
Facsimile: 501-821-8726

Provided, that the foregoing notice provision shall not be applicable to notices and other communications between SERC, as the CEA, and SPP as the Registered Entity for an SPP Registered Function, which notices and other communications shall instead be provided or transmitted in accordance with the NERC Uniform CMEP.

13. Governing Law.

When not in conflict with or preempted by federal law, this Agreement will be governed by and construed in accordance with the laws of Delaware without giving effect to the conflict of law principles thereof. The Parties recognize and agree not to contest the exclusive or primary jurisdiction of the Commission to interpret and apply this Agreement; provided, however, that if the Commission declines to exercise or is precluded from exercising jurisdiction of any action arising out of or concerning this Agreement, such action shall be brought in any state or federal

court of competent jurisdiction in Delaware. All Parties hereby consent to the jurisdiction of any state or federal court of competent jurisdiction in Delaware for the purpose of hearing and determining any action not heard and determined by the Commission.

14. Headings.

The headings and captions in this Agreement are for convenience of reference only and shall not define, limit, or otherwise affect any of the terms or provisions hereof.

15. Entire Agreement.

This Agreement constitutes the entire agreement, and supersedes all prior agreements and understandings, both written and oral, among the Parties with respect to the subject matter of this Agreement.

16. Execution of Counterparts.

This Agreement may be executed in counterparts and each counterpart shall have the same force and effect as the original.

NOW, THEREFORE, the Parties have caused this Agreement to be executed by their duly authorized representatives, to be effective as of the Effective Date.

SERC RELIABILITY CORPORATION

SOUTHWEST POWER POOL, INC.

By: _____

By: _____

Name: R. Scott Henry

Name: Stacy Dochoda

Title: President and CEO

Title: General Manager
SPP Regional Entity

Date: _____

Date: _____

**AGREEMENT BETWEEN
SERC RELIABILITY CORPORATION ~~AND~~ and
SOUTHWEST POWER POOL REGIONAL ENTITY
CONCERNING COMPLIANCE MONITORING AND ENFORCEMENT
OF ~~SPP~~ SOUTHWEST POWER POOL, INC. REGISTERED FUNCTIONS**

THIS AGREEMENT ("Agreement") made effective as of ~~July 12, 2010~~ (the "Effective Date"), between the SERC Reliability Corporation ("SERC"), an organization established to develop and enforce Reliability Standards, and Southwest Power Pool Regional Entity ("SPP RE") a division of ~~SPP~~ Southwest Power Pool, Inc. ("SPP"), an organization established to develop and enforce Reliability Standards within the geographic boundaries identified on Exhibit A (referred to herein as the "SPP RE Region") to the "Amended and Restated Delegation Agreement between the North American Electric Reliability Corporation ("NERC") and ~~Southwest Power Pool, Inc.~~ "SPP" (referred to herein as the "SPP RE Region")", and for other purposes. SERC and the SPP RE may be individually referred to herein as "Party" or collectively as "Parties."

RECITALS

I. SERC is a party to a certain "Amended and Restated Delegation Agreement ~~B~~etween ~~NERC~~ ~~the North American Electric Reliability Corporation~~ and SERC" Reliability Corporation (the "NERC-SERC Delegation Agreement"), which has been approved by the Federal Energy Regulatory Commission ("Commission") and which states in Section 6 thereof, in pertinent part, that SERC shall enforce Reliability Standards (including Regional Reliability Standards) through a compliance monitoring and enforcement program set forth in Exhibit D to the NERC-SERC Delegation Agreement.

II. SPP is a party to a certain "Amended and Restated Delegation Agreement ~~B~~etween ~~the North American Electric Reliability Corporation~~ NERC and ~~SPP~~ Southwest Power Pool, Inc." (the "NERC-SPP Delegation Agreement"), which has been approved by the Commission and which states in Section 6 thereof, in pertinent part, that the SPP RE shall

enforce Reliability Standards (including Regional Reliability Standards) within the geographic boundaries set forth in Exhibit A to the NERC-SPP Delegation Agreement through a compliance monitoring and enforcement program set forth in Exhibit D to the NERC-SPP Delegation Agreement.

III. SPP serves as a Regional Transmission Organization and is currently registered as an Interchange Authority (“IA”), Planning Authority (“PA”), Reliability Coordinator (“RC”), Reserve Sharing Group (“RSG”), Transmission Planner (“TP”), and Transmission Service Provider (“TSP”) in the SPP RE Region. In this Agreement, the ~~RC~~-IA, PA, RC, RSG, TP and TSP functions are sometimes referred to as the “SPP Registered Functions,” and SPP is referred to as the “Registered Entity” with respect to its performance of the SPP Registered Functions.

IV. To avoid any appearance of a lack of independence in compliance monitoring and enforcement for SPP Registered Functions, SERC and the SPP RE hereby agree, subject to approval by NERC and by the Commission, that SERC should assume responsibility for the Compliance Monitoring and Enforcement Program (“CMEP”) with respect to the SPP Registered Functions within the SPP RE Region, and that the terms on which responsibility for the CMEP with respect to the SPP Registered Functions within the SPP RE Region shall be ~~transferred to~~ and performed by SERC should be memorialized in this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants and agreements contained herein, the Parties, intending to be bound, agree as follows:

1. Responsibilities of SERC.

(a) Beginning on the Effective Date, SERC will perform all responsibilities of the Compliance Enforcement Authority (“CEA”) as specified in the NERC uniform CMEP, Appendix 4C to the NERC Rules of Procedure (“ROP”), as amended from time to time (the “NERC Uniform CMEP”), within the SPP RE Region with respect to the SPP Registered Functions.

(b) Without limiting the scope of SERC's responsibilities as stated in ~~S~~subsection 1(a) of this Agreement, SERC agrees to perform the following activities within the SPP RE Region:

(1) Administer all compliance processes in Section 3.0 of the NERC Uniform CMEP with respect to the SPP Registered Functions, in accordance with the NERC Annual CMEP Implementation Plan required by Section 4.1 of the NERC Uniform CMEP for each year. If at any time, SPP Registered Functions change, SERC will monitor the Registered Functions in effect at that time.

(2) Lead all compliance audits and compliance ~~violation~~ investigations ("CVI") of the SPP Registered Functions.

(i) SERC shall conduct a scheduled compliance audit of the SPP Registered Functions in accordance with the frequency established by NERC in the CMEP. As SPP is currently registered, SERC will audit the RC function at least once every three (3) years and shall conduct a scheduled compliance audit of the remaining functions at least once every six (6) years.

(ii) Scheduled compliance audits of the SPP Registered Functions ~~shall include all actively monitored standards~~ shall be in accordance with the NERC Annual CMEP Implementation Plan.

(iii) As required by the NERC ROP, all compliance audits of the SPP RC function shall be conducted on site. Spot checks or other compliance monitoring methods may be completed off site.

(3) Determine if Notices of Possible Violations and Notices of Alleged Violations, as those terms are defined in the CMEP, and proposed penalties or sanctions should be issued to SPP with respect to the SPP Registered Functions, and calculate or determine any proposed penalties or sanctions in accordance with the NERC *Sanction Guidelines*.

(4) Administer processes as specified in Section 5.0 of the NERC Uniform CMEP with respect to any ~~notices of~~ Alleged Violations, as that term is defined in the CMEP, and proposed penalties or sanctions issued with respect to the SPP Registered Functions.

(5) Review and approve proposed Mitigation Plans submitted by an SPP Registered Function, and monitor implementation and completion of approved Mitigation Plans, in accordance with Section 6.0 of the NERC Uniform CMEP.

(6) Determine if Remedial Action Directives should be issued to SPP with respect to an SPP Registered Function, and issue such Remedial Action Directives if determined to be necessary, in accordance with Section 7.0 of the NERC Uniform CMEP.

(7) Conduct settlement negotiations for any violations of Reliability Standards discovered by SERC per this agreement, if requested by SPP, in accordance with Section 5.4 of the NERC Uniform CMEP.

(8) Provide due process hearings for the SPP Registered Functions with respect to notices of Alleged Violations, proposed penalties and sanctions, disputed Mitigation Plans, and disputed Remedial Action Directives, as requested by SPP, in accordance with Attachment 2, Hearing Procedures, to the NERC Uniform CMEP.

(c) Compliance audit teams, ~~CVICI~~ teams, and review teams for self-certifications, spot check responses, periodic data submittals, self-reports, exception reports and complaints submitted by or relating to an SPP Registered Function shall not include any employees of SPP, but may include employees of other Regional Entities, NERC and Commission staff members. Provided, that in accordance with Section 2(c) of this Agreement, SERC may request and obtain technical advice and assistance from SPP employees, acting in a consulting or advisory capacity, who are not employed in an SPP Registered Function.

2. Responsibilities of SPP.

(a) ~~As the Registered Entity for the SPP Registered Functions,~~ SPP shall establish and designate to SERC a primary compliance contact for each SPP Registered Function, in accordance with Section 2.0 of the NERC Uniform CMEP.

(b) ~~As the Registered Entity for the SPP Registered Functions,~~ SPP shall timely respond to and comply with all notices, requests for information and schedules issued by SERC as the CEA pursuant to the NERC Uniform CMEP.

(c) The SPP RE shall provide subject-matter experts (“SMEs”) as requested by SERC to provide technical advice and assistance to SERC, in SERC’s discretion, in carrying out the CMEP with respect to the SPP Registered Functions. A SME provided by the SPP RE may be an employee of SPP or an industry volunteer, provided, that no SME provided by the SPP RE may be employed by SPP in an SPP Registered Function. The Parties agree that SMEs provided by the SPP RE shall only be used by SERC in a consulting or advisory capacity to provide expertise and advice on technical matters pertaining to the SPP Registered Functions, shall have no decision-making responsibilities with respect to any compliance processes or compliance enforcement matters, and shall not be a member of any compliance audit team, ~~CVICI~~ team, or review team for self-certifications, spot check responses, periodic data submittals, self-reports, exception reports or complaints submitted by or relating to an SPP Registered Function.

(d) The SPP RE shall reimburse SERC the actual costs of SERC’s performance of the CMEP with respect to the SPP Registered Functions, including an appropriate allocation of SERC’s ~~G~~eneral and ~~A~~administrative costs, in accordance with Section ~~45~~ of this Agreement.

(e) Except as provided in this Agreement, the SPP RE shall continue to perform all CMEP responsibilities in the SPP RE Region in accordance with the NERC-SPP Delegation Agreement.

3. Disposition of Penalties Paid by SPP with respect to an SPP Registered Function.

Any penalties to be paid by SPP for violations of Reliability Standards by an SPP Registered Function, shall be transmitted to NERC, to be used by NERC as a general offset to NERC's budget for its activities as the Electric Reliability Organization under the Federal Power Act for the following year, in accordance with the *NERC Accounting, Financial Statement and Budgetary Treatment of Penalties Imposed and Received for Violations of Reliability Standards*.

~~**4. Transfer of Responsibilities for CMEP Activities With Respect to SPP Registered Functions That Are In Progress on the Effective Date.**~~

~~SERC shall assume full responsibility, as the CEA, for completion of all compliance processes with respect to the SPP Registered Functions within the SPP RE Region that are in progress as of the Effective Date, including without limiting the foregoing, (i) completion and issuance of reports of compliance audits and CVICI of the SPP Registered Functions, (ii) completion of review of, and issuance of any findings or reports concerning, any self-certifications, spot checks, periodic data submittals, self-reports, exception reports or complaints, submitted by or pertaining to a SPP Registered Function, (iii) determination of whether any notice of Alleged Violations and/or proposed penalties or sanctions should be issued to a SPP Registered Function as a result of any such compliance processes, (iv) processing of any notices of Alleged Violations and/or proposed penalties or sanctions that were issued before the Effective Date, or are issued after the Effective Date as the result of compliance processes conducted before the Effective Date, and (v) review, approval and monitoring of implementation and completion of any Mitigation Plans required of a SPP Registered Function as the result of compliance processes conducted before the Effective Date.~~

5.4. Compensation to SERC for Performance of CMEP With Respect to the SPP Registered Functions.

- (a) ~~Compensation for 2010 through December 31, 2012.~~

~~For the period between the Effective Date of this Agreement and December 31, 2010, SERC shall invoice SPP RE the amount of \$40,000 in for invoices of \$10,000 each. The first such invoice will be issued on or about the Effective Date and the remaining three invoices shall be issued at approximately equal intervals between the Effective Date and December 31, 2010. SPP RE shall remit to SERC the amount of each invoice by check or electronic funds transfer to SERC within twenty (20) business days following the date of each invoice.~~

~~(b) —~~ Compensation for Years Subsequent to 2010.

~~(i) —~~ In its annual Business Plans and Budgets submitted to NERC and the Commission for ~~the year 2011 and subsequent~~ years within the term of this Agreement, SERC shall identify a portion of its CMEP budget (the “SPP Registered Functions CMEP Budget”), including an appropriate allocation of SERC’s ~~G~~general and ~~A~~administrative ~~costs~~costs (~~the “SPP Registered Functions CMEP Budget”~~), that is attributable to the performance of the CMEP with respect to the SPP Registered Functions. SERC’s allocation of resources to the performance of its obligations under this Agreement and the corresponding budgeted amount shall be subject to approval by NERC and by the Commission as part of their overall approval of SERC’s business plan and budget. The amount of SERC’s SPP Registered Functions CMEP Budget shall also be included in the SPP RE’s business plan and budget that is submitted to NERC and to the Commission for approval. The amount of the SPP Registered Functions CMEP Budget for each year, as approved by the Commission, shall (i) ~~shall~~ be excluded from the calculation of SERC’s assessments to Load-Serving Entities (“LSEs”) in the SERC region for each such year, and (ii) ~~shall~~ be included in the calculation of the SPP RE’s assessments to LSEs in the SPP RE Region for each such year. ~~SERC shall invoice SPP RE for the amount of the SPP Registered Functions CMEP Budget in four equal quarterly amounts during each year, with the invoices to be issued by SERC to SPP RE on or about January 1, April 1, July 1 and October 1 and to be paid by SPP RE by check or electronic funds transfer to SERC within (20) business days following the date of the invoice.~~

~~(c) — Reconciliation of Costs.~~

~~No later than 90 days after the end of a budget year, SERC shall provide to SPP RE a statement of actual expenses incurred by SERC in the fulfillment of SERC's responsibilities under this agreement for that budget year. The statement shall disclose the actual costs of labor, travel and meetings, and all other direct costs, as well as SERC's allocation of its General and Administrative costs. The statement shall summarize the reasons for any variances as compared to the budget amount. SERC shall provide supporting documentation for the final statement upon request by SPP RE. The total variance for the concluded budget year shall be incorporated as a compensating adjustment in both the SERC and SPP RE budgets in the second year following the budget year and, as approved by NERC and the Commission, reflected in the quarterly invoices from SERC to SPP RE and quarterly payments by SPP RE to SERC in such year.~~

~~(d) — Supplemental Invoice.~~

~~If during any budget year, including the initial budget year 2012, the actual cost of performing SERC's responsibilities under this agreement exceeds the budgeted funding by more than ten (10) percent of SERCs budgeted cash reserve (for example as may be necessitated by the conduct of a compliance violation investigation or hearing), SERC shall have the right to issue supplemental invoices to SPP RE to recover in full all actual costs incurred above the budgeted funding. Upon receipt of such a supplemental invoice, SPP RE shall pay the full amount of the invoice by check or electronic funds transfer to SERC within sixty (60 days).~~

~~— (be)(b) Billing~~

~~SERC will submit an itemized invoice to the SPP RE, on or before the twentieth (20th) day of each month, for actual costs (including an appropriate allocation of SERC's general and administrative costs) incurred during the previous month for work undertaken pursuant to this Agreement. The SPP RE shall pay SERC within sixty (60) days for the expenses SERC has~~

incurred and for which it has submitted an invoice. SERC shall track the actual costs of the work as it is performed, and should actual costs be on track to exceed budgeted amounts, SERC shall notify the SPP RE of this at the next billing cycle.

SERC shall invoice SPP RE for the amount of the SPP Registered Functions CMEP Budget in four equal quarterly amounts during each year, with the invoices to be issued by SERC to SPP RE on or about January 1, April 1, July 1 and October 1 and to be paid by SPP RE by check or electronic funds transfer to SERC within twenty (20) business days following the date of the invoice.

(c) True-up Reports

The Parties shall record their costs and revenues associated with the performance of this Agreement at the same level of line-item detail as is used for their budgets that are submitted to NERC for approval by NERC and by the Commission. Each Party shall include in its annual true-up report submitted to NERC a separate section showing the Party's actual and budgeted amounts of costs and revenues associated with performance of this Agreement for the year with explanations of variances.

65. Term, Renewal Term, Termination and Early Termination.

(a) Initial Term. The ~~Initial~~Term of this Agreement shall be from the Effective Date through December 31, ~~2012~~2017.

(b) Renewal Terms. This Agreement shall automatically not renew without notice or other action by either Party, at the end of the ~~Initial~~ Term specified in (a) or any Renewal Term for a Renewal Term of five (5) years; provided, however, that either Party may give written notice to the other Party at least twelve (12) months prior to the end of the Term specified in (a) of an intent not to renew this Agreement; and provided, further, that during a Renewal Term

~~either Party may terminate this Agreement by providing a written notice to the other Party at least twelve (12) months prior to the desired termination date. Additionally, this Agreement shall not automatically renew if NERC gives written notice to the Parties, at least twelve (12) months prior to the end of the Term or any Renewal Term, that the Parties should request NERC's approval to renew the Agreement, in which case the Parties shall submit a request to renew the Agreement to NERC at least nine (9) months prior to the end of such Term or Renewal Term. In the event of a termination of this Agreement, SERC shall continue to perform the CMEP role with respect to the SPP Registered Functions within the SPP RE Region, in accordance with the terms of this Agreement and the NERC Uniform CMEP until another entity acceptable to the Commission is selected to take, and takes, responsibility for performance of the CMEP with respect to the SPP Registered Functions, without the express approval of NERC and the Commission. If either Party does not plan to seek approval for renewal of the agreement, that Party must give written notice to the other Party and NERC, at least one (1) year prior to the end of the Initial Term. In the event the Parties intend to renew the Agreement, they shall make a joint filing to NERC not later than April 1, 2012 2014 requesting approval of the renewal. In the event of termination of the Agreement, SERC will work with SPP RE to transfer responsibility for any compliance activities in progress to the entity that will be the CEA for SPP.~~

(c) Early Termination. Notwithstanding the provisions of subsections 65(a) and 65(b) of this Agreement, Early Termination of this Agreement shall occur in the following events:

(i) If SPP or SERC ceases to be a Regional Entity, this Agreement shall terminate as of the end of the calendar year that SPP ceases to be a Regional Entity.

(ii) If SPP or SERC ceases to be a Registered Entity in the SPP RE Region, this Agreement shall terminate as of the last date that SPP or SERC ceases to be a Registered Entity for any SPP Registered Function.

(iii) If both parties agree in writing to terminate this Agreement at any time.

(iv) If any provision of this Agreement, or the application thereof to any person, entity or circumstance, is held by a court or regulatory authority of competent jurisdiction to be invalid, void, or unenforceable, or if a modification or condition to this Agreement is imposed by the Commission, the Parties shall endeavor in good faith to negotiate such amendment or amendments to this Agreement as will restore the relative benefits and obligations of the signatories under this Agreement immediately prior to such holding, modification or condition. If either Party finds such holding, modification or condition unacceptable and the Parties are unable to renegotiate a mutually acceptable resolution, either Party may unilaterally terminate this Agreement. Such termination shall be effective as of one (1) year following written notice by either Party to the other Party, or at such other time as may be mutually agreed by SERC and the SPP RE.

(v) ~~Provided, that if~~ in the event of the Early Termination of this Agreement,

~~(i)~~ SERC will transfer responsibility for completion of all CMEP –compliance processes that are in progress as of the date of Early Termination, or within a reasonable time thereafter, as mutually agreed to by the ~~p~~Parties, to the entity that will be the CEA for SPP.

(d) In the event of termination or Early Termination of this Agreement, the costs associated with the wind-down of this Agreement and transfer of any compliance processes in progress to the new CEA are payable by the SPP RE to SERC in accordance with Section 54 of this Agreement.

76. Representations of the Parties.

(a) Representations of the SPP RE. The SPP RE represents and warrants to SERC that: –(i) the SPP RE is and shall remain during the term of this Agreement validly existing and in good standing pursuant to all applicable laws relative to this Agreement, (ii) no applicable law,

contract or other legal obligation prevents the SPP RE from executing this Agreement and fulfilling its obligations hereunder, (iii) entry into this Agreement by the SPP RE is duly authorized under its governing corporate documents, and (iv) the person or persons executing this Agreement on behalf of the SPP RE are duly authorized to do so.

(b) Representations of SERC. SERC represents and warrants to SPP that: (i) SERC is and shall remain during the term of this Agreement validly existing and in good standing pursuant to all applicable laws relative to this Agreement, (ii) no applicable law, contract or other legal obligation prevents SERC from executing this Agreement and fulfilling its obligations hereunder, (iii) entry into this Agreement by SERC is duly authorized under its governing corporate documents, and (iv) the person or persons executing this Agreement on behalf of SERC are duly authorized to do so.

87. Limitation of Liability.

SERC and the SPP RE agree not to sue each other or their directors, trustees, officers, employees, and persons serving on their committees and subgroups based on any act or omission of any of the foregoing in the performance of duties pursuant to this Agreement or in conducting activities under the authority of Section 215 of the Federal Power Act, other than seeking a review of such action or inaction by the Commission. SERC and the SPP RE shall not be liable to one another for any damages whatsoever, other than for non-payment of or failure to remit compensation due pursuant to Section 54 of this Agreement, including without limitation, direct, indirect, incidental, special, multiple, consequential (including attorneys' fees and litigation costs), exemplary, or punitive damages arising out of or resulting from any act or omission associated with the performance of SERC's or the SPP RE's responsibilities under this Agreement or in conducting activities under the authority of Section 215 of the Federal Power Act, except to the extent that SERC or the SPP RE is found liable for gross negligence or intentional misconduct, in which case SERC or SPP RE shall not be liable for any indirect,

incidental, special, multiple, consequential (including without limitation attorneys' fees and litigation costs), exemplary, or punitive damages.

98. No Third Party Beneficiaries.

Nothing in this Agreement shall be construed to create any duty to, any standard of care with reference to, or any liability to any third party.

109. Confidentiality.

During the course of the Parties' performance under this Agreement, a Party may receive Confidential Information, as defined in Section 1500 of the NERC ROP. Except as set forth herein, the Parties agree to keep in confidence and not to copy, disclose, or distribute any Confidential Information or any part thereof, without the prior written permission of the issuing Party, unless disclosure is required by subpoena, law, or other directive of a court, administrative agency, or arbitration panel, in which event the recipient hereby agrees to provide the Party that provided the Confidential Information with prompt notice of such request or requirement in order to enable such issuing Party to (a) seek an appropriate protective order or other remedy, (b) consult with the recipient with respect to taking steps to resist or narrow the scope of such request or legal process, or (c) waive compliance, in whole or in part, with the terms of this Section ~~109~~. In the event a protective order or other remedy is not obtained or the issuing Party waives compliance with the provisions, the recipient agrees to furnish only that portion of the Confidential Information which the recipient's counsel advises is legally required and to exercise best efforts to obtain assurance that confidential treatment will be accorded to such Confidential Information. In addition, each Party shall ensure that its officers, trustees, directors, employees, subcontractors and subcontractors' employees, and agents to whom Confidential Information is exposed are under obligations of confidentiality that are at least as restrictive as those contained herein. This confidentiality provision does not prohibit reporting

and disclosure by SERC, as the CEA with respect to the SPP Registered Functions, in accordance with Section 8.0 and other provisions of the NERC Uniform CMEP.

4110. Amendment.

Neither this Agreement nor any of the terms hereof, may be amended unless such amendment is made in writing and signed by the Parties.

4211. Dispute Resolution.

In the event a dispute arises under this Agreement between SERC and the SPP RE, representatives of the Parties with authority to settle the dispute shall meet and confer in good faith in an effort to resolve the dispute in a timely manner. In the event the designated representatives are unable to resolve the dispute within thirty (30) days or such other period as the Parties may agree upon, each Party shall have all rights to pursue all remedies, except as expressly limited by the terms of this Agreement. Neither Party shall have the right to pursue other remedies until the Dispute Resolution procedures of this Section 4211 have been exhausted. This Section 4211 shall not apply to enforcement actions or Remedial Action Directives by SERC, as the CEA, against an SPP Registered Function, or hearings conducted at the request of SPP as the Registered Entity for an SPP Registered Function, pursuant to the NERC Uniform CMEP.

4312. Notices.

Whether expressly so stated or not, all notices, demands, requests, and other communications required or permitted by or provided for in this Agreement shall be given in writing to a Party at the address set forth below, or at such other address as a Party shall designate for itself in writing in accordance with this Section, and shall be delivered by hand or reputable overnight courier:

If to SERC:

SERC Reliability Corporation

If to the SPP RE:

Southwest Power Pool Regional Entity.

2815 Coliseum Centre Drive
Suite 500
Charlotte, NC 28217
Attn: Marisa Sifontes
Facsimile: 704-357-7914

~~415 North McKinley,
Suite 14016101 La Grande
Suite 103~~
Little Rock, AR 7220523
Attn: Stacy Dochoda
Facsimile: 501-821-8726

Provided, that the foregoing notice provision shall not be applicable to notices and other communications between SERC, as the CEA, and SPP as the Registered Entity for an SPP Registered Function, which notices and other communications shall instead be provided or transmitted in accordance with the NERC Uniform CMEP.

1413. Governing Law.

When not in conflict with or preempted by federal law, this Agreement will be governed by and construed in accordance with the laws of Delaware without giving effect to the conflict of law principles thereof. The Parties recognize and agree not to contest the exclusive or primary jurisdiction of the Commission to interpret and apply this Agreement; provided, however, that if the Commission declines to exercise or is precluded from exercising jurisdiction of any action arising out of or concerning this Agreement, such action shall be brought in any state or federal court of competent jurisdiction in Delaware. All Parties hereby consent to the jurisdiction of any state or federal court of competent jurisdiction in Delaware for the purpose of hearing and determining any action not heard and determined by the Commission.

1514. Headings.

The headings and captions in this Agreement are for convenience of reference only and shall not define, limit, or otherwise affect any of the terms or provisions hereof.

1615. Entire Agreement.

This Agreement constitutes the entire agreement, and supersedes all prior agreements and understandings, both written and oral, among the Parties with respect to the subject matter of this Agreement.

1716. Execution of Counterparts.

This Agreement may be executed in counterparts and each counterpart shall have the same force and effect as the original.

NOW, THEREFORE, the Parties have caused this Agreement to be executed by their duly authorized representatives, to be effective as of the Effective Date.

SERC RELIABILITY CORPORATION

SOUTHWEST POWER POOL, INC.

By: _____

By: _____

Name: R. Scott Henry

Name: Stacy Dochoda

Title: President and CEO

Title: General Manager
SPP Regional Entity

Date: _____

Date: _____

MRC Standards Process Input Group (SPIG) Recommendations

Action

Discussion of Member Representatives Committee (MRC) input.

Background

In February 2012, the MRC was asked to commence a working group to provide policy input and recommendations for specific improvements to the existing NERC reliability standards development process. The Standards Process Input Group (SPIG) commenced in March and sought industry input and feedback on a variety of issues which included:

- Quality of standards, to include process and product
- Timeliness
- Efficiency and effectiveness
- Importance and significance of meeting ANSI requirements

The SPIG gathered valuable input and insight on a number of significant issues related to standards development and compiled a report consisting of five recommendations. The MRC followed by the Standards Oversight and Technology Committee (SOTC) plan to discuss, during May 8, these recommendations to determine:

- Which have merit and which need additional refinement;
- If concerns relative to production, efficiency and quality, raised by stakeholders and regulators, have been addressed;
- Whether additional changes to the governance of the standards development process are needed to supplement the SPIG's report; and
- What oversight the SOTC and Board of Trustees will want to see over how implementation issues are analyzed and ultimately proposed for endorsement, acceptance, or approval.

The MRC plans to discuss, during its May 8 meeting, these recommendations to determine which have merit and which need additional refinement. Once the SPIG has received the MRC's input it will finalize a proposal for the implementation of the recommendations before providing a package to the Board of Trustees for their endorsement and action at a later date. In some cases, changes to the Rules of Procedure may be required for final implementation, which will take additional time to develop and gain approval.

The SPIG will present the draft report and its recommendations to the MRC and SOTC for additional discussion and targets the final report and recommendations for Board of Trustees approval in late May 2012.

Recommendations to Improve the NERC Standards Development Process

Member Representatives Committee (MRC)
Standards Process Input Group (SPIG)

Draft — April 2012

RELIABILITY | ACCOUNTABILITY



Preface

Formation of the Standards Process Input Group

At its February 9, 2012 meeting, the NERC Board of Trustees (BOT) requested the assistance of the NERC Member Representatives Committee (MRC) to provide policy input, and a proposed framework, for specific improvements needed to the standards development process. The MRC Chair and Vice Chair invited several members of the MRC, two NERC Board of Trustees members, the NERC CEO, and the Standards Committee (SC) Chair to join with them as participants in the Standards Process Input Group (SPIG) in developing recommendations to improve the standards development process in the following areas:

- Clarity on the reliability objectives, technical parameters, scope, and the relative priority of the standards project.
- The drafting process (developing the specific technical content of the standard).
- Standards project management and workflow.
- Formal balloting and commenting.

To help ensure that the SPIG focused its efforts on the best areas for improvement, they began their process by gathering input from subject matter experts (SMEs), including the regions, MRC, Standard Drafting Team leaders, NERC staff, and other stakeholders by asking the following:

- What are the issues that are keeping the process from improving the reliability benefits of the standards?
- What are the impediments to improving the efficiency of completing a new standard or standard revision?
- Are stakeholder resources being used efficiently? If not, then why?

SPIG Timeline for Input

- Trades input was provided to NERC BOT in January 2012
- Outreach Survey comments received from 105 stakeholders in late February
- SPIG conference call with FERC staff and initial SPIG planning meeting conducted in early March
- SPIG provides preliminary report to MRC for input in early April
- Input from MRC received by April 13
- Additional SPIG planning meeting to consider MRC input conducted April 19-20
- Report revised, finalized, and posted with MRC agenda on April 25
- MRC discussion at MRC meeting on May 8
- Final report to NERC BOT in late May

Table of Contents

Preface	i
Executive Summary.....	1
Introduction	3
Recommendations from the SPIG.....	5
Recommendation 1: American National Standards Institute.....	5
Recommendation 2: Reliability Issues Steering Committee (RISC)	6
Recommendation 3: Interface with Regulatory and Governmental Authorities	10
Recommendation 4: Standards Product.....	12
Recommendation 5: Standards Development Process and Resources.....	14

Executive Summary

The Standards Process Input Group (SPIG) organized by the NERC Member Representatives Committee (MRC) is proposing in this report a number of changes to the way NERC develops Reliability Standards and other solutions intended to improve the priority, product and process of standards development. Inherent in these proposed changes is an effort to better understand, articulate and incorporate, into the standards development process, the appropriate accountabilities for standards development.

For example, Section 215 of the Federal Power Act creates accountability for the Federal Energy Regulatory Commission (FERC), first to certify an Electric Reliability Organization (ERO) for the purpose of establishing and enforcing reliability standards for the bulk power system, and then to approve the standards developed by the ERO. As such, FERC is accountable to the U.S. Congress, which passed the law that created Section 215.

Section 215 also creates accountability for NERC by requiring that the ERO, certified by FERC, have a demonstrated ability to develop and enforce reliability standards that provide for an adequate level of reliability of the bulk power system. This accountability extends to the NERC management to see that high quality standards are developed in an efficient and effective way and to the NERC Board of Trustees (Board) that must approve those standards before they are filed with governmental regulatory authorities in the U.S. and Canada.

Finally, the stakeholders, whose technical expertise is essential to the development of the standards, have a shared accountability with NERC and with each other to see that the right standards are developed in a fair, open, balanced and inclusive way.

One of the principal recommendations of the SPIG, is the creation of a Reliability Issues Steering Committee (RISC) that is intended to address these issues of accountability by ensuring that NERC develops the right standards, in the right way, and in a timely and efficient manner. To accomplish this, the RISC will conduct front-end, high level review of nominated reliability issues and direct the initiation of standards projects or other solutions that will address the reliability issues.

In addition to recommending the creation of the RISC, the SPIG also recommends that Reliability Standards Audit Worksheets (RSAWs) be developed concurrent with their associated standards and posted along with those standards for comment. The purpose here is to make sure that the RSAWs are aligned with the intent and wording of the standards to reduce the need for Interpretations and Compliance Application Notices.

Lastly, the SPIG is recommending a redesign of the composition and process used by Standards Drafting Teams to make more efficient and effective use of the subject matter expertise resident in the industry, and to provide those experts with additional support resources in terms of project management and facilitation, legal expertise, and technical writing support.

The recommendations also aim to strengthen consensus building, first on the need for a standard and then on the requirements themselves.

Collectively, these recommendations suggest a major revision of how decisions to develop standards are determined in the first place and, once the decision is made that a new or revised standard is needed, to see that it is developed in the most efficient, effective, and timely way, taking into account throughout the process the costs, benefits and justification for all standards.

Introduction

Priority, product and process are the three main focus areas addressed by the recommendations of the SPIG regarding their review and analysis of the NERC standards development process.

The SPIG provides five recommendations designed for action and for discussion. The analysis of feedback received throughout this project indicates that more discussion should occur around the variety of the changes, improvements, and implementation being proposed in these recommendations, as listed below and described in more detail in this report.

Recommendation 1: American National Standards Institute — NERC should continue to meet the minimum requirements of the American National Standards Institute (ANSI) process to preserve ANSI accreditation.

Recommendation 2: Reliability Issues Steering Committee — The NERC Board is encouraged to form a Reliability Issues Steering Committee (RSIC) to conduct front-end, high level review of nominated reliability issues and direct the initiation of standards projects or other solutions that will address the reliability issues.

Recommendation 3: Interface with Regulatory and Governmental Authorities — The NERC Board is encouraged to task NERC management, working with a broad array of ERO resources (e.g., MRC, technical committees, Regional Entities, trade associations, etc.) to develop a strategy for improving the communication and awareness of effective reliability risk controls which increases input and alignment with state, federal, and provincial authorities.

Recommendation 4: Standards Product Issues — The NERC board is encouraged to require that the standards development process address:

- The use of results-based standards (RBS);
- Cost effectiveness of standards and standards development;
- Alignment of standards requirements/measures with Reliability Standards Audit Worksheets (RSAWs); and
- The retirement of standards no longer needed to meet an adequate level of reliability.

Recommendation 5: Standards Development Process and Resource Issues — The NERC Board is encouraged to require the standards development process to be revised to improve timely, stakeholder consensus in support of new or revised reliability standards. The Board is also encouraged to require standard development resources to achieve and address:

- Formal and consistent project management; and
- Efficient formation and composition of Standard Drafting Teams (SDTs).

These recommendations were derived from a synthesis of stakeholder responses categorized into the following three concentrated areas:

I. ANSI: Accreditation

- Preserve ANSI accreditation in order to ensure openness, transparency, consensus building, balance of interests and due process
- Ensure checks and balances of the ANSI process
- Limit application of requirements that can hinder progress
- Limit negative ballots without comment
- Consider other options if ANSI prevents efficiency gains

II. PRODUCT: Quality of Standards

- Consider the cost effectiveness (limited value justification)
- Improve clarity in terms of the reliability objective and benefit
- Ensure auditability
- Improve supporting documentation or administrative records
- Improve registered entity and auditor understanding
- Involve industry, NERC and FERC in the quality review earlier in the standards development process
- Seek clarity and technical justification upfront
- Be sensitive not to gear towards compliance risk rather than reliability risk

III. PROCESS: Efficiency, Timeliness and Effectiveness

- Address the SDT composition (need expertise in legal, technical writing, compliance, etc.)
- Improve timeliness and effectiveness in terms of commenting/balloting (need to consider the manual effort and timing associated with posting, grouping and responding)
- Manage the number of standards coming through the process at the same time (to ensure the right number can be processed efficiently)
- Seek convergence on consensus (to avoid taking too long to achieve)
- Improve efficiencies (to avoid taking too long)
- Implement a project manager and facilitator (need within the SDT and the back office of NERC)
- Improve communications and coordination between industry, NERC and FERC staff; especially in terms of the compliance/enforcement process

Recommendations from the SPIG

Recommendation 1: American National Standards Institute

Issue

Should NERC continue using the American National Standards Institute (ANSI) process for developing standards?

Recommendation

NERC should continue to meet the minimum requirements of the ANSI process to preserve ANSI accreditation.

Background

The SPIG’s initial survey of the industry asked “How important are ANSI accreditation and ANSI principles (openness, transparency, consensus-building, fair balance of interests, and due process) to the NERC standards development process?” The majority of responses agreed that NERC standards development process should continue to at least meet the minimum ANSI requirements (Figure 1).

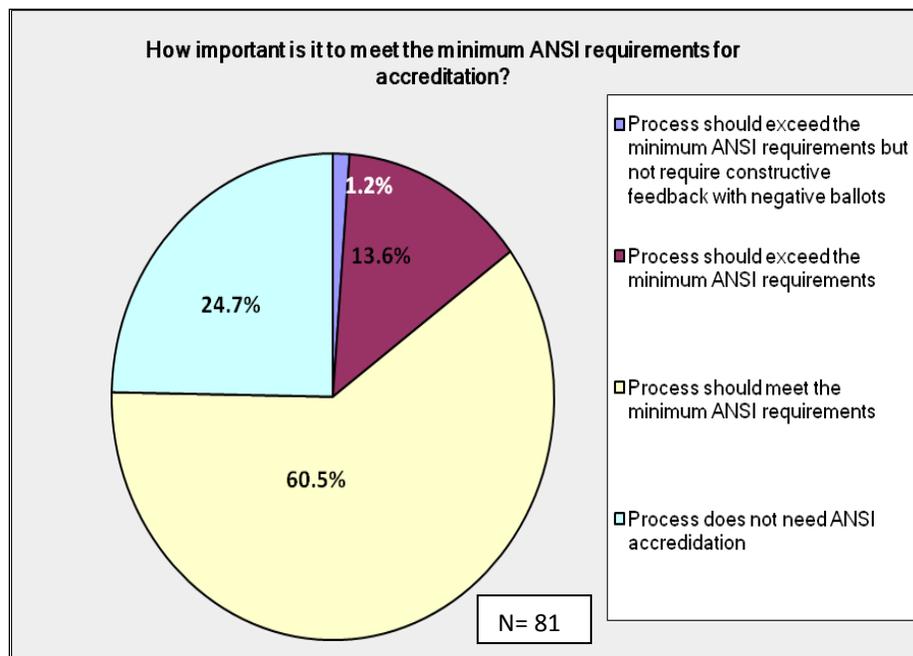


Figure 1: Results from SPIG survey of the Industry, April 2012

According to ANSI, accreditation signifies the standards developer is committed to an open, fair and time-tested consensus process that benefits stakeholders. Developers are accredited to the requirements contained in the *ANSI Essential Requirements: Due Process Requirements for American National Standards*. NERC staff confirms that the current standards process meets and in some cases exceeds the ANSI Essential Requirements.

Recommendation 2: Reliability Issues Steering Committee (RISC)

Issue

How should NERC determine:

- What actions are needed to address identified risks to reliability?
- Whether the development of a standard is necessary and its cost/benefit to reliability is justified?
- What should be the priority and timeline for standards development?

Recommendation

The Board is encouraged to form a Reliability Issues Steering Committee (RISC) to conduct front-end, high level review of nominated reliability issues and direct the initiation of standards projects or other solutions that will address the reliability issues.

Proposed Details

The RISC would:

- Be comprised of stakeholders including, but not limited to:
 - Chairs and vice chairs of the technical committees;
 - Select MRC members and other stakeholders;
 - Chair, approved by the Board; and
 - NERC Senior Staff member.
- Utilize a broad range of industry and other expertise.
- Analyze performance gaps, technical viability, reliability benefit, cost impact/justification, clarity of standard's scope, etc.
- Advise the Board on key initiatives and priorities; recommends standards projects or alternatives (Figure 2).
- Report directly to Board (and not the MRC).
- Require Board review and approval of any significant new ERO initiatives or reordering of ERO strategic priorities.
- Not supersede the role of Standards Committee.
- Set milestones and timelines for standards projects.
- Conform to NERC Bylaws and Rules of Procedure.

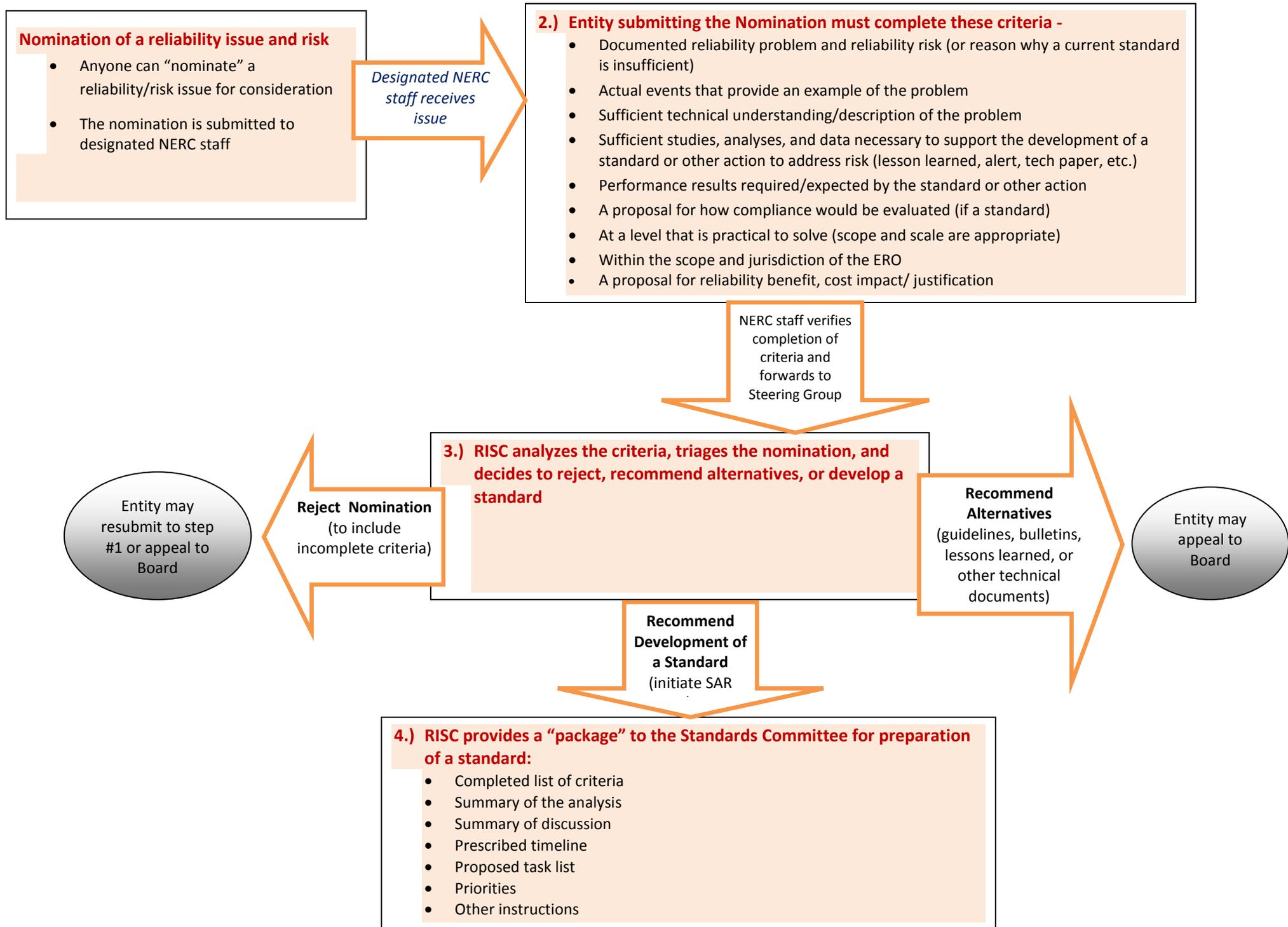
Additional Issues to be Addressed (per the Board's Discretion) During the Implementation Phase

- Role of the RISC in three-year reliability SDP.
- Modification to existing standards including elimination of duplicative or low value standards.
- Role of RISC with respect to FERC directives.
- Communication between the RISC, Standards Committee (SC), Standards Oversight and Technology Committee, MRC and Board and its technical committees.
- Relationship with governmental authorities.

Explanation of Figure 2: Proposed Front-End Process Flow Chart

- Anyone can “nominate” a reliability/risk issue, via designated NERC staff, for consideration by the RISC. Upon verification and satisfactory completion of the nomination criteria, the RISC may decide to:
 1. Reject the nomination;
 2. Recommend alternative action other than standards; or,
 3. Develop a standard.
- If the nomination is rejected by the RISC, an appeals process will be available.
- Recommended alternatives to standards may include the development of guidelines, bulletins, alerts, lessons learned, best practices, technical documents, etc. If a standard is recommended, a project management “package” will be prepared by the RISC for the SC, including (as appropriate):
 - The completed list of criteria
 - Analysis of performance gaps, technical viability, reliability benefit, cost impact/justification, clarity of standard’s scope, etc.
 - Discussion
 - Timeline
 - Task list
 - Priorities
 - Other instructions
- The RISC may refer a “package” to the SC with instructions to prepare a standard. The RISC should also inform the MRC and Board of its actions.

Figure 2: Proposed Front-End Process Flowchart (pathway for the Reliability Issues Steering Committee – RISC)



Recommendation 3: Interface with Regulatory and Governmental Authorities

Issue

How can NERC improve the communication and awareness of NERC's strategic initiatives on major risks to reliability to increase alignment of NERC with the concerns of state, federal, and provincial authorities?

Recommendation

The Board is encouraged to task NERC management, working with a broad array of ERO resources (e.g., MRC, technical committees, Regional Entities, trade associations, etc.) to develop a strategy for improving the communication and awareness of effective reliability risk controls which increases input and alignment with state, federal, and provincial authorities.

Proposed Details

- Interface with governmental authorities to align priorities and timing of reliability initiatives. Establish and align priorities early on during the nomination of the reliability issue.
- Develop methods to effectively communicate progress and manage expectations.
- Promote effective rules of engagement of state, federal, and provincial regulatory staff in accordance with jurisdictional requirements.
- Following successful ballot of standard and approval by the Board, pre-filing meetings will be held with FERC staff and individual Commissioners to help ensure FERC approval without conditions; and similar efforts will apply with governmental authorities in Canada.

Additional Issues to be Addressed (per the Board's Discretion) During the Implementation Phase

- Responsibility for managing the details above, concerning progress and expectations.
- Encourage regulatory authorities to permit staff to submit written comments to the drafting team during informal and formal comment periods.

Background

The SPIG provides as additional reference and guidance the [Roles and Responsibilities: Standards Drafting Team Activities](#), approved by the SC in July 2011, includes the following policy guidance, approved by the NERC Board at its October 29, 2008 meeting, to guide standard drafting teams' responses to regulatory authority staff involvement in standard drafting activities:

- a. The standard drafting team has sole responsibility for drafting and approving the language in the proposed standards that are presented to the SC for ballot.

- b. NERC and the SC support the involvement of regulatory authority staff in all standards drafting team activities, where permitted by law.
- c. NERC recognizes that regulatory authority staff does not speak for the regulatory authority itself and, as such, the input they provide is considered advice.
- d. In the event regulatory authority staff does choose to participate in drafting team activities, they should be treated as any non-voting observer or participant.
- e. Standard drafting team members should seek out the opinion of regulatory authority staff, consider the regulatory staff input on its technical merits, and respond to written comments offered during a public posting period as it would seek opinions from, consider the technical merits of, and respond to comments offered by other industry stakeholders.
- f. To the extent that regulatory authority staff advice is offered to the drafting team (or members thereof) in a forum that is not public and open to all industry participants, the standard drafting team should consider the input as advice.
- g. If the team chooses to act on regulatory authority staff advice offered in a non public forum, the standard drafting team chair should either:
 - Request the regulatory authority staff to provide the advice during an open meeting or conference call of the drafting team; or,
 - Document his/her understanding of the issues or advice presented, and include the information in an open industry comment period with the accompanying changes to the proposed standards.

Recommendation 4: Standards Product

Issue

How will standards be developed to effectively achieve reliability objectives through clear, high quality Results-Based Standards (RBS) requirements in a cost effective manner?

Recommendation:

The Board is encouraged to require that the standards development process address:

- *The use of RBS;*
- *Cost effectiveness of standards and standards development;*
- *Alignment of standards requirements/measures with Reliability Standards Audit Worksheets (RSAWs); and*
- *The retirement of standards that are no longer needed to meet an adequate level of reliability.*

Proposed Details

- Utilize RBS model as the basis for all standards.
 - i. Evaluate all existing standards and revise to meet format of RBS.
 - ii. Retire any existing standards that are not chosen to be modified into a RBS format per Board approval.
 - iii. Develop all new standards in RBS format.
- Ensure cost effectiveness of standards through documentation of alternatives analysis.
- Include cost impact/reliability benefit analysis in the final standards package posted for ballot.
- Ensure clarity on reliability objectives and compliance obligations.
 - i. SDT is responsible for the development of the standard including requirements and measures.
 - ii. Compliance staff will develop RSAWs (that will be used in the auditing of compliance) in conjunction and coincident with the development of the standard.
 - iii. Post entire package for stakeholder comment, including standards and RSAWs (RSAWs are not balloted).
 - iv. Changes to RSAWs after the ballot body develops measure/standard require Board approval.
- Revise Essential Elements of the Standards Template to eliminate redundancies such as Violation Severity Levels (VSLs).
- Consider “applicability” provisions and criteria for those most impacted by implementing a standard.

Additional Issues to be Addressed (per the Board’s Discretion) During the Implementation Phase

- Establish process to consider elimination of standards and standards requirements that have minimal value.
 - i. The recent FERC Find, Fix, Track and Report (FFTR) Order encourages the reduction of unnecessary requirements and a structured process needs to be developed to achieve this.
 - ii. Additional options may include a task to the RISC, Operating Committee, or Planning Committee, as determined by the Board.

Recommendation 5: Standards Development Process and Resources

Issue

How can the existing standards development process be improved upon and streamlined and how can resources be better utilized to ensure effective, efficient, and expeditious standards development?

Recommendation

The Board is encouraged to require the standards development process be revised to improve timely, stakeholder consensus in support of new or revised reliability standards. The Board is also encouraged to require standard development resources to achieve and address:

- *Formal and consistent project management*
- *Efficient formation and composition of SDTs*

Proposed Details

- The drafting team will post responses to each comment received during the *final*, formal comment period prior to the recirculation ballot. For other postings, there is no ANSI requirement to post responses to the comments.
- Modify the comment process to:
 - i. Bundle responses to comments.
 - ii. SDT will post draft standard for informal comment period of 30 days, but not be required to respond to comments.
 - iii. Promote an automated system for managing comments.
 - iv. Conduct industry webinars between successive ballots to enhance understanding of issues and facilitate consensus.
 - v. Facilitate consensus by encouraging industry collaboration and submittal of coordinated comments through Regional Entities and trade groups.
- Ballot process shall:
 - i. Use all votes cast by ballot pool member to establish quorum.
 - ii. Provide options for voting “No” with guiding choices for the answer with a comment section on the ballot.
- Formalize the use of formal, rigorous project management (i.e., trained leaders, facilitators, scribes, etc.) within SDTs to ensure greater efficiency and effectiveness of the SDTs.
- Revise formation and composition of SDTs model.
 - i. Incorporate the support of technical writers, legal, compliance and rigorous and highly trained facilitation support.

- ii. Ensure adequate representation and competencies based on complexity of the issue.
- Promote efficiency and timeliness by setting milestones and progress reports.

Additional Issues to be Addressed (per the Board’s Discretion) During the Implementation Phase

- Reinforce mechanisms to add during the commenting process.
 - i. Locked list of answer options (e.g., “risk to reliability,” “cost concerns,” etc.).
 - ii. “Other” option for the No vote list with a comment section that requires explanation that this approach will balance input to empower the SC to conduct a more thorough balloting process.
 - iii. Consider bolding of text instructions on all ballots that emphasize the importance of clarity.
 - iv. Consider the advantage/disadvantage to establishing voting record for each participant/entity.

2012 State of Reliability Report

Action

Review and accept.

Background

The NERC *2012 State of Reliability* report continues to evolve from the 2011 foundational report, *2011 Risk Assessment of Reliability Performance*.¹ The 2012 report was prepared by the NERC Performance Analysis Subcommittee² (PAS) under the direction of the Planning Committee and NERC staff in collaboration with many technical groups,³ analyzing specific indications of bulk power system reliability, including the:

- Operating Committee:
 - Resources Subcommittee (RS)
 - Frequency Working Group (FWG)
 - Operating Reliability Subcommittee (ORS)
- Planning Committee
 - Reliability Assessment Subcommittee (RAS)
 - System Protection and Control Subcommittee (SPCS)
 - Event Analysis Working Group (EAWG)
 - Transmission Availability Data System Working Group (TADSWG)
 - Generating Availability Data System Working Group (GADSWG)
 - Demand Response Availability Data System Working Group (DADSWG)

The goal of this report is to objectively review and assess the state of reliability based on metric trends to provide an integrated view of reliability performance. The key findings and recommendations serve as technical input to NERC's Reliability Standards and project prioritization, compliance operations process improvement, event analysis, reliability assessment, and critical infrastructure protection.

Among the 18 metrics that address the characteristics of an adequate level of reliability (ALR), trends indicate the bulk power system has been performing consistently well. There are no significant upward or downward trends from 2008 to 2011. Based on the data and its analysis, the following six key findings were identified:

1. Bulk power system reliability remains adequate.
2. Frequency response performance appears flat with no deterioration.
3. Protection system misoperations are a significant reliability issue.

¹ http://www.nerc.com/files/2011_RARPR_FINAL.pdf

² <http://www.nerc.com/filez/pas.html>

³ <http://www.nerc.com/page.php?cid=1|117>

4. Equipment failure appears to be a significant reliability issue.
5. Wind generation and demand response growth call for performance assessment.
6. More data, time and research is needed to produce deeper understanding of root causes for significant reliability issues and develop effective action steps.

Severe Impact Resilience: Considerations and Recommendations Report

Action

Review and accept the *Severe Impact Resilience: Considerations and Recommendations* report prepared by the Severe Impact Resilience Task Force (SIRTF) as part of the *Coordinated Action Plan*¹ to address high-impact, low-frequency (HILF) risks.

Background

To help the electricity industry better understand HILF risks, NERC and the U.S. Department of Energy (DOE) issued a report titled, "*High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*"². In November 2010, the NERC Board of Trustees approved a *Coordinated Action Plan* under the leadership of the NERC Technical Committees to establish four task forces to address this work. The *Severe Impact Resilience: Considerations and Recommendations* report provides the conclusions of one of the task forces, the SIRTF.

The report provides guidance to industry asset owners and operators (entities) in the form of recommendations to enhance the resilience of the bulk power system (BPS). Three HILF scenarios were specifically considered as the initiating events, but the recommendations in this report may be applicable to any severe-impact scenario.

- **Coordinated physical attack** – A coordinated physical attack on key nodes of the BPS critically disables difficult to replace equipment in multiple generating stations or substations and could have a significant effect on the remainder of the system. A prolonged period of time is required to fully restore the BPS to normal operation.
- **Coordinated cyber attack** – A coordinated disruption disables or impairs the integrity of multiple control systems, or intruders take operating control of portions of the BPS such that generation or transmission system is damaged or mis-operated.
- **Geomagnetic disturbance**³ – A severe geomagnetic disturbance damages difficult to replace generating station and substation equipment and causes a cascading effect on the remainder of the system. A prolonged period of time is required to fully restore the BPS to normal operation.

The guidance offered in this report reaches beyond the emergency response capabilities entities typically have in place. To emphasize this, the SIRTF developed two important concepts that run throughout this report; Severe Event and New Normal. A Severe Event is an emergency situation so catastrophic that complete restoration of electric service is not possible and the BPS is operated at a reduced state of reliability and supply for months or possibly years through a New Normal period.

The suggestions offered throughout this report are intended to prompt entities to develop their own approaches and flexible plans that would be applicable under a wide variety of

¹ Ref. Coordinated Action Plan

http://www.nerc.com/docs/ciscap/Critical_Infrastructure_Strategic_Initiatives_Coordinated_Action_Plan_BOT_Apprd_11-2010.pdf

² Ref. High Impact Low Frequency report <http://www.nerc.com/files/HILF.pdf>

³ Ref. *Interim Report: Effects of Geomagnetic Disturbances on the Bulk Power System* <http://www.nerc.com/files/2012GMD.pdf>. This report concluded that the loss of reactive power is the most likely outcome from a severe solar storm centered over North America.

circumstances. The report offers 33 key recommendations that are of a planning and operational nature, and entities are strongly encouraged to consider these from a strategic and leadership perspective, in particular:

- Enhance existing restoration drills and exercises to incorporate HILF scenarios that include interdependencies with other critical infrastructures such as telecommunications.
- Recognize that plans and operating practices will need to be continually assessed and adjusted as necessary over an extended period that could last months or years following a Severe Event.
- Involve neighboring jurisdictions and government agencies by sharing plans and building a better understanding of how these plans will be coordinated and implemented.

While the majority of the recommendations are intended for entity consideration, the NERC Operating Committee has identified several for further action. These efforts will be coordinated with the other Technical Committees and the Electricity Sub-sector Coordinating Council.

The *Severe Impact Resilience: Considerations and Recommendations* report has been reviewed and approved by the Operating Committee, Planning Committee, and Critical Infrastructure Protection Committee. The Electricity Sub-sector Coordinating Council has also endorsed the report.

Severe Impact Resilience: Considerations and Recommendations

Severe Impact Resilience Task Force

FINAL DRAFT

NOTE

This document is a final draft for approval by NERC's Technical Committees.

Following Technical Committee approval, NERC's Board of Trustees will be asked to endorse the report.

RELIABILITY | ACCOUNTABILITY



NERC's Mission

The North American Electric Reliability Corporation (NERC) is an international regulatory authority established to enhance the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; assesses adequacy annually via a 10 year forecast and winter and summer forecasts; monitors the BPS; and educates, trains, and certifies industry personnel. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the U.S. Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada.¹

NERC assesses and reports on the reliability and adequacy of the North American BPS, which is divided into eight regional areas, as shown on the map and table below. The users, owners, and operators of the BPS within these areas account for virtually all the electricity supplied in the U.S., Canada, and a portion of Baja California Norte, México.



FRCC Florida Reliability Coordinating Council	SERC SERC Reliability Corporation
MRO Midwest Reliability Organization	SPP Southwest Power Pool, Incorporated
NPCC Northeast Power Coordinating Council	TRE Texas Reliability Entity
RFC ReliabilityFirst Corporation	WECC Western Electricity Coordinating Council

Note: The highlighted area between SPP and SERC denotes overlapping regional area boundaries: For example, some load serving entities participate in one region and their associated transmission owner/operators in another.

¹ As of June 18, 2007, the U.S. Federal Energy Regulatory Commission (FERC) granted NERC the legal authority to enforce Reliability Standards with all U.S. users, owners, and operators of the bulk power system, and made compliance with those standards mandatory and enforceable. In Canada, NERC presently has memorandums of understanding in place with provincial authorities in Ontario, New Brunswick, Nova Scotia, Québec, and Saskatchewan, and with the Canadian National Energy Board. NERC standards are mandatory and enforceable in Ontario and New Brunswick as a matter of provincial law. NERC has an agreement with Manitoba Hydro making reliability standards mandatory for that entity, and Manitoba has recently adopted legislation setting out a framework for standards to become mandatory for users, owners, and operators in the province. In addition, NERC has been designated as the “electric reliability organization” under Alberta’s Transportation Regulation, and certain reliability standards have been approved in that jurisdiction; others are pending. NERC and NPCC have been recognized as standards-setting bodies by the Régie de l’énergie of Québec, and Québec has the framework in place for reliability standards to become mandatory. NERC’s reliability standards are also mandatory in Nova Scotia and British Columbia. NERC is working with the other governmental authorities in Canada to achieve equivalent recognition.

Table of Contents

- Table of Contents ii
- 1.0 Executive Summary 1
 - Understanding a Severe Event..... 2
 - Enhancing Resilience..... 2
 - Recommendations 2
 - Operations 3
 - Monitoring the BPS..... 4
 - Communications 4
 - Short-term and Long-term System Planning 4
 - Protection and Control 5
 - Interdependencies with Other Critical Infrastructures 5
 - Coordination with Government..... 5
 - Taking Care of People 6
 - Logistics and Self-Sustained Operations..... 6
 - Preventing and Responding to Physical Attacks..... 6
 - Emergency Financing 6
 - Conclusions 7
 - Recommendations for Entity Action..... 7
 - NERC’s Reliability Standards under a Severe Event..... 7
 - Acknowledgements..... 8
- 2.0 Introduction 9
 - 2.1 Background and Key Concepts..... 10
 - 2.1.1 Use of Terms 10

2.1.2 Understanding a Severe Impact Event	10
2.1.3 Impact of a Severe Event on the BPS.....	10
2.1.4 Impact of a Severe Event on Society	11
2.1.5 Understanding Resilience	11
2.1.6 Understanding the New Normal.....	14
2.1.7 New Normal Challenges.....	16
2.1.8 The Applicability of NERC Standards During a Severe Event.....	17
3.0 Operations.....	18
3.1 Immediate Automatic Response.....	19
3.2 Operational Authority.....	20
3.3 Initial Operator Response	21
3.4 Island Stability	23
3.5 Load Shedding.....	25
3.6 Generation Dispatch and Automatic Generation Control (AGC).....	28
3.7 Variable Generation	29
3.8 Training	30
4.0 Monitoring the BPS.....	31
4.1 Generator Output	32
4.2 Operating Limits.....	33
4.3 Monitor Flows on BPS Facilities	34
4.4 Loss of Control Centers – Both Primary and Backup	36
5.0 Communications	39
5.1 Communications Relationships.....	40
5.2 General Communications Recommendations	41
5.3 Communication Protocol Recommendations:.....	44

5.4 Emerging Technology Recommendations	45
6.0 Short-term and Long-term System Planning	47
6.1 Consequences of a Severe Event on System Planning Functions.....	48
6.2 Planning During the Mitigation Phase	49
6.3 System Planning during the Return to Normal Phase	51
6.4 Design Considerations	51
7.0 Protection and Control.....	54
7.1 Preparation Phase.....	55
7.2 Mitigation Phase	57
7.3 Restoration Phase	58
7.4 Training	60
8.0 Interdependencies with Other Critical Infrastructures	62
8.1 Communications Sector	64
8.2 Dams (hydroelectric) Sector	65
8.3 Energy Sector	65
8.4 Information Technology Sector	66
8.5 Nuclear Sector.....	67
8.6 Transportation Sector	68
8.7 Critical Infrastructure Sectors that Depend on Electricity.....	69
9.0 Coordination with Government.....	71
9.1 Overview of Government Authorities	71
9.2 Coordination and communications prior to an event: planning, exercising, and training	72
9.3 Initial Communication And Coordination	74
9.4 Coordination and Communication During Restoration	75
10.0 Taking Care of People	77

10.1 Accommodation.....	77
10.2 Safety Considerations	78
10.3 Employee and Family Issues	79
10.4 Respite Facilities.....	80
10.5 Counseling.....	81
11.0 Logistics and Self Sustained Operations	83
11.1 Specialized Equipment.....	83
11.2 Standard Equipment	84
11.3 Fuel for Transportation and Backup Generators	85
11.4 Transportation Routes	86
11.5 Personnel and Facility Resources.....	86
12.0 Preventing and Responding to Physical Attacks.....	89
12.1 Challenges to Protecting the BPS.....	90
12.2 Recommended Prevention Strategies	90
12.3 Recommended Preparation Strategies.....	91
12.4 Recommendations for Response and Mitigation Strategies	95
12.5 Recommendations for Restoration Strategies	96
13.0 Financing Emergency Operations	97
13.1 Getting Prepared for Emergency Financing.....	98
Appendix 1: Task Force Scope	100
Appendix 2: Mitigations for Monitoring the BPS.....	104
Appendix 3: Mitigations for Physical Attacks	113
Appendix 4: Resilience Discussion Worksheet	114
Introduction	114
Decision Making.....	114

Business Continuity and Restoration Plans	115
Operations	117
Logistics and Interdependencies	119
Financing	121
Appendix 5: Severe Event Response Checklist	122
System Topology	122
Generation	123
Transmission Lines and Substations	123
Key Equipment	123
Communications	124
Monitoring	125
Financing	125
Appendix 6: NERC SIRTf Roster	126
Appendix 7: NERC SIRTf Report Drafting Team.....	132

1.0 Executive Summary

The North American bulk power system (BPS) is one of the most critical of infrastructures, vital to society in many ways, but it is not immune to severe disruptions that could threaten the health, safety, or economic well-being of the citizens it serves. The electric power industry has well established planning and operating procedures in place to address “normal” emergency events (e.g., hurricanes, tornadoes, ice storms) that occur from time to time and disrupt electric reliability. However, the electricity industry has much less experience with planning for and responding to high-impact events that have a low probability of occurring.

To help the electricity industry better understand these low probability risks, NERC and the U.S. Department of Energy (DOE) issued a report titled, “High-Impact, Low-Frequency (HILF) Event Risk to the North American Bulk Power System”². Subsequently, the NERC Board of Trustees approved a Coordinated Action Plan under the leadership of the NERC Technical Committees to establish four Task Forces to address this work. This report provides the conclusions of the Severe Impact Resilience Task Force (SIRTF).

The report provides guidance to industry asset owners and operators (entities) in the form of recommendations to enhance the resilience of the bulk power system. Three severe-impact HILF scenarios were specifically considered as the initiating events, but the recommendations in this report may be applicable to any scenario.

- **Coordinated physical attack** – A coordinated physical attack on key nodes of the BPS critically disables difficult to replace equipment in multiple generating stations or substations and could have a significant effect on the remainder of the system. A prolonged period of time is required to fully restore the BPS to normal operation.
- **Coordinated cyber attack** – A coordinated disruption disables or impairs the integrity of multiple control systems, or intruders take operating control of portions of the BPS such that generation or transmission system is damaged or mis-operated.
- **Geomagnetic disturbance** – A severe geomagnetic disturbance damages difficult to replace generating station and substation equipment and causes a cascading effect on the remainder of the system. A prolonged period of time is required to fully restore the BPS to normal operation.

The report offers 33 key recommendations that are of a planning and operational nature, and entities are strongly encouraged to consider these from a strategic and leadership perspective, in particular:

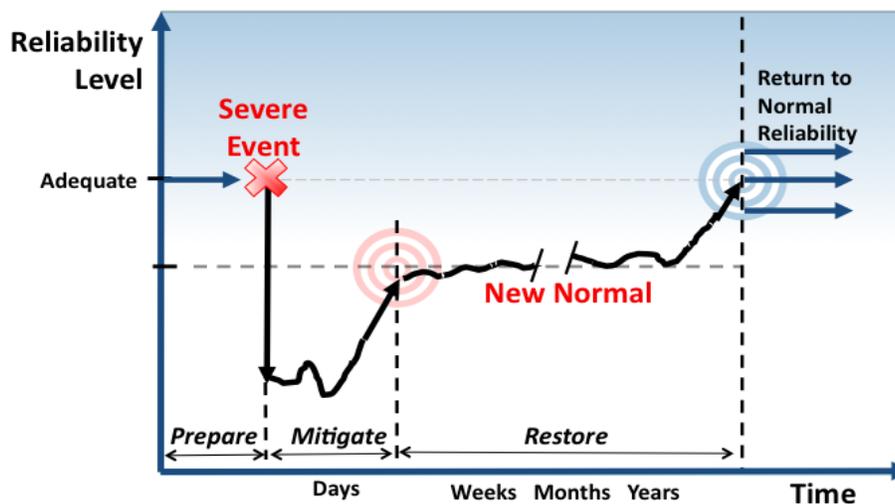
- Enhance existing restoration drills and exercises to incorporate HILF scenarios that include interdependencies with other critical infrastructures such as telecommunications.

² Ref. High Impact Low Frequency report <http://www.nerc.com/files/HILF.pdf>

- Recognize that plans and operating practices will need to be continually assessed and adjusted as necessary over an extended period that could last months or years following a severe event.
- Involve neighboring jurisdictions and government agencies by sharing plans and building a better understanding of how these plans will be coordinated and implemented.

Understanding a Severe Event

The guidance offered in this report is intended to reach beyond the emergency response capabilities entities typically have in place. To emphasize this, the SIRTf developed two important concepts that run throughout this report; Severe Event and New Normal. A Severe Event is an emergency situation so catastrophic that complete restoration of electric service is not possible. The BPS is operated at a reduced state of reliability and supply for months or possibly years through the New Normal period as illustrated below.



Enhancing Resilience

By definition, a Severe Event will present enormous challenges as entities within the electricity industry strive to restore and maintain reliable operations under rapidly changing circumstances never before experienced. It will not be possible to meet all electricity consumers' demands for rapid restoration of service as entities prioritize their work with limited resources. The recommendations and suggestions offered throughout this report are intended to prompt BPS entities to develop their own approaches and flexible plans that would be applicable under a wide variety of circumstances. These suggestions are in the form of industry guidelines that describe practices that may be used by individual entities according to local circumstances, as opposed to standards.

Recommendations

The SIRTf has considered what aspects of emergency operation and restoration would be particularly challenged through a Severe Event and considered options to enhance the resilience of the BPS. Entities are encouraged to consider how they might apply the

recommendations offered in this report to their own circumstances in a Severe Event scenario. Entities are encouraged to test their plans through drills or exercises that build further on the Severe Event scenarios.

The following summarizes the key recommendations of this report and are described in the body of the report in further detail.

Operations

The Operations section of this report discusses the many challenges associated with operating the BPS following a Severe Event. Rather than operating as part of a large interconnected (and therefore more stable) grid, system operators may need to manage a number of small electrical islands and implement load shedding or rotating blackouts for extended periods of time (weeks, months or years). The Operations section proposes that entities consider the following key recommendations.

1. Consider which entities would take the independent actions and the tools needed to stabilize islands when communications capability is severely disrupted or unavailable.
2. Consider how operating reserve would be managed during islanded operation and frequent periods of insufficient supply to meet demand.
3. Consider ways to adopt and apply the terms critical load and priority load across all BPS entities to improve consistent use during a Severe Event.
4. Consider alternate means to dispatch generation if normal automated systems, including automatic generation control, are unavailable.
5. Consider if or how variable generation would be dispatched through restoration and islanded operation.
6. Consider enhancing regular restoration drills and exercises to train staff on communication protocols and independent control actions in the event of loss of or degraded telecommunications.
7. Consider using more extreme exercise scenarios that involve simulated rotating blackouts and islanded operations on a larger scale and for extended periods of time.

Monitoring the BPS

The Monitoring the BPS section discusses the challenges associated with maintaining situational awareness in order to operate the BPS following a Severe Event. A Severe Event may disrupt the flow of data, tools, or facilities needed to operate the BPS. Alternate mechanisms and processes would be needed to maintain a wide area view of situational awareness when it is more important than ever. The Monitoring the BPS section proposes that entities consider the following key recommendations.

8. Consider developing processes to quickly study island configurations and develop suitable temporary operating limits.
9. Consider developing processes to monitor BPS flows in the absence of reliable automated systems and communications.
10. Consider the simultaneous loss of primary and backup control centers and how essential functions will continue to be performed.

Communications

The Communications section discusses the challenges associated with restoring and operating the BPS when communications facilities are severely degraded or unavailable. The Communications section proposes that entities consider the following key recommendations.

11. Consider installing renewable generation (e.g., wind, solar) at critical BPS facilities to supplement standby generators.
12. Consider alternate means to communicate when primary means of communication are completely unavailable for extended periods of time.
13. Consider robust training, drills, and exercises to fully test critical restoration steps using alternative voice and data communications (e.g., satellite telephones).

Short-term and Long-term System Planning

The Short-term and Long-term System Planning section discusses the challenges associated with providing sufficient personnel and facilities to prepare the necessary system studies and plans needed to support restoration and long-term recovery. This section proposes that entities consider the following key recommendations.

14. Consider the potential loss of planning resources (e.g., equipment, data) as well as damage to the system. Review business continuity plans to ensure that system planning resources are adequately considered.
15. Consider the appropriate use of key system planners who may be required immediately, and for prolonged periods, to perform studies not previously considered.
16. Consider performing selected studies in advance (e.g., equipment interchangeability) that could help speed restoration.
17. Consider the spare equipment critical to BPS restoration and ways to improve availability of these spares.

Protection and Control

The Protection and Control section discusses the challenges associated with safely operating the BPS as its configuration continues to change to respond to the loss or unavailability of critical elements. This section proposes that entities consider the following key recommendations.

18. Consider ways to implement large-scale changes in system protection schemes to support islanded operation and changing BPS configurations, and what decision points would be needed.
19. Consider ways to quickly reconfigure relay settings in the event large-scale changes are needed.

Interdependencies with Other Critical Infrastructures

The Interdependencies with Other Critical Infrastructures section discusses the contribution and impact that other industries such as communications, oil and natural gas, and water have on the ability of the electricity industry to restore and operate the BPS. This section proposes that entities consider the following key recommendations.

20. Consider working with communications service providers to identify which of their facilities are critical to BPS operations. Determine which BPS and distribution facilities supply them and what backup power capacity is in-place (e.g., batteries, standby generators).
21. Consider alternate suppliers, transportation paths, and agreements to support generating station fuel supply chains (e.g., coal, natural gas).
22. Consider working with information technology service providers that are critical to BPS operations and consider augmenting the subject matter expertise of staff and suppliers to support these systems.
23. Consider alternate means to supply BPS power to nuclear plants and confirm these loads as critical to restoration and public safety.

Coordination with Government

The Coordination with Government section discusses the need to build effective relationships with the appropriate government agencies in order to help manage serious public health and safety issues. This section proposes that entities consider the following key recommendations.

24. Confirm the roles, authorities, and points of contact between BPS entities and as appropriate, local, state/provincial, and federal governments.
25. Coordinate with local and state/provincial government authorities and consumer stakeholders to identify priority loads to mitigate the impact on public health and safety.
26. Consider developing a list of regulatory exemptions or waivers that will materially improve restoration and operation (e.g., plant emissions, truck driver hours) and consult with state/provincial and federal agencies.

Taking Care of People

The Taking Care of People section discusses how entities can assist with the extraordinary demands that employees and their families may face. This section proposes that entities consider the following key recommendation.

27. Consider ways to support the health, safety, and well-being of personnel and their families in the face of extraordinarily demanding circumstances.

Logistics and Self-Sustained Operations

The Logistics and Self-Sustained Operations section discusses the challenges associated with the logistics of acquiring the equipment needed to restore and operate the BPS. This section proposes that entities consider the following key recommendations.

28. Consider with fuel suppliers ways to prioritize the supply and delivery of fuel for emergency standby generators and essential work vehicles.
29. Consider how your business continuity or disaster recovery plan would change if you are unable to rely on mutual support arrangements.

Preventing and Responding to Physical Attacks

The Preventing and Responding to Physical Attacks section discusses the unique challenges associated with physical attacks. This section proposes that entities consider the following key recommendations.

30. Consider actions that can be taken to protect BPS assets by involving local communities and law enforcement (e.g., reinforcing their awareness of BPS facilities that are critical to operations).
31. Consider ways to improve security when designing or refurbishing existing BPS facilities.
32. Consider ways to improve coordination and cooperation with local/state/provincial law enforcement.

Emergency Financing

The Emergency Financing section briefly discusses the challenges associated with the extraordinary requirements for funds needed to restore the BPS when major facilities need to be rebuilt or replaced. This section proposes that entities consider the following key recommendation.

33. Consider how extreme financial challenges will be addressed in consultation with financial institutions, suppliers, and government agencies.

Conclusions

This report addresses important aspects related to enhancing the resilience of the BPS in the face of a Severe Event. It provides entities with practical options to enhance their capabilities to prepare, mitigate and restore the operation of the BPS.

Recommendations for Entity Action

This report examines the aspects of emergency operation and restoration that would be particularly challenged through a Severe Event and provides options to enhance the resilience of the BPS. The suggestions offered throughout this report are intended to prompt entities to develop their own approaches and flexible plans that would be applicable under a wide variety of circumstances. This report considers all aspects of resilience; robustness, resourcefulness, rapid recovery, and adaptability. Entities are encouraged to critically examine their current capabilities, and to consider what else they may need to do to manage restoration and operations during a Severe Event.

While the report offers 33 key recommendations that are of a planning and operational nature, entities are strongly encouraged to consider these from a strategic and leadership perspective, in particular:

- Enhance existing restoration drills and exercises to incorporate Severe Event scenarios that include interdependencies with other critical infrastructures such as telecommunications.
- Recognize that plans and operating practices will need to be continually assessed and adjusted as necessary over an extended period that could last months or years following a severe event.
- Involve neighboring jurisdictions and government agencies by sharing your plans and building a better understanding of how these plans will be coordinated and implemented.

NERC's Reliability Standards under a Severe Event

While this report does not propose that new standards be developed to address a Severe Event, as entities consider and implement the recommendations in this report there may be opportunities to enhance existing standards.

The SIRTf discussed the applicability of the NERC³ standards through a Severe Event, and whether entities should be exempt from possible compliance actions⁴ under these circumstances. The SIRTf reviewed the NERC standards and concluded that standards support safe and reliable operation and should be applicable during a Severe Event. While it is conceivable that during a Severe Event an entity will violate certain standard requirements given the intensity of planning and operating challenges through the New Normal period, it would be impossible to predict these circumstances in advance.

³ Ref. NERC Standards, <http://www.nerc.com/page.php?cid=1|7>

⁴ NERC has the legal authority to enforce compliance with NERC Reliability Standards, which it achieves through a rigorous program of monitoring, audits and investigations, and the imposition of financial penalties and other enforcement actions for non-compliance.

On balance, the SIRTF concluded that entities do not need guidance on the applicability of standards during a Severe Event. Although a Severe Event may put entities in a position where they cannot comply with all standards, entities are in the best position to “do the right thing” for reliability and public safety, and self-report any violation of NERC standards as time and circumstances permit.

Acknowledgements

This report was prepared by a team of industry subject matter experts with a broad understanding of what is needed to respond to emergency situations to reliably restore and operate the interconnected bulk power system. They contributed their knowledge, experience, and time to the SIRTF in technical areas such as power system operation, transmission planning, generating plant operation, protection and control, distribution operations, communications, logistics, emergency planning, crisis response, and cyber and physical security.

Members of the SIRTF Report Drafting Team are identified in Appendix 7 of this report.

Many other SIRTF members provided valuable feedback and are identified in Appendix 6.

2.0 Introduction

The North American bulk power system (BPS) is one of the most critical of infrastructures and is vital to society in many ways. The electric power industry has well established planning and operating procedures in place to address the “normal” emergency events (e.g., hurricanes, tornadoes, ice storms) that occur from time to time and disrupt electricity reliability⁵. However, the electricity industry has much less experience with planning for and responding to high-impact events that have a low probability of occurring or have not yet occurred.

To help the electricity industry better understand these low probability risks, in June 2010, NERC and the U.S. Department of Energy issued a report titled, “*High-Impact, Low-Frequency Event Risk to the North American BPS*”⁶. In November 2010, the NERC Board of Trustees (BOT) approved the Electricity Sub-sector Coordinating Council’s (ESCC) *Critical Infrastructure Strategic Roadmap*⁷ that provides the framework to identify the actions needed to enhance reliability and resilience under these high-impact low-frequency (HILF) scenarios. At the same time, the BOT approved a *Coordinated Action Plan*⁸ developed by NERC and the leadership of the NERC Technical Committees that identifies specific initiatives, key deliverables, and milestones to implement the ESCC’s Strategic Roadmap. The Coordinated Action Plan identified four task forces needed to address this work. This report provides the conclusions of one of them – the SIRTF.

The SIRTF was established in December 2010 by the NERC Operating Committee (OC) to develop guidance and options to enhance the resilience of the BPS to withstand and recover from three severe-impact HILF scenarios:

- Coordinated physical attack
- Coordinated cyber attack
- Geomagnetic disturbance

This effort has challenged the SIRTF in a number of ways.

- The industry has already demonstrated its ability to respond to large-scale emergencies such as the 2003 Northeast Blackout, Hurricane Katrina and more recently Hurricane Irene using flexible response plans that are designed to be effective regardless of the cause or consequences of the event. As a result, some entities may feel they are already prepared and nothing more needs to be done.
- By definition, HILF events have rarely or never occurred, and therefore it is very difficult to determine with confidence what additional action is required even by industry experts who are responsible for planning and operating the BPS through extreme emergency

⁵ Ref. NERC Adequate Level of Reliability http://www.nerc.com/docs/standards/Adequate_Level_of_Reliability_Defintion_05052008.pdf

⁶ Ref. High Impact Low Frequency report <http://www.nerc.com/files/HILF.pdf>

⁷ Ref. Critical Infrastructure Strategic Roadmap http://www.nerc.com/docs/escs/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf

⁸ Ref. Coordinated Action Plan http://www.nerc.com/docs/ciscap/Critical_Infrastructure_Strategic_Initiatives_Coordinated_Action_Plan_BOT_Apprd_11-2010.pdf

events. The Tohoku, Japan earthquake and tsunami that devastated the Fukushima nuclear plant is a vivid reminder that HILF events can occur.

- The postulated HILF events could cause service disruptions lasting weeks, months and perhaps years – well beyond the industry’s experience over the past 100 years of reliable operation.

The SIRTF has recognized these challenges and through this report offers the electricity industry a wide range of suggestions and ideas. The diverse nature of HILF events does not lend itself to technical engineering solutions broadly applicable across the electricity industry. Therefore, the report does not propose mandatory requirements. Instead, the report offers suggestions and ideas to entities that own or operate the BPS. Entities are encouraged to consider these suggestions and apply them according to their own local circumstances and needs.

The SIRTF considered what aspects of emergency operation and restoration would be particularly challenged through these severe-impact events, and considered options to enhance the resilience of the BPS. In many cases, the suggestions can be applied to any HILF scenario, regardless of the specific threat.

2.1 Background and Key Concepts

At an early stage in its work, it became apparent that SIRTF members had different experiences and therefore no common view of what is meant by terms such as “severe impact” event, “resilience”, and “New Normal” operation. The SIRTF needed to define these terms so that members would have a common platform from which to propose solutions that build on the electricity industry’s current ability to respond to emergencies and prepare for worse in a consistent manner.

2.1.1 Use of Terms

A number of technical terms related to the planning and operation of the BPS are used throughout this report. Please refer to the NERC Glossary of Terms⁹ for definitions.

2.1.2 Understanding a Severe Impact Event

A severe impact event (Severe Event) means that complete restoration is not possible and the BPS is operated at a reduced state of reliability and supply for an extended period of time, for months or possibly years – a New Normal. The following describes a Severe Event; one that stresses the electricity industry’s capabilities well beyond its already robust emergency response capabilities.

2.1.3 Impact of a Severe Event on the BPS

- The event is beyond the planning criteria provided by NERC planning standards¹⁰, such as System Performance Following Extreme BES Events.

⁹ Ref. NERC Glossary of Terms http://www.nerc.com/files/Glossary_12Feb08.pdf

¹⁰ Ref. NERC standard TPL-004, ref. <http://www.nerc.com/files/TPL-004-0.pdf>

- The event is beyond the scenarios typically exercised by entities as part of the NERC Emergency Preparedness and Operations standards¹¹.
- It is expected to take six months to a year to return the BPS to pre-event operations.
- As a result of insufficient generation and transmission resources, system operators must shed load without advanced notice and regularly implement rotating blackouts to manage BPS reliability.
- The duration and magnitude of these rotating blackouts have a direct societal impact and risk further degradation to the BPS as other critical infrastructures are affected by the electricity disruptions.
- Multiple information technology and communications systems have failed – entities contend with issues that restrict the ability of system operators to effectively communicate, operate, and monitor the BPS.
- The event is persistent or recurring throughout the mitigation and restoration phases, further hindering recovery and restoration.

2.1.4 Impact of a Severe Event on Society

- The media or government authorities describe the magnitude of the event using words such as “catastrophe”, “disaster” or “massive disruption”.
- BPS entity staff experience a high degree of physical and psychological demands for an extended period of time.
- The safety and well being of large numbers of the public, entity staff, or their families are at risk.
- The resources required to respond exceed the financial capacity of some entities.

2.1.5 Understanding Resilience

“Resilience” is generally defined as the ability to recover or adjust to misfortune or change. More specifically, the ASIS SPC.1-2009 standard on Organizational Resilience¹² defines, “Resilience is the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event.” In recent years, in the context of strategies needed to enhance the reliable operation of critical infrastructures, resilience has come to be valued as much as protection. But what exactly is meant by resilient critical infrastructures? How is resilience measured and how do we determine how much is needed?

Infrastructure Resilience

Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.

¹¹ NERC Emergency Planning and Operations standards, ref. <http://www.nerc.com/page.php?cid=2|20>

¹² ASIS SPC.1-2009, http://www.asisonline.org/guidelines/ASIS_SPC.1-2009_Item_No._1842.pdf

In October 2010, a study group¹³ of the National Infrastructure Advisory Council issued its report “*A Framework for Establishing Critical Infrastructure Resilience Goals*”¹⁴. The report provides a broader construct for resilience originally conceived by resilience expert Stephen Flynn. The construct is based on four features organized in a sequence of events prior to, during, and after a Severe Event.

¹³ The NIAC Study Group included a number of representatives from the electricity industry, including several members of the Electricity Sub-sector Coordinating Council.

¹⁴ Ref. <http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf>

Figure 1: NIAC Resilience Construct



Table 1: NIAC Resilience Construct

Sequence	Feature
Prior to an Event	Robustness —The ability to keep operating or to stay standing in the face of disaster. In some cases, it translates into designing structures or systems to be strong enough to take a foreseeable punch. In others, robustness requires devising substitute or redundant systems that can be brought to bear should something important break or stop working. Robustness also entails investing in and maintaining elements of critical infrastructure so that they can withstand low-probability but high-consequence events.
During an Event	Resourcefulness —The ability to skillfully manage a disaster as it unfolds. It includes identifying options, prioritizing what should be done both to control damage and to begin mitigating it, and communicating decisions to the people who will implement them. Resourcefulness depends primarily on people, not technology.
After an Event	Rapid recovery — The capacity to get things back to normal as quickly as possible after a disaster. Carefully drafted contingency plans, competent emergency operations, and the means to get the right people and resources to the right places are crucial. ¹⁵
At All Times	Adaptability — The means to absorb new lessons that can be drawn from a catastrophe. It involves revising plans, modifying procedures, and introducing new tools and technologies needed to improve robustness, resourcefulness, and recovery capabilities before the next crisis.

¹⁵ “Rapid” recovery as used by the SIRTf does not mean rapid recovery to the pre-crisis operational level but to the New Normal.

2.1.6 Understanding the New Normal

North America's BPS is one of the most reliable in the world. BPS owners and operators consistently demonstrate their ability to respond to emergencies and restore service under the most challenging and adverse circumstances.

The electricity industry makes extensive use of emergency and business continuity planning, risk modeling, supply chain management, accountable organizational structures, emergency exercises, tabletop drills, operator training, safety procedures, redundant and backup systems, mutual assistance, and effective operational communications protocols.

While this industry-wide capability has proven effective in responding to the "normal" emergencies we face from time to time, it is unlikely to be sufficient through a Severe Event. The SIRTf uses the term "New Normal" to describe degraded planning and operating conditions unlike anything the industry has ever experienced in North America that could exist for months or years.

Emergency Restoration

The entities that operate North America's BPS are well practiced in preparing for and responding to emergencies. North America experiences far more severe weather events such as hurricanes, tornadoes, and ice storms than any other continent. This challenge will continue, as extreme weather events appear to be increasing in both frequency and intensity.

Figure 2: Severe Event Phases

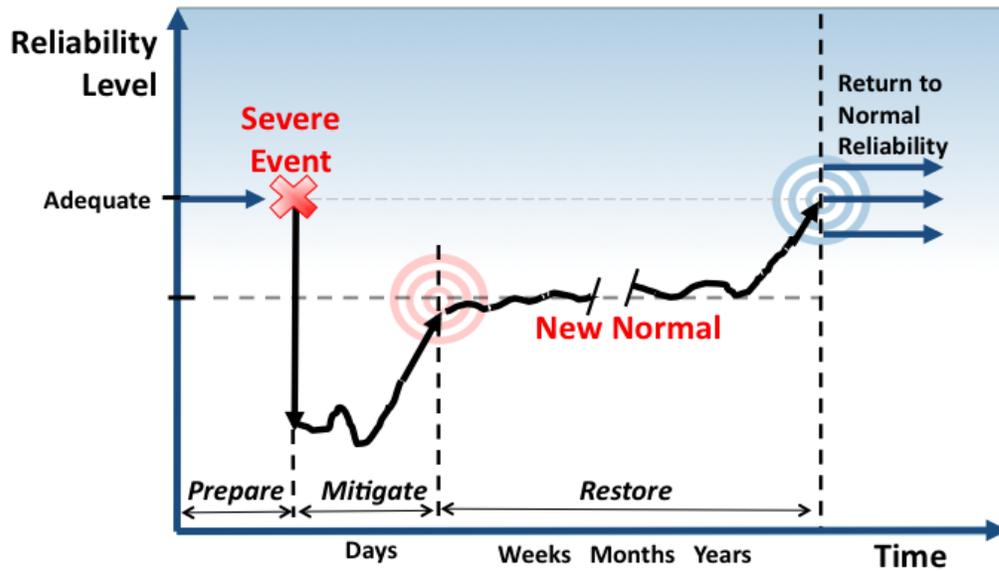


Table 2: Severe Event Phases

Phase	Duration	Characteristics
Prepare	At all times	Entities enhance existing and develop new emergency response capabilities.
Mitigate	Days	Entities implement plans to minimize the impact on BPS equipment and maximize electricity service to consumers. Resources such as reserve capacity, spare equipment, and personnel are inadequate to return the BPS to normal operation.
Restore	Weeks, months, possibly years	There is a risk that further Severe Events may occur. Resources such as personnel, spare equipment, and manufacturing capacity become increasingly limited. Other critical infrastructures are affected, reducing communications services and the availability of water, food, fuel, medical care, fire and police response. Over time, consumer load patterns change as people re-locate or implement their own energy solutions.
Return to Normal Reliability	Months, possibly years	Reliability may not return to pre-event levels. Lessons-learned from the event may eventually increase reliability in some areas as the BPS is reinforced, or decrease in other areas where consequences of the event continue to impose operational limitations.

2.1.7 New Normal Challenges

The following describes some of the challenges that would need to be managed through the weeks and months of New Normal operation. This is not an exhaustive list and is intended to illustrate conditions that owners and operators have not yet experienced and may have difficulty imagining.

- Although power is reliably restored to some consumers, planned and unplanned rotating blackouts disrupt service without warning as system operators manage BPS reliability with limited generation and transmission resources and unfamiliar operating conditions.
- Equipment damage and resource limitations force the BPS to be operated as a number of electrically disconnected islands, reducing the stability and reliability inherent in the large interconnected BPS.
- Other critical infrastructures are affected by electricity disruptions. For example, gasoline and diesel fuel shortages will occur as oil refineries take several days or longer to recover from each electricity service disruption.
- System operators need to dispatch generation and operate the transmission system manually using verbal direction that increases the likelihood of human error. Sporadic or limited electronic communications mean system operators need to rely on hardcopy documents that are less frequently updated.
- As a result of reduced generation and transmission resources and uncertain operating conditions, the BPS is operated with reduced efficiency and requires a larger margin of operating reserve, further aggravating the shortage of generation.
- Consumers experience large fluctuations in voltage and frequency that may trip sensitive electronic equipment.
- System protection devices configured for normal operation may be too restrictive for the voltage, current, and frequency variations inherent in a degraded operating state and would need to be adjusted to reflect these different operating conditions.
- Disrupted or unreliable automated trading or tagging systems limit the ability of balancing authorities and reliability coordinators to schedule and manage electricity flows between balancing areas.
- Extreme workload pressures on system operators, engineers, and other personnel limit the ability to meet certain standards requirements that do not compromise safe and reliable operations.

2.1.8 The Applicability of NERC Standards During a Severe Event

By definition, a Severe Event will present enormous challenges to electricity entities as they strive to restore and maintain reliable operations under rapidly changing circumstances never before experienced. It will not be possible to meet all electricity consumers' demands for early service restoration, as entities prioritize their work with limited human and material resources.

The SIRTF discussed the applicability of the NERC16 standards under these circumstances, and whether entities should be exempt from possible compliance actions¹⁷ through a Severe Event. The SIRTF reviewed the NERC standards and concluded that the vast majority of the standards support safe and reliable operation that would be equally applicable during a Severe Event, as they would during normal operation. While it is conceivable that an entity may decide to violate a certain standard in order to accelerate broader restoration objectives, it would be impossible to predict these circumstances in advance of any event, let alone a Severe Event.

Some of the NERC standards are administrative in nature and require, for example, that entities perform periodic documentation reviews in order to demonstrate compliance with the standards. Clearly, these activities would not be considered a high priority during a Severe Event. While there may be some merit in identifying these "administrative" standards as not applicable during a Severe Event, on balance, the SIRTF felt any discussion of standards and compliance during an event may be more of a distraction for entities, rather than help them remain focused on making the right operational decisions. Furthermore, as NERC's standards are evolving, and efforts are being made for all standards to become more performance and outcome-based. Over time, this will reduce or eliminate standards that are administrative in nature.

On balance, the SIRTF concluded that entities do not need guidance on the applicability of standards during a Severe Event. Although a Severe Event may put entities in a position where they cannot comply with all standards, entities are in the best position to "do the right thing" for reliability and public safety, and self-report any violation of NERC standards as time and circumstances permit.

¹⁶ Ref. NERC Standards, <http://www.nerc.com/page.php?cid=117>

¹⁷ NERC has the legal authority to enforce compliance with NERC Reliability Standards, which it achieves through a rigorous program of monitoring, audits and investigations, and the imposition of financial penalties and other enforcement actions for non-compliance.

3.0 Operations

This section identifies the challenges associated with operating the BPS following a Severe Event. Many aspects of operations in the New Normal are not entirely different from what we have experienced to date but will be much more challenging for a number of reasons. For example, island operation in itself is nothing new – we currently operate the North American grid in four large islands known as the Interconnections. The challenge in operating islands following a Severe Event scenario is that the islands will be much smaller, more numerous, may comprise areas that fall under the authority of several different operating entities, and last for significantly longer periods of time (weeks, months or years) than we have previously experienced. Load shedding activities are also likely to be similar to, and very likely based upon, existing load shedding and rotating blackout plans required to respond to EEA-3 conditions (interruption of firm load). However, our experience with implementing load shedding plans has been limited to relatively short periods of time – a few hours or at most a day or two. In contrast, under Severe Event conditions, rotating blackouts may need to be implemented for an extended period of time and for significantly longer rotation intervals.

Following a Severe Event on the BPS we should expect that it will not be possible to fully restore the BPS to pre-event conditions and the system will be significantly degraded. In order to operate the BPS it will likely be necessary to operate in multiple electrical islands¹⁸, use emergency criteria, use rotating blackouts, and utilize a number of independent control actions¹⁹ to maintain the supply and demand balance and manage frequency and voltage. Rotating blackouts help manage the supply and demand balance by rotating supply to different blocks of load, typically on a geographic basis, on a defined schedule or timeline.

The operation of these electrical islands may need to be performed by entities that are not normally responsible for system operator²⁰ functions such as Distribution Providers. As a result, these entities could become the system operator until such time as control is returned to the Balancing Authority or Transmission Operator for the balancing area. Following a Severe Event it is not possible to predict what islands will be formed and this is further complicated when these island boundaries cross the balancing areas that are very familiar during normal operation. In fact, this occurred following the August 14, 2003 blackout that affected large portions of the Midwest and Northeast United States and Ontario (see sidebar).

Islanding Experience from the 2003 Northeast Blackout

Ontario's Beck and Saunders hydroelectric stations, along with some Ontario load, the New York Power Authority's Niagara and St. Lawrence hydroelectric stations and 765 kV AC interconnection with Quebec, remained connected to the western New York system, supplying load in upstate New York immediately following the event.

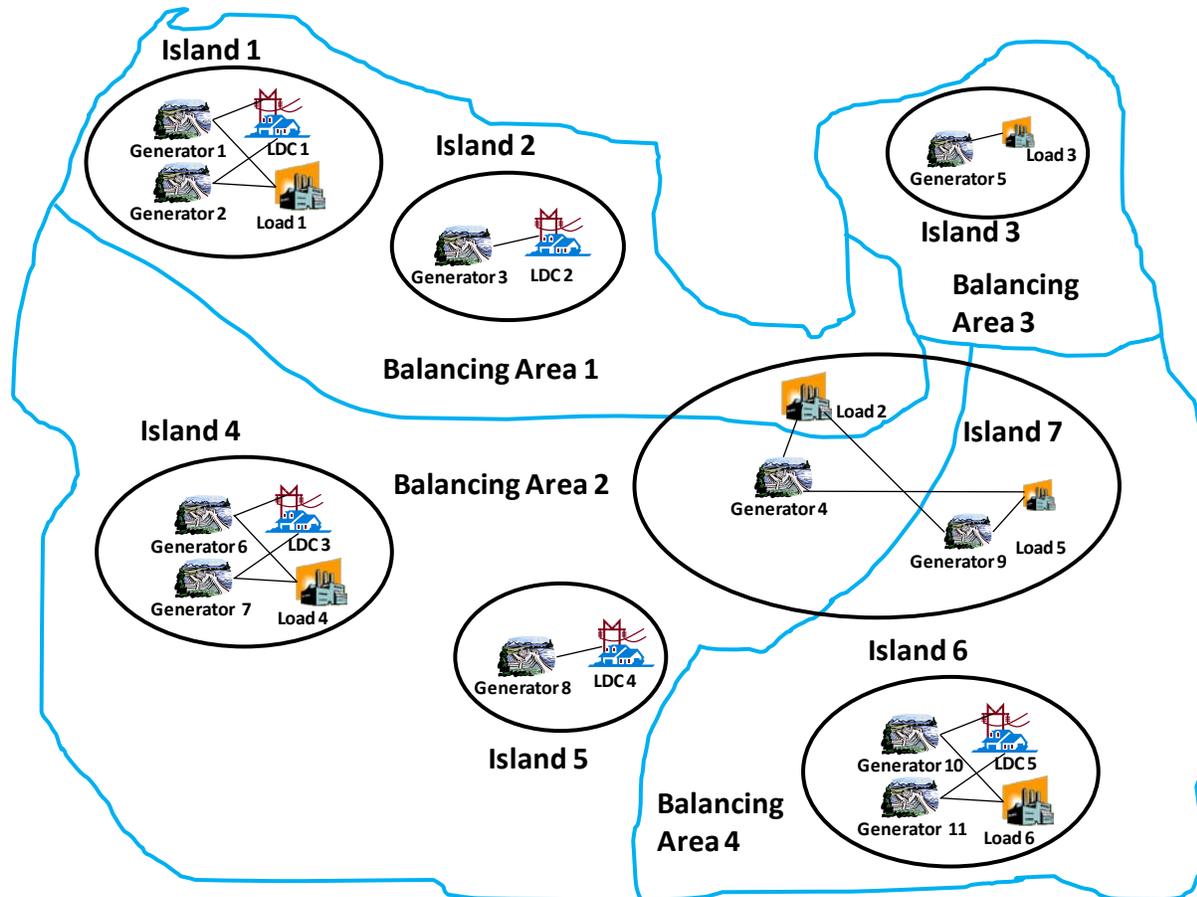
¹⁸ Islanding is the complete separation of a portion of the power system from the remaining interconnected system following a system disturbance. Islands can be comprised of generation sources, transmission elements, distribution elements and loads.

¹⁹ Independent actions are those operating actions required to enable power system restoration without prior communication to the Reliability Coordinator for approval.

²⁰ A System Operator is anyone who performs the system operator function as defined in NERC's Glossary of Terms.

The following diagram illustrates a likely scenario following a Severe Event. The BPS may form islands that do not respect traditional operator boundaries. While many islands depicted are within a single Balancing Authority (BA) Area, Island 7 is shown to exist in three distinct Balancing Areas.

Figure 3: Islanded Operation



The following sections provide more details around these challenges and the need for delegated authority and independent actions.

Assumptions

This section assumes that a substantial number of supply resources are unavailable for an extended period of time and as much as or more than 50 percent of total instantaneous demand cannot be served in the islands. The cause(s) for this inability may vary significantly and are not limited to a lack of generation resources. The situation may be extremely widespread or it could be limited to specific areas within a single balancing area. At least initially, communication and control is impaired such that at least a portion of switching will need manual operations by field personnel.

3.1 Immediate Automatic Response

Immediately following the Severe Event islands are likely to form as transmission lines between areas of the system trip. Automatic under-frequency load shedding and generator tripping may

also occur as protective relays react to the transient voltages, frequency and power flows caused by the separation. Islands with small amounts of generation and load have less inertia and as such experience larger frequency swings, are harder to control, and are more likely to collapse from subsequent generation loss than are the existing four Interconnections.

Also, many of today's loads are frequency or voltage sensitive or both (such as computers, industrial control systems, other electronic devices) and may trip off-line as a result of these swings. The challenge with frequency or voltage sensitive load loss is that it will come back on the system once electrical parameters are within the prescribed range. Also this can be further complicated with the increase in automatic schemes within the distribution system for "self healing" (smart grids). This uncoordinated load restoration possibly increases the risk of island collapse.

Recommendations

Entities should develop policies on how to treat smart grid components and frequency or voltage sensitive loads in islanding situations. The appropriate management of these components will increase situational awareness.

3.2 Operational Authority

Following the immediate, automatic system response, it is critical to determine the extent of the islands and which entity(s) are in "control" of the surviving islands. This determination would likely be made by the Transmission Operators (TO). To be in control of an island an entity needs to have the ability and decision making authority to monitor and control the assets (generation, transmission and load) within the island's boundaries. Decisions may include the need to shed load, dispatch generation, put equipment in service, etc. Although the Reliability Coordinator maintains overall responsibility of the BPS, including the synchronization²¹ of the islands, it may not have sufficient monitoring and communication to direct the operation of each island. With limited or no communication it is important that each of the entities know what independent actions they should take on loss of BPS supplied power.

Recommendations

- Reliability Coordinators (RC) and Balancing Authorities (BA) should consider developing loss of communications and delegation protocols for responsible entities in their footprint and with adjacent RCs and BAs to allow seamless transfer to the responsible entity during loss of communication or monitoring scenarios or when islands cross jurisdictions.

²¹Synchronization is the closing of a circuit breaker between two electrically disconnected, energized parts of the power system. When synchronizing islands it is crucial to match voltages on both sides of the circuit breaker before closing. If this matching or "synchronizing" process is not done correctly, a power system disturbance will result and equipment (including generators) can be damaged. In order to synchronize properly, three different aspects of the voltage across the circuit breaker must be closely monitored. The three aspects of the voltage are called the synchronizing variables and are:

1. The voltage magnitudes
2. The frequency of the voltages
3. The phase angle difference between the voltages

- Establish and practice through simulation or tabletop exercises the independent actions that entities are expected to take upon loss of BPS supplied power. This might include:
 - TO, Local Distribution Companies and directly connected wholesale customers opening all de-energized breakers under their operational control.
 - Generator Operators (GO) opening all de-energized unit and switchyard circuit breakers under their direct operational control, and beginning black start procedures for certified black start facilities.
 - GO securing station service with any available generation units in accordance with local instructions and agreements. This may include restarting hydroelectric generation units to run them at speed-no-load by closing the unit breaker (using synch bypass or synchronizing to other units).
 - For generation facilities with the capability to energize-out a portion of the BPS, GO would stabilize units and prepare them to energize transmission circuits as directed by the TOP.

Note: It is important to establish the bounds for such independent actions to ensure that stability and reliability are not jeopardized.

Key Recommendation #1 Operations
Consider which entities would take the independent actions and the tools needed to stabilize islands when communications capability is severely disrupted or unavailable.

3.3 Initial Operator Response

Following the immediate, automatic response the next priority is to take operating control actions to stabilize any islands of generation and load that remain.

Recommendations for System Operators

In order to stabilize the island the System Operator should:

- Determine the extent of the island (i.e. its electrical boundaries) and monitor frequency.
- Determine if the energy management system is communicating with the power plant control systems. If so, then setting Automatic Generation Control (AGC) to flat frequency control is desirable to allow a faster response to frequency deviations. This may not be desirable if telemetered tie-lines to adjacent systems are part of the island.
- In the absence of AGC, determine which generating units can have their droop curves adjusted to operate as the ‘driver’ unit in isochronous mode. It may be appropriate to spread this control over a number of units and set the unit’s basepoint to the mid range of its operation.
- Once the size of the island increases consider if and when it is appropriate to restore the droop setting on the ‘driver’ unit.

- Manage the load-generation balance by dispatching available generation and by using load shedding as necessary. Operators must also recognize the difficulty in solving for Area Control Error (ACE) with limited telemetry.

Recommendations for Reliability Coordinators

In addition to the above System Operator actions, the RC may be in a position to perform some high level coordination tasks to facilitate a long term islanded operation, including:

- Generator fuel supply tracking, scheduling and prioritization²².
- Providing situation assessments (e.g., status of nuclear plants) and future prognoses to stakeholders including government, the media, and the general public.
- Assisting system operators to operate their islands within the context of the situation. The RC may have a wider area view of the BPS and be able to coordinate operation and restoration activities across the various islands.
- Document and keep current the voice communications technologies and procedures available to communicate with other entities. Other entities could contact their RC to determine alternate means to communicate.

Recommendations for Power Plant Operators

Rapidly changing frequency outside normal bounds is likely an indication that the plant has formed an island with some load on the system. As noted above, the operation of the island may need to be performed by entities that are not normally responsible for System Operator functions, so that the plant operator may well communicate with a different entity than its normal system operator (e.g., BA, TO). As a result of island formation, power plant operators should examine their plant outputs and consider doing the following:

MW Output

- For AGC plants, power plant operators should determine if the energy management system is communicating with the power plant control system and leave any units on AGC.
- If no longer receiving signals, place units in manual and try to contact the System Operator and maintain unit output.
- For all other units, follow protocols for loss of communication and await further instruction from the System Operator.

Frequency

- Maintain output and attempt to contact the System Operator.
- Utilize the NERC Y2K Constant Frequency Operations Guide²³ to inform operational strategy in the event of communication loss.

²² In some jurisdictions, for example those within competitive electricity markets for generation, the Reliability Coordinator has no role in tracking, planning or scheduling generator fuel supplies.

- Make all available units ready for operation.
- If units trip, stabilize them and prepare to resynchronize following direction from the System Operator.
- Secure station service.

Voltage

- Maintain Automatic Voltage Regulation (AVR) on automatic.
- When AVR is unavailable, minimize changes to MVAR output unless the plant is at risk.
- As directed by the System Operator, adjust power system stabilizer.

3.4 Island Stability

Large interconnected power grids are inherently stable because they have many sources of governor-controlled generation and relatively predictable load patterns. Conversely, small islands are ‘high gain’ systems where relatively small changes in generation or load can cause large changes in power system parameters such as voltage and frequency which may cause equipment to trip on existing protection settings. Although this action may impede restoration, these settings are critical to ensure that we do not damage critical assets essential to restoring the BPS. Also, many of the mechanisms and criteria that dictate how we manage the system may be unavailable or require significant rethinking.

System Operators should consider the following to build and maintain stable islands.

Load

- Use distribution load controlled by SCADA to rapidly restore initial load, as time considerations may prohibit local manual operation.
- Maintaining the load-generation balance will require that System Operators anticipate the changing load pattern over time. This ability to forecast primary demand without historical data will be limited by a lack of detailed knowledge of the load in a portion of the normal balancing area. Although the peak load that can be served in the island is limited by available generation, the System Operator will need to understand the load pattern to manage frequency deviations as load picks up and drops off throughout the day. In addition, load levels in the island will likely be significantly lower than pre-event levels as industrial and commercial loads take time to recover following the severe event and resume some level of operation. The load will grow over time as operations resume but be limited by available generation.
- Prepare to limit restoring loads that are highly variable (e.g. smelter or arc furnace loads).

²³ Ref. NERC Constant Frequency Operations Guide, <https://www.frcc.com/handbook/Shared Documents/COM - Communications/Constant Frequency Operations Guide 100208.pdf>

- Local field personnel who are familiar with the characteristics of loads at the distribution level will be critical to the development of a workable plan to anticipate and respond to changing conditions as the New Normal evolves.

Generation

- Maintaining the load-generation balance requires that we know the capability and limitations of the various generation types in the island, and have a means to dispatch them. Market mechanisms, schedules, and automatic generation control are likely to be unavailable or impaired.
- Governor response of the surviving units may be limited or may not be available. Also, in the absence of AGC, generators that can operate in isochronous mode become extremely important to maintain system frequency. Therefore the location and availability of generators that can operate in isochronous mode needs to be known to allow stable island operations. BA's should consider identifying the governor responses of generators within their balancing area and those that can operate in isochronous mode so this can be shared appropriately following a Severe Event.
- Variable generation, such as wind and solar, require special consideration which may require these generation sources be limited if they are in relatively small islands.
- Generation may be limited due to regulatory requirements or license conditions that are appropriate for normal operation but may need to be revised under New Normal conditions.
- Generators that remain off-line for extended periods of time require BPS-supplied power or backup generation to support station service, further limiting the generation resources available to serve other loads.

Operating Reliability

Adequate operating reliability must be re-examined in the context of an island – normal operating reserve and system operating limits may no longer be appropriate.

- It is important to understand the limitations imposed by large voltage angle differences²⁴ and synch-check relays when reconnecting generation to the BPS. In order to protect nearby generators from high electromechanical transient stresses that occur during the switching of network elements, through studies, consider increasing the allowed maximum angle to accelerate or enable the restoration process or to allow reclosing.

The Importance of Phase Angle Requirements

During the Italian blackout of 2003, auto-reclosers failed to restore key inter-tie lines due to the large voltage angle across them – about 42 degrees. During the 2003 Northeast Blackout, synch check relays hindered system restoration.

²⁴ UCTE, "Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy," ed, 2004 and NERC, "Final Report on the August 14, 2003 Blackout in the United States and Canada," ed, 2004.

- Adequate operating reliability must be re-examined in the context of an island. Normal operating reserve and System Operating limits may no longer make sense when all available generation needs to be on-line to serve as much load as possible. Manual and automatic load shedding may become the main source of operating reserve.
- The System Operator should consider how they might optimize operating reserve while operating is islands.

Key Recommendation #2 | Operations

Consider how operating reserve would be managed during islanded operation and frequent periods of insufficient supply to meet demand.

3.5 Load Shedding

In the early stages of islanded operation System Operators need to quickly determine their energy and capacity situation. During this time, they are likely to manage the load-generation balance using load shedding. Load shedding plans need to consider the priority or importance of loads such as critical power system loads and other dependent critical infrastructures such as telecommunications. System Operators must also ensure that sufficient load remains available for automatic underfrequency load shedding (UFLS) to help protect the island from collapse. It is assumed that UFLS set points will not be adjusted initially following a Severe Event, as these levels are still required to arrest frequency decay, however may be examined periodically during the New Normal timeframe. This is discussed more thoroughly in the *Protection and Control* section of this report. As restoration progresses, system operators will be challenged to forecast anticipated load patterns for numerous smaller load pockets contained within each electrical island.

System Operators must also be aware of the different load types in the islands, particularly those prone to large swings in consumption such as electric arc furnaces and large motors. If not already shut down, these consumer loads may need to be severely curtailed until the island becomes sufficiently robust to cope with the load variability. Similarly, System Operators will need to know the maximum load block they can restore in an island as additional generation becomes available.

Recommendations:

- It is important to define, up front, what are considered “critical”²⁵ and “priority” loads for system restoration and managing load shedding. These terms are defined in the table below. Ensure that critical power system loads and other critical infrastructure loads such as certain telecommunications centers are excluded from load shedding plans.
- Conversely, consider loads that might be non-essential (e.g., street lighting, billboards) which might be without power until full restoration (to the pre-event levels) is achieved.

²⁵ The term “critical load” is different than the term Critical Asset as defined in the NERC Standard CIP-002.

Table 3: Critical and Priority Loads

Critical Loads	Priority Loads
<p>Critical loads are BPS loads essential to perform restoration and maintain reliability. In some cases, these loads are within distribution systems. During restoration, other loads may be designated as critical loads if they are essential to support restoration (e.g., load required to manage voltage). Examples of critical loads include:</p> <ul style="list-style-type: none"> • Station service at control centers, transmission substations and generating stations • Power system communications facilities • Protective relays and schemes • Monitoring and control systems 	<p>Priority loads are important consumer loads that need to be restored promptly to mitigate the impact on public health and safety, the environment, or the economy. Priority loads connected to the high voltage transmission system or to the distribution system are often excluded from load shedding schedules. Some examples of priority loads include:</p> <ul style="list-style-type: none"> • Oil refineries and pipelines • Telecommunications centers • Hospitals • Water treatment and sewage plants • Key military facilities.

Key Recommendation #3 | Operations

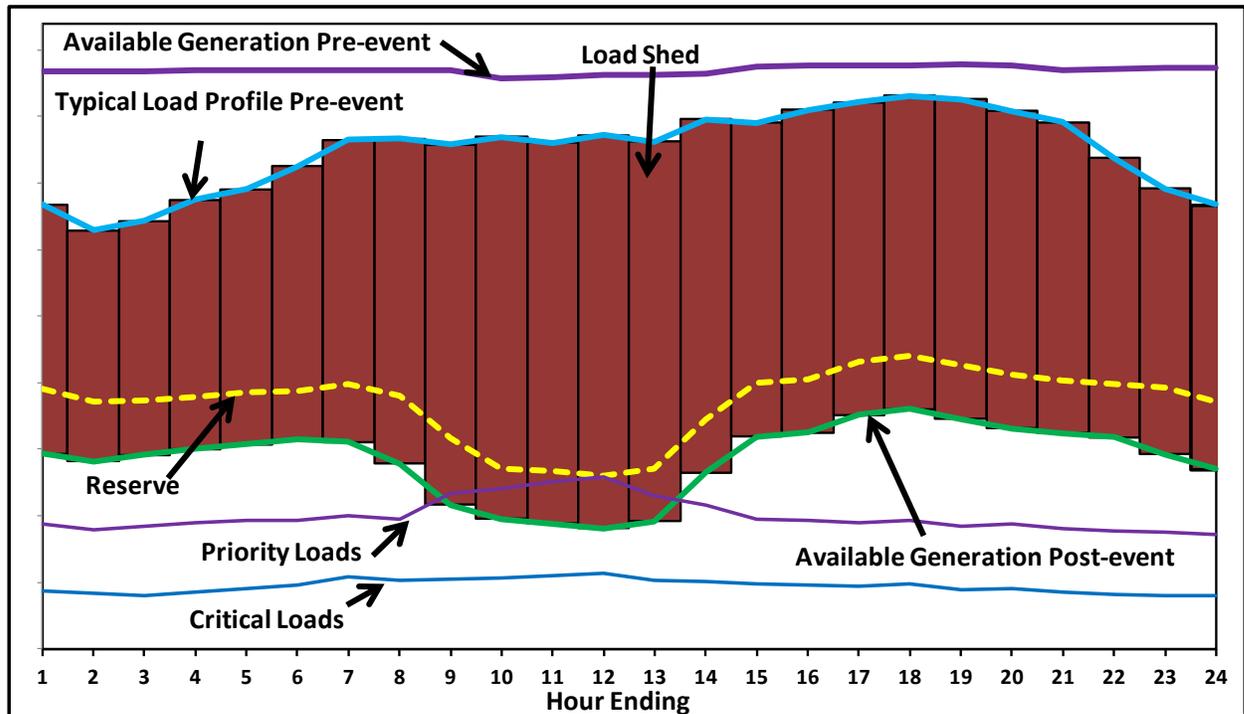
Consider ways to adopt and apply the terms “critical load” and “priority load” across all BPS entities to improve consistent use during a Severe Event.

- In the event of sustained rotational load shedding (rotating blackouts) communication becomes a key factor to ensure that affected areas understand what power supply they will have, at what time and for how long. Due to the potential impacts on public health and safety, these communications need to be carefully considered and coordinated with local distribution companies, local law enforcement agencies, emergency responders and government officials. Although the specifics of this communication cannot be established ahead of time, entities should develop a communication strategy in consultation with key stakeholders.
- Develop mechanisms to predict new load patterns in each island.
- Identify loads characterized by large swings in demand. Detailed knowledge of the types of loads in each island will allow the system operator to appropriately manage them to maintain island operating reliability.
- Develop, through system studies and industry experience, rules of thumb to help the operators determine the maximum size of a block of load that can be safely added to an island, based on the available MVA of synchronized generation.

- Since it is impossible to predict the extent of islanding formation following a Severe Event it may not be practical to share operational information ahead of time. It is important therefore that information-sharing strategies are established in preparation for such events to expedite this information dissemination and address any confidentiality concerns.

The ability to serve load within islands is expected to be limited following Severe Events. The red line in the figure below shows a typical load profile for an area under normal conditions. The green line represents the load that can be served following a Severe Event, the difference between the red and green lines is the total amount of load that will not be served, and the difference between the green line and the dashed yellow line represents generation or load shed reserved for contingencies.

Figure 4: Inability to Serve All Load During Restoration



3.6 Generation Dispatch and Automatic Generation Control (AGC)

Following the formation of islands, it may not be viable to have a centralized dispatch function based on bids and offers, so system operators will need to have an alternate means to dispatch. Similarly, AGC may not be available due to limitations on the number of islands it can control or loss of frequency or tie-line measurement. Even in the absence of AGC capability, the System Operator must have a reliable frequency measurement in the island. Also, one or more generators must be capable of isochronous operation (i.e. zero droop) to restore frequency following changes in load. System Operators need to have information on the capability and limitations of the various generation types in the island, including those that are energy limited or may have fuel supply or other operational restrictions.

Recommendations

- Develop alternate dispatch mechanisms, including communication protocols.
- Investigate the viability of installing more frequency measuring devices to increase signal redundancy or using other sensing devices such as phasor measurement units.
 - Alternatively, coordinate with other infrastructures that may be monitoring frequency from distributed devices and develop the means to share this information.
- Investigate using multiple sources for tie-line flow measurement (e.g., Inter-Control Center Communication Protocol from neighboring entities, redundant metering capability).
- Consider the viability of using AGC to simultaneously control multiple islands.

- Consider mechanisms that allow the transfer of pockets of load and associated generation near a tie line to an adjacent BA for operation within the electrical borders of that BA. Generation within the pocket could be dispatched via voice communications at a relatively fixed level while the adjacent BA provides load following capability via the tie lines.
- Determine which generators can change their droop curves – modify governors as necessary.
- Plan that nuclear generation may be off line, and develop contingency plans in conjunction with the generator owners and operators to help ensure that BPS-supplied power is available.
- Document generator capabilities and limitations in an area so this information can be readily shared should the dispatch function be delegated to an entity that does not normally perform this role.
- Information sharing protocols should be developed ahead of time with organizations that are most likely to need this type of information following a Severe Event. These protocols may need non-disclosure agreements.

Key Recommendation #4 | Operations

Consider alternate means to dispatch generation if normal automated systems, including automatic generation control, are unavailable.

3.7 Variable Generation

Variable generation (Wind and Solar) is becoming a more prevalent form of generation, and has unique characteristics that must be considered during restoration. Some (generally smaller) wind turbines are not truly dispatchable, but have variable output as a function of wind speed. For those wind generators connected to the distribution system, operators need to be aware of their impact but may not have real-time system monitoring of their output.

Normally, automatic controls connect and disconnect banks of wind generation according to the wind speed and any maximum cap set by the wind generator operator. This variability of output is not a concern when the system is in a normal state, but can be problematic during a restoration, particularly when trying to stabilize or synchronize islands.

Recommendations

- System operators should consider developing policies on how they treat variable generation (i.e., wind, solar) during island operation. These policies could address such matters as:
 - Treatment variable generation when their varying outputs cause unacceptable voltage or frequency deviations.
 - The impact of disconnecting all wind and solar generation at once either through tripping or directed actions. This may cause the island to collapse if the variable generation exceeds a specific percentage of the island's generation capacity.

- Disconnecting wind generation in banks and the need to compensate with other generation or through load shedding to maintain frequency.
- In blacked-out areas, consider disconnecting these resources and leaving them out of service until the latter stages of restoration.
- Consider connecting variable generation to large-scale storage devices radially to optimize variable generation output.

Key Recommendation #5 | Operations

Consider if or how variable generation would be dispatched through restoration and islanded operation.

3.8 Training

Consider enhancing existing training for system operators and field personnel to address the challenges of a Severe Event.

- Manual synchronization of islands.
- Islanded operations with local control area operators assuming control of certain islands.
- Communication tabletop exercises to verify and train on new coordination and communication protocols between various entities including a loss of, or significantly degraded, communications.
- Implementing rotating blackouts for extended periods of time.
- Identify, accommodate, and implement changes to priority loads.

Key Recommendation #6 | Operations

Consider enhancing regular restoration drills and exercises to train staff on communication protocols and independent control actions in the event of loss of or degraded telecommunications.

Key Recommendation #7 | Operations

Consider using more extreme exercise scenarios that involve simulated rotating blackouts and islanded operations on a larger scale and for extended periods of time.

4.0 Monitoring the BPS

The [2003 Blackout Report](#)²⁶ emphasized the importance for system operators to maintain situational awareness of the BPS. In the case of Reliability Coordinators there is also the need to maintain situational awareness over a wide area that extends beyond their immediate operating zone. Due to the interconnected nature of the BPS, system operators also rely on the system conditions and data of their interconnected neighbors.

To achieve and maintain situational awareness the electricity sector has over the past decades developed increasingly sophisticated tools consisting of metering points, communications networks and sophisticated software to monitor the BPS more frequently, accurately, and precisely than ever before. Within each entity, these tools typically monitor thousands of data points every few seconds at transmission sub-stations, lines, and generators.

While these tools are designed to be robust with availability rates of at least 99 percent, they do occasionally fail. Therefore, every operating entity has backup, call-out, and response plans to rapidly diagnose and address problems. Yet as strong as these regularly exercised plans are, a Severe Event could create such wide spread degradation of these tools or data that many operators throughout the interconnections may at best see only a portion of the BPS required to operate the system reliably.

System operators need to ensure that they have sufficient visibility and control in order to sustain a stable island. Inability to control the various parameters can lead to instability of the island and result in equipment damage. In this section, we offer options to continue to monitor the operation of the BPS, in spite of degraded system monitoring tools such as:

- **Energy Management System (EMS)** — provides system operators with data and analysis to monitor and operate the transmission system. An EMS includes several important functions.

August 2003 Northeast Blackout – Recommendation

“#22. Evaluate and adopt better real-time tools for operators and reliability coordinators.”

Since the 2003 Blackout the industry has continued to evaluate and adopt better tools that support real-time operation. System operators and Reliability Coordinators have enhanced their tools to provide decision support and situational awareness with greater granularity, accuracy, and a wider area view. In addition, NERC’s reliability standards require minimal acceptable levels of this capability for system operators. Entities continue to explore and leverage state of the art technologies such as phasor measurement units and other new methods to monitor, anticipate, and respond to real-time thermal, voltage, and stability challenges.

²⁶ US-Canada Joint Power Outage Task Force <https://reports.energy.gov/BlackoutFinal-Web.pdf>

- The “model” of the EMS provides a mathematical representation of the BPS to enable contingency analysis and other monitoring functions.
- The State Estimator uses the model to calculate data points that are not physically metered and can help validate data or estimate missing data in the event of metering failures.
- Security Analysis software provides sophisticated “What If” contingency analysis so operators can be prepared to take prompt action if BPS elements such as generating units or transmission lines become unavailable.
- Automatic Generation Control (AGC) to automatically raise or lower the output of certain generators to dynamically balance total generation output with consumer demand.
- **Generation Management System (GMS)** – provide power plant operators with data and analysis to monitor, control and operate multiple power plants to keep generation resources on schedule. GMS may also include AGC functions.

Assumptions

This section assumes that the tools used to maintain BPS situational awareness are compromised or substantially degraded for an extended period of time. Telecommunications capabilities are also in a significantly degraded state. Entities must monitor and operate a BPS that is unfamiliar and likely in an unstudied state. Entities will need to communicate and share information both internal to its operating footprint and external to neighboring entities.

4.1 Generator Output

Either MW or MVAR output data is unavailable from the energy management systems or is of questionable quality. System operators should consider the below.

Recommendations

- Following an event, create communication schedules to have power plant operators report current and projected MW and MVar output for each unit.
- Develop block loading schedules so that Generator Operators understand in advance what actions will be taken depending on system conditions (e.g., frequency readings, time of day, interconnection point voltage schedules).
- System operators could define specific operating ranges for generators that could assist in verifying that operating directives are reasonable and bona fide.
- Operating to such schedules might be difficult in the early stages of a Severe Event as the system may be less stable and operating with fewer resources. As a result, ranges may need to be larger to provide greater operating latitude, but as operating experience with the New Normal system is achieved operators might tighten these ranges.

4.2 Operating Limits

System operators must continually ensure they are operating equipment within established limits in order to avoid further damage to equipment and support reliability. Operating limits may need to be recalculated as configuration changes will alter system impedances and system flows will be radically different from normal operation. Operators will need to perform these recalculations periodically throughout the Severe Event. For each recalculation, affected entities will need to consider how close they should operate to the limit based on their understanding of the risk of the next contingency. If the risk is determined to be high, it may be better to operate further away from the limit but serve less load. If the risk is determined to be lower, it may be better to operate closer to the limit and serve more load.

Recommendations

- **Hard Copy Reference Material** — Provide thermal limit ratings for each facility in hardcopy form. Periodically confirm these ratings with automated values when on-line calculations are available.
- **Standard Operating Procedures** — BPS entities change their facility ratings at particular triggers depending on system conditions. Some entities change their ratings seasonally, others have very granular temperature sets of ratings that are different for day and night operations. During a Severe Event, system operators could implement standard operating procedures for switching to different temperature sets at established times. This will help ensure that control actions are coordinated and both parties use the same limit at the same time and under the same conditions. However, these ideas would likely only be explored after the system has returned to a greater level of predictability. It is more likely that following a Severe Event the best recourse would be for operators to utilize conservative limits.
- **Conservative Limits** — System Operators could default to pre-studied conservative limits to provide additional robustness to the transmission system in order to absorb an anticipated threat. These conservative limits could represent N-2 or maximum credible contingencies and position the BPS in a more resilient mode of operation.
- **Revisit Design/Operating Assumptions** — Following an event, system operators may need to revisit the assumptions underpinning their limits (i.e., operating in a number of small islands will create far different flows on the system than during normal interconnected operation). Design assumptions that need to be reviewed include the type and amount of load, the interconnected/networked nature of the system, generation mix, and system transfers and flows.
 - The New Normal operating environment may require system operators to operate with far more risk of potentially damaging equipment and/or cascading islands. Redefining these operating assumptions may provide greater flexibility to serve more customers provided any short-term gains are balanced against potential long-term consequences.
 - Reassessment of operating limits may also be driven by physical damage or long-term unavailability of assets.

- If these changes in assumptions drive changes to limits, the operating entity should communicate these changes with its Reliability Coordinator and any interconnected neighbor.

Key Recommendation #8 | Monitoring the Bulk Power System

Consider developing processes to quickly study island configurations and develop suitable operating limits.

- **Operate to the Most Conservative Reading** – Normally when either a limit or the monitored flows are in question, operators should always operate to the most conservative readings/limits may require reconsideration in the New Normal. Entities should consider when this fundamental requirement might not be achievable in the New Normal. Example decision criteria might include:
 - Reconsider operating to the more conservative reading/limit when the result might create far greater social impact (e.g., inability to serve priority loads that have a clear impact on public safety).
 - What entities need to be consulted to understand possible consequences? Can emergency management organizations better help frame such decisions?
 - Safety of nuclear units may be put at greater risk if an operator were to default to the more conservative limit that would require switching a line providing BPS power out of service. Accepting the short-term risk of keeping the line in service, might be the more prudent and safe decision for the overall community.

4.3 Monitor Flows on BPS Facilities

Having system operators continually understand either the actual or modeled flows of tie lines and internal transmission facilities is essential in system operations (these readings are as critical as an altimeter is to a pilot). As such, an adversary could have either altered an EMS Model’s representation of the topology of the system (altered which elements are modeled in service or out) or have changed the modeled flows and possible impacts (impacts to State Estimation and Security Analysis results)?

Recommendations

Consider operating without any state estimation, relying only on actual power system flows for weeks to months.

- Prior to an event, conduct studies with the EMS to understand the bare amount of data required to keep the current state estimation model and security analysis applications solving.
- Assess whether greater levels of load or generation aggregation could be used to reduce the amounts of required data.
- Consider if a simplified model with reduced granularity could be stored locally or on a separate portion of the Information Technology (IT) network. Consider if this model could be uploaded to the EMS and integrated with the state estimator and identify:

- Subject matter experts needed.
- Time and effort required.
- Procedures needed to implement if subject matter experts are not available?
- Testing and training.
- Assess what conservative operating restrictions may be needed to mitigate the reduced accuracy of the simplified model (e.g., conservative limits for certain facilities).
- Create a prioritized list of the data points most critical to understanding the operating state of a given operating area (the canaries in the coal mine).
- Consider the need to reconfigure study models to reflect an extended period of islanded operation, and at what stage of the New Normal this would be undertaken.
- Consider the field personnel and communications capabilities needed to sustain 24x7 manual monitoring at critical data points. To enhance this capability, consider:
 - Training required to provide accurate monitoring and maintain safety.
 - Developing procedures and reporting formats for each facility.
 - Using security personnel for some monitoring duties.
 - Communications equipment, facilities and methods.
 - Pre-arranged reporting times.
- If the Internet is available, consider using social media (e.g., Twitter feed) to facilitate reporting.

Key Recommendation #9 | Monitoring the Bulk Power System

Consider developing processes to monitor BPS flows in the absence of reliable automated systems and communications.

- **Use of Phasor Measurement Units** – Throughout the Eastern, Western and ERCOT interconnections, phasor measurement units (PMUs) are being installed to enhance the granularity of BPS data. PMUs provide system operators a paradigm shift in situational awareness. Rather than measuring the system every few seconds, PMUs can measure the system tens-of-times per second. It has been said that PMUs are to current EMS models as CATSCANS or MRIs are to X-rays. As exciting as these emerging possibilities are for operations, what is intriguing from a resilience perspective is that many of the new applications using PMU data provide new opportunities compared with traditional EMS applications and data communication links.
 - System operators are currently field testing new PMU applications and considering how these may provide a completely independent source of data.
 - PMU applications could be driven by data collected at particular points via data concentrators, and may provide system operators with essential data using far fewer PMU readings.

- As these PMU applications are developed to become full production operations applications, organizations may consider how to keep the PMU applications independent of EMS applications and support hardware. The end result may be that PMU applications might not only enhance current operational reliability but support reliability and resilience in a New Normal environment.
- **Use of FNET** — Research into island detection based upon the use of frequency disturbance recorders (FDRs) originally installed as part of the frequency monitoring network²⁷ (FNET) program developed at Virginia Tech is currently under way as part of the GridEye²⁸ program managed by the University of Tennessee and the Oak Ridge National Laboratory. The proposed project seeks to combine FDR data and offline analysis to provide a practical, low cost implementation of island boundary visualization based upon existing technology and real-time/historical data.

4.4 Loss of Control Centers – Both Primary and Backup

This section addresses concerns and issues that would result when there has been a loss of both the primary and backup control centers for a BA, TO, or RC. Most likely the risk of losing both control centers is very remote. However, following the 2011 Fukushima disaster, the Chairman of the Nuclear Regulatory Commission commented that if such a disaster had occurred in the U.S., the Commission would have directed evacuations within 50 miles of the impacted plant(s). How many operating entities have both of their control centers in the 50 mile radius of a single, if not multiple, nuclear plants? There is no panacea for the numerous problems that would be manifested in this scenario; however, there are a number of things that could be addressed before, during, and after such an event that would lessen its impact. Yet the following recommendations are not intended to encourage the building of tertiary (back-up to backup capability); however these ideas are shared to elicit consideration of the how to avoid or respond to the very remote possibility of losing both control centers.

Recommendations

- When considering a new location for the primary or alternate control centers consider building the new facility a distance from the other which would avoid common risks including natural and man-made concerns such as 1) earthquake fault zones, 2) hurricane or tornado zones, 3) evacuation radius for nuclear and chemical plants, 4) tsunami risks 5) volcano eruption zones 6) chemical spills from rail or highway accidents and manufacturers, or other risks. It is understood that the greater the distance between control centers the longer it would take to occupy the backup control center; as such there are inherent tradeoffs between the possibility of losing the ability of controlling a portion of the grid while the entity is occupying its backup control center.
- Consider developing arrangements with neighboring BA, TO, or RC, [Power Plant or Market Dispatch Office] to share or use their control facilities.
 - Share telemetry between entities.

²⁷ Ref. FNET, <http://fnetpublic.utk.edu/>

²⁸ Ref. Grid Eye, http://www.ornl.gov/sci/electricdelivery/pdfs/GridEye_Fact_Sheet.pdf

- Use Inter-Control Center Communication Protocol from a third party.
- Deploy multiple, diversely routed telemetry communications paths from selected critical remote terminal units to data concentration hubs which are not co-located with the control centers.
 - From each of those data concentration hubs, telemetry could be fed to both the primary and alternate control centers, or a 3rd party with which there is a contract to share their control center/capabilities.
 - A mini SCADA²⁹ SCADA or EMS could either be located at or mobilized to a data concentration hub to allow limited emergency system control with the loss of both control centers.
 - As the industry continues to deploy and leverage Phasor Measuring Units (PMU's) within operations, entities may consider concentrating the PMU data at a tertiary site away from the primary and back-up control centers. Having the PMU concentrator and user interfaces might provide for a bare bones tertiary control center.
- During the time the entity is required to operate at a location other than the primary and backup control center, physical security would have to be maintained at the alternate site. The physical design should enable this to be accomplished quickly and easily. Contracts should be developed in advance for any needed security services.
- Consideration should be given to the logistics required for self-sustained operations, at an alternate site. This would involve sufficient office space for engineering, computer, and dispatch personnel, as well as, the supplies and storage for food and water for an extended period.
- Consider building operator-training simulators at a location independent of both the primary and back up control centers. Though the simulator will not have the complete capabilities of the primary control center or backup control center, if connected to particular data concentration hubs it may permit operators to control portions of the BPS within the parameters of the New Normal.
- Should entities consider having their Storm/Emergency Response centers at tertiary sites with some limited level of system control and information?
- Often control centers of large areas have many subordinate control centers. These subordinate control centers could range from being a local control of a large transmission owner to a small municipal operating entity. Regardless of size and particular monitoring capabilities, these subordinate entities could participate in drills where they must operate in the absence of direction and oversight. As such, if a large entity were to lose both its primary and backup control centers, efficient BPS operations may have been impacted, but effective operations may still be maintained through a far

²⁹ A mini SCADA has less functionality and capacity than a primary SCADA, with fewer telemetry points and limited advanced applications, if any. It usually is capable of at least monitoring tie line flows with neighbors.

more diverse group of operating entities. In order to achieve effectiveness, parties may need to consider the training and drills needed to create the confidence and capabilities to achieve reliability under this distributed model.

- If there is a warning of a possible attack or major system event, operating entities may want to consider staffing each of the sites where it has some operating capability. In the event that anyone or multiple sites are damaged the remaining facility may be able to take control, if only partially.
- From a cybersecurity perspective, both control centers could be significantly degraded if the primary and backup control centers are simultaneously exploited through the means by which entities keep the facilities synchronized. In an environment of heightened cyber threat, operating entities may consider not keeping these facilities synchronized and utilizing different sets of cyber controls and hardware to ensure that both centers do not have common vulnerabilities to potential cyber threats.

Key Recommendation #10 | Monitoring the Bulk Power System

Consider the simultaneous loss of primary and backup control centers and how essential functions will continue to be performed.

5.0 Communications

The reliable operation of the BPS depends on a highly reliable communications infrastructure. North America's BPS has been described as the world's largest machine; generation resources, consumer load, field operations, and centralized controls are all separated by significant geographic distances and the actions of any single entity can significantly impact others. Although communication, both voice and data, is very important in normal operations, during a crisis situation it is absolutely critical³⁰.

During a Severe Event it is expected that communications will be degraded to some extent, and entities may experience the complete loss of normal communications. Despite this, operating entities must strive to continue to monitor the system and direct operations at all times regardless of circumstances. This section discusses alternatives to address the challenges associated with degraded communications.

Assumptions

This section assumes that communications is degraded as a result of a Severe Event for a number of reasons:

- Impact on communications infrastructure from one or more of the following:
 - Loss of BPS power supply to telecommunications facilities.
 - Physical damage to telecommunications facilities.
 - The user volume of communications exceeds the capacity of communications facilities, especially cellular and satellite telephone networks.
- New and unfamiliar communications protocols that are not required during normal operation may need to be arranged with entities or individuals.
- Electricity market functions that depend on automated dispatch will be dramatically reduced or suspended, creating the need for manual operator control and direction.

³⁰ A cyber attack will pose particular risks to the systems used to operate the BPS. This is addressed by NERC Cyber Attack Task Force report, currently under development.

5.1 Communications Relationships

The need for reliable communications depends on the operating relationships between entities. The following table illustrates key working relationships and the types of communications most critical to BPS operations through a Severe Event.

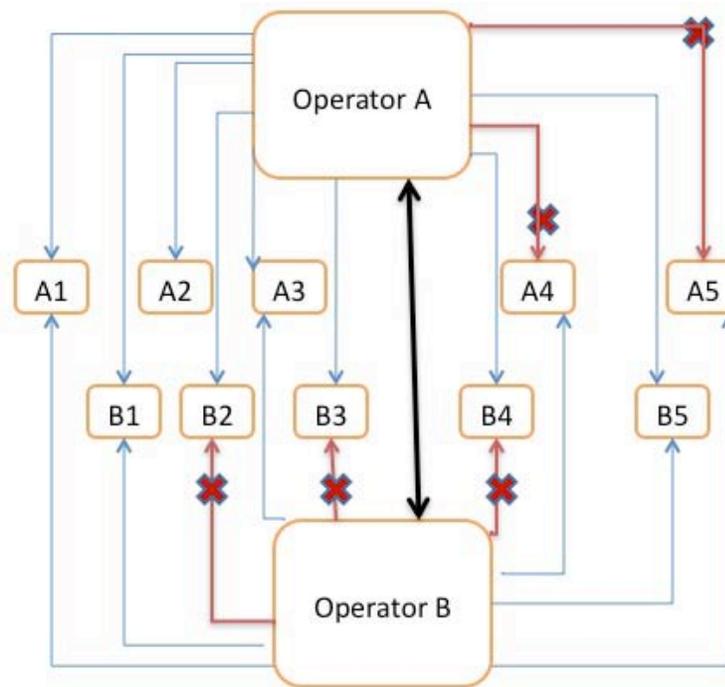
Table 4: Key Communications Relationships	
Relationship	Key Communications
1. Between field personnel, through the Distribution Provider and Transmission Operator, and the control center of the Transmission Operator	<ul style="list-style-type: none"> • Assess situation at remote facilities • Manually read meters and equipment status indicators • Operate equipment (e.g. opening and closing breakers)
2. Between the Balancing Area and the Generator Operator within an island	<ul style="list-style-type: none"> • Determine generator status and schedule, including fuel and operating limitations • Direct generation schedules (MW and Mvar) • Monitor frequency • Determine which unit could operate as the driver unit in isochronous mode
3. Between the plant Generator Operator and its connected Transmission Operator	<ul style="list-style-type: none"> • Determine generator status, schedule, and constraints on unit output • Determine transmission line and substation loadings • Implement restoration sequence • System configuration
4. Between the generation/transmission operators and their suppliers of equipment and services	<ul style="list-style-type: none"> • Determine fuel, equipment, and other resource requirements • Secure reliable delivery of essential fuel, equipment, and other resources
5. Between the control centers of neighboring but not necessarily interconnected Transmission Owners, Transmission Operators, Balancing Authorities, and Reliability Coordinators	<ul style="list-style-type: none"> • Confirm generation and transmission status and limitations • Methods of controlling generation to match load throughout the zone • Decide plans to synchronize islands • Identify opportunities to provide mutual assistance
6. Between the Transmission Operator control centers and the Reliability Coordinator	<ul style="list-style-type: none"> • Discuss and coordinate restoration and operation options and strategy • Confirm operating authorities

Table 4: Key Communications Relationships	
Relationship	Key Communications
7. Communications with Government entities (e.g., local and state emergency operations centers)	<ul style="list-style-type: none"> • Assess situation • Determine prognosis for restoration of service • Identify needs and priorities • Coordinate with other critical infrastructures • Coordinate public communications (e.g. schedules for rotating blackouts) • Identify safety and security needs and solutions • Keep informed about status and manage expectations for service
8. Between the consumer loads and the Distribution Service Provider	<ul style="list-style-type: none"> • Provide information regarding the nature of loads within the area such as priority loads, large or variable loads, issues related to cold load pickup • Coordinate and communicate service restoration information and rotating blackout schedules • Communicate restoration information and manage customer’s expectations for service quality

5.2 General Communications Recommendations

- The *Interdependencies with Other Critical Infrastructures* section of this report suggests ways to work with telecommunications service-providers to better understand interdependencies and mitigate the risks associated with BPS and telecommunications infrastructure disruptions.
- Consider co-locating BA and TO functions within the same work center in order to reduce communication requirements and assist with the synchronization complexity of restoration.
- When examining backup communications options, minimize the number of repeater hops to reduce the number of possible failure points. Configure satellite telephones so they operate point-to-point without the need for intermediate ground stations. Entities should be flexible and prepared to create a network that may include hops to other entities in their wider area through whom they can communicate as illustrated in the figure below.

Figure 5: Alternate Communications Paths



Operator A has communications with key facilities A1, A2, and A3 but does not have communications with A4 and A5. And Operator B cannot communicate with B2-B4. When Operator A confirmed it had communications with Operator B, it found Operator B could communicate with facilities A4 and A5. As such Operators A and B developed a communications relaying relationship. While Operator A is working to restore communications to all of its facilities, it is trying to assist Operator B with getting communications with facilities B2, B3, and B4.

- Entities should consider installing mobile radios compatible with those used by neighboring entities, and developing protocols to share assigned channels.
- When preparing for the Y2K transition period, many entities implemented satellite telephones and continue to rely on them in the event primary communications facilities are unavailable. NERC should consider assessing the extent to which they can presently be used to coordinate operations between entities within each Interconnection.
- Identify personnel in advance who have communications skills, such as HAM radio or social networking media such as Facebook or Twitter. If the Internet continues to be available these methods could be very effective in communicating rapidly to the public at large.
- Consider backup generation wind generation and solar cells at communications sites to prolong the power supply to these resources. Note that sources of variable generation will require significant energy storage capability.

Key Recommendation #11 | Communications

Consider installing renewable generation (e.g., wind, solar) at critical BPS facilities to supplement standby generators.

- Prepare plans for long-term fuel delivery to backup generation at entity-owned communications sites.
- If time permits before a degradation of communications, increase the utilization of system “All-Call” and the NERC Reliability Coordinator Information System (RCIS) to notify operating entities of increased operating activity and the need to coordinate major system activities.
- If primary communication links to remote terminal units are down but other communication lines are functioning consider how an Operating Entity could leverage sub-station security communications capabilities (i.e., radios, fiber communications) to relay critical power system flows, without significantly jeopardizing these systems.
- Local emergency management services (e.g., police, fire, military) vehicle radios may provide both physical security and communications capabilities at critical sub-stations.
- Local HAM Radio chapters often have agreements with local emergency operations centers to provide communications in times of emergencies. Consider reaching out to these chapters³¹ to integrate into business continuity planning and possibly drills and exercises.
- The military once had wire telephone communications gear. If available in local armories how could operating entities and the military use such wired communications between critical operating nodes within a particular island (this option would require physically laying the wire and staffing switch boards).

Key Recommendation #12 | Communications

Consider alternate means to communicate when primary means of communication are completely unavailable for extended periods of time.

³¹ Radio Amateur Civil Emergency Service <http://www.qsl.net/races/> and Amateur Radio Emergency Service <http://www.arrrl.org/ares>

5.3 Communication Protocol Recommendations:

Reporting Formats

- Know which are the critical data points are needed to assess the current operating state (review and refresh the protocols developed for Y2K to report critical operating data).
- If all sites are reporting during a single time period (or even staggered), prioritize which stations report first (e.g., by criticality of the information, alphabetical order, or other method). Structured and sequential communications will help manage communications volumes and delayed or missed calls.
- Develop a standardized reporting format so more information can be passed more effectively (i.e., location, reading 1, reading 2, issues, possible opportunities, actions).
- If spreadsheets are used to record the data, consider if dedicated laptops are needed to consolidate the data, or if hardcopy forms available at data collection points would be sufficient.
- **Consistent Conference Call Protocols** – The individuals providing information will change throughout the New Normal period. Communications must be clear and concise and the leader of the conference calls must drive participants to stay focused on the essential elements of information; the information needed to identify issues and decide the necessary actions.
- **Communications Protocols for Field Personnel** – Develop, train, and exercise field personnel on the communications protocols they will use.
 - Prepare a specific reporting format and common protocols.
 - If needed, assign each critical data point a reporting time, so that the various parties are coordinated.
 - Prepare for an extended period of degraded communications with field personnel (i.e., posting these procedures at the stations with critical data points).
- **Protocols for Releasing Information to the Public** – Throughout the New Normal period, people will need to understand how restoration is proceeding so they can make their own decisions to care for themselves, their family, and their community. If there is limited information available from media outlets, entities could consider posting important information (e.g., rotating blackout schedules) at government offices such as police stations or post offices and at locations where people will congregate (e.g., food and water delivery points).
- **Standing Orders for Personnel** — Standing orders are a prescribed set of instructions for people to take action in the absence of communications or leadership direction. Standing orders could be developed to direct key personnel to report to designated locations following a Severe Event or direct a sub-station technician to clear each bus and open each breaker following a large scale blackout.
- **Validating Sources of Information** — The New Normal may create different operating relationships with operators communicating with and being directed by people they do not know. Consider establishing validation protocols to confirm identities. Develop

“challenge and password” protocols or other information known only to certain persons. Consider how these passwords would be developed, shared, protected, and periodically changed.

Key Recommendation #13 | Communications

Consider robust training, drills, and exercises to fully test critical restoration steps using alternative voice and data communications (e.g., satellite telephones).

5.4 Emerging Technology Recommendations

NOTE: The following suggestions assume the Internet is available. The diverse and distributed nature of the Internet’s network infrastructure makes it highly resilient. Local Internet Service Providers and the “last mile” of connectivity to the end user may be the weakest links if they are directly affected by the Severe Event.

- **Masked websites** — Entities could each develop masked (i.e., not listed under the entity’s normal domain) websites to display critical readings.
 - Coordinate the development of these websites with other entities so they are designed, secured, and tested (these may require another web presence beyond your entity’s currently “secure portal”).
 - These websites could support data scraping so that other entities could scrape from multiple sites and upload to spreadsheets to assist in model updates or offline analysis of system conditions. To facilitate this, decide which common data format (e.g., XML, or RSS feeds) will be used. The data scraping could potentially dump the values into PSSE models or other off line studies or analysis.
- **Alternate use of security cameras** — If there is insufficient staff to read key metering points consider using security cameras to monitor a meter (more acceptable when the threat is not a physical attack threat).
 - Consider using the physical security monitoring center to relay the meter readings to operations personnel.
 - If multiple entities require these readings consider uploading the camera feed to a webpage. This would significantly reduce the verbal reporting burden and multiple entities could access the data as their models or processes required.
- **Mobile devices** — Smart phones and tablet computers could be used as cameras, video cameras, or for conference calls.
- **Ad hoc networks** — Consider what was done during the Arab Spring uprising in Egypt to continue communications even when the Internet was significantly limited, using for example, Mobile Ad Hoc Networks (MANET). Below is an excerpt from IEEE *Building a Subversive Grassroots Communications Network*, Ritchie King, Jul 2011.

- **Social media** — Consider using social media such as Twitter feeds for reporting. Consider developing Twitter accounts that could be used to share critical data from substation to control center, and control center to neighbors. This could be an extension of an entity's existing social network, but directed to system and field operations rather than consumers.

6.0 Short-term and Long-term System Planning

This section offers guidance for both short-term (also known as operational) and long-term system planning functions through a Severe Event. While long-term system planning functions may seem less immediately impacted by a Severe Event than other functions, both short-term and long-term system planners should be equally prepared to ensure their functional resilience.

This section considers the impact on system planners of a Severe Event that damages or degrades planning resources and capabilities.

Affected System Planners

System planners are typically divided into short-term (or operational, less than 12 months time horizon) or long-term (greater than 12 months). While there are significant differences in these functions, there is sufficient similarity in how they are affected by a Severe Event that both are considered in this section. Where appropriate, differences are noted.

System Planning Tools and Facilities

System planning engineers typically work as integrated groups in an office environment with a central computer network, telephone network, and access to real time information from operating centers.

Information and data needed for system planning is typically in several forms: traditional paper files, drawings, and maps are located in or near the planning center, records of in-progress current project work in both paper and digital form are at the planner's desk, and shared data such as system load flow base cases are likely to be located in computer servers which may be local or remotely accessible through the IT network. Maintaining backup copies of data is typically a challenge; paper records, even if duplicated, are unlikely to be maintained in a backup location. System planners may periodically create backups of in-progress work but the copies are typically maintained locally. Only the data located on servers is likely to be adequately and securely maintained with off-site backup.

System planning tools and software are typically concentrated at one or two locations. Some software such as load flow, fault analysis, stability, relay settings, and economic analysis will be installed on individual user laptop and desktop computers and many programs require software tokens or are locked to the user's computer. More complex software and associated databases may be installed on local or networked servers. Some short-term system planning software, such as an interface to a state estimator or other real-time system information, is more likely to be installed on dedicated computers in physically and electronically secure locations.

Other system planning tools such as calculators, drafting equipment, plotters, printers, & scanners, are typically located in a central planning office for general use.

Experience from Hurricane Katrina

Following Hurricane Katrina, Entergy transmission planners were unable to enter their headquarters in downtown New Orleans for several weeks. This substantially affected their ability to provide timely support, and limited confidence and speed of restoration and reconstruction efforts.

6.1 Consequences of a Severe Event on System Planning Functions

The consequences of a Severe Event may include the following, discussed in further detail below and elsewhere in this report.

- Temporary loss of access to system planning offices and tools.
- Temporary loss of access to protected or backed up software.
- Loss of communications.
- Unusual demands on system planners for studies.
- A need for studies of systems with multiple BPS elements out of service.
- Loss of personnel, unable or unwilling to rejoin the system planning function.

Loss of Access to Facilities, Software, and Data

Loss of access to system planning offices, tools, and communications are typically addressed in business continuity plans. In the event that tools and facilities become available, but data is inaccessible, essential information will need to be developed from other sources. Operations will have backup centers where versions of system planning cases may be found. Joint and interregional studies may also be a source for replacement information.

The particular concern with loss of access is that even though it is likely that facilities and tools can often be replaced, if attention is not paid to implementing and sustaining spare equipment and data backups, a significant delay can occur before system planners are able to function again.

Key Recommendation #14 | Short-term and Long-term System Planning

Consider the potential loss of system planning resources (e.g., equipment, data) as well as damage to the system. Review business continuity plans to ensure that system planning resources are adequately considered.

Unusual Demands on System Planners for Studies

Demands on system planners will be immediate, intense, and continuous as system conditions change and configurations evolve. For example, the April 27, 2011 tornadoes affecting TVA required analysis to operate multiple unplanned islands, and study previously unconsidered configurations. Similarly, the loss of the HV transmission cables supplying the Auckland, New Zealand central business district in 2006 required planners to incorporate the temporary overhead lines.

Experience from the 2011 Japanese Earthquake

The 2011 Japanese earthquake and tsunami and the destruction of all transmission facilities supplying the Fukushima nuclear plant required rapid multiple expedient responses that placed extreme demands on planners.

The tasks of system planners will evolve through the mitigation, restoration, and New Normal phases of a Severe Event.

- **Mitigation Phase** — Establish and recover essential system planning facilities. Restore as much of the BPS as possible to reliable operation with a focus on supplying critical and priority loads. Perform essential studies to support BPS operation in unstudied states. Perform studies needed to support island synchronization, system reconfiguration, and potentially conflicting requirements for emergency supply to priority loads. Tasks may require only a limited number of system planners, but with specialized skills and local knowledge.
- **Restoration Phase** — Continue to recover and construct facilities adequate to support longer-term system planning. Develop the studies needed to consider options to return generation and transmission facilities to service. Begin to develop longer-term plans for new facilities. During this phase, the need for system planners may increase from a small core of specialists to a full complement of planning staff.
- **Return to Normal Phase** — Restore complete system planning capabilities. Reconcile short and long-term system planning requirements to improve BPS reliability. Resume long-term system planning functions.

Key Recommendation #15 | Short-term and Long-term System Planning

Consider the appropriate use of key system planners who may be required immediately, and for prolonged periods, to perform studies not previously considered.

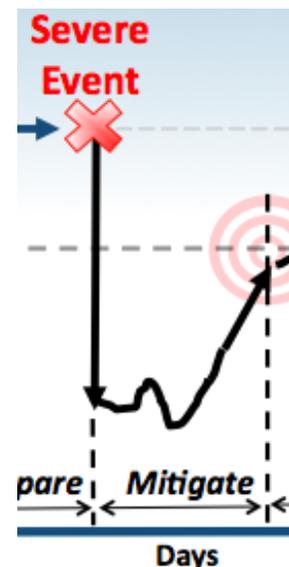
6.2 Planning During the Mitigation Phase

Support Real-Time Operations

The first priority for system planners will be to establish communication with essential staff and recover essential planning facilities and data needed to begin work. Once this is done, the immediate priority will be to support system operators in their efforts to restore the BPS and supply electricity to customers to the extent possible on a prioritized basis. The initial surviving system will likely be in an “unstudied” state. Therefore, real time assessments will need to be performed and step-by-step restoration procedures confirmed by studies before control actions are taken.

The volume of work and the need for rapid response is likely to require that some long-term system planners be re-assigned to the short-term system planning effort during the mitigation phase and perhaps even into the early portions of the restoration phase.

If there is widespread damage to the system, system planning studies may need to consider using temporary configurations such as partially restored substations. Studies may include operation with less than normal margins, contingencies that may cause loss of load, reconsideration of breaker fault ratings, and reconsideration of transformer overloads. Normal design criteria such as voltage may not apply in the early stages following the Severe Event. System planners and management should re-evaluate planning requirements considering the consequences of the Severe Event.



Temporary Facility Ratings

System planners may need to consider temporary above-normal ratings in order to restore the BPS quickly. An ability to quickly calculate and integrate such ratings should be available.

Replacement Equipment

While entities have the ability to withstand normal emergencies events and quickly restore their systems from existing or quickly obtained spares, a Severe Event may render purchased spares unavailable for a prolonged period. In this case continuing operation with temporary design solutions using sub-optimal equipment may be required. Maintaining records and databases of equipment characteristics as reconstruction proceeds, particularly when equipment is substituted on a contingency basis, may be a challenge. While most entities have comprehensive transformer spares programs, use of spares in expedient restoration situations may result in unbalanced configurations. Studies may be required of protection and operating limits.

Planning Following the April 27, 2011 Tornadoes

Following the multiple tornados affecting the Tennessee Valley Authority, the Browns Ferry nuclear plant had lost all but one of its seven 500kV transmission connections. As the transmission lines were successively restored to service, multiple unstudied configurations had to be reviewed in coordination with plant restoration.

Advance System Planning

Items of advance system planning should be considered as an aid to help speed the mitigation phase. Examples include:

- Perform system studies and maintain records of equipment interchangeability.
- Perform studies to identify the islands that would likely form during a Severe Event, and their sources of generation, including sources of generation (e.g., cogeneration at an industrial plant) not normally supplying the BPS.]

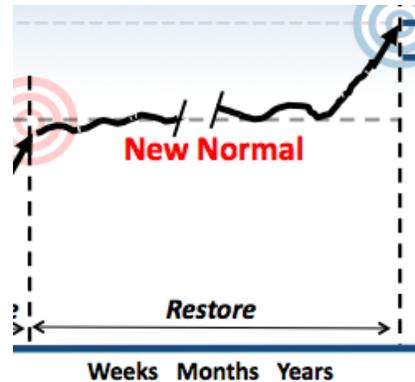
Key Recommendation #16 | Short-term and Long-term System Planning

Consider performing selected studies in advance (e.g., equipment interchangeability) that could help speed restoration.

System Planning during the Restoration Phase

As immediate real time operating demands are met, system planning will transition from the immediate mitigation phase to longer-term restoration of the BPS. Temporary staff reassignments are likely to continue. The system planning function will grow from an initial core of specific expertise and begin to approach pre-event capabilities. In study targets, it is possible that restoration and construction will be significantly different from the original BPS configuration. Factors may include:

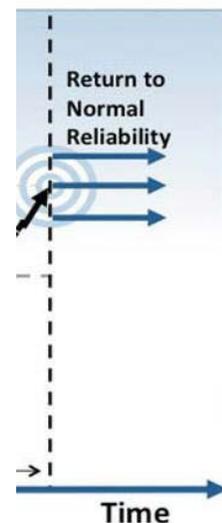
- Long term loss of load, e.g., industrial or residential loads that may be lost for extended periods.
- Budget limitations as operations, maintenance and capital funds are reallocated to manage more immediate priorities. This is discussed further in the section *Emergency Financing* section of this report.



6.3 System Planning during the Return to Normal Phase

By this time the restoration of system planning capabilities will be complete, although it may differ from the original. System planning efforts may be required to reconcile short and longer-term plans with the requirements of the post-New Normal system and its remaining loads. System planning will likely have achieved restoration of regular planning schedules. Entities will be reflecting on their experiences and considering significant changes in long-term plans. Factors may include:

- Permanent loss of load, in particular, industrial load.
- Permanent budget changes, either lower or higher, and possibly new funding and approval mechanisms.
- Loss of experienced planning staff, expertise, and resources.



6.4 Design Considerations

While system planners are typically not responsible for the physical planning and design of lines and substations, they are well positioned to offer recommendations toward improving reliability, including the following.

Critical Spare Equipment

Emergency spares may not be identical to the equipment they replace and may result in unbalanced configurations that require protection and operating limits studies.

Entities have spare equipment criteria for critical equipment such as transformers, transmission line and substation, and generating unit components. However, a Severe Event may render purchased spares insufficient or unavailable for a prolonged period. In this case, operation with temporary designs may be required. To further enhance resilience, line and substation planning could include:

- Increase Equipment Standardization** — To promote greater interchangeability of components, increase the standardization of component specifications such as physical size and electrical rating. For example, TVA has minimized the number of single-phase 500 kV transformer designs that it currently purchases, and has extensive studies on file of the interchangeability of differing designs. Others have established standard sizes and ratings for transformers, breakers, conductors, and other equipment.
- Standardized 500 kV
Transformers used by
Tennessee Valley Authority
- Following two 500 kV transformer failures in 2001, TVA developed an approach that reduced costs and procurement time, and increased interchangeability of spares by limiting transformer purchases to seven standard designs, and using external rather than internal reactors.
- Location of Spare Equipment** — The location of spare equipment may be important. The spare equipment should be readily assessable, but a physical distance from the equipment being replaced to minimize the possibility of damage as a result of collateral or intentional actions. In higher voltage substations using banks of 3 single phase transformers, a 4th spare transformer is typical and physical separation of the spare should be part of the station design.
 - In-Situ Spares** — It is common practice to situate spares (such as high voltage transformers) adjacent to in-service equipment within same station to minimize restoration times due to equipment failure. Again, physical separation of these transformers should be maximized and otherwise protected from the potential of collateral damage caused by the destruction of the other. Other means to separate in-service spares could include using blast walls, complete redundancy in switching devices (breakers) and relay protection.
 - Use of Adjacent Substations** — Maintaining a safer distance between in-service spares could also be accomplished, depending on application and location, through storage at adjacent substations.
 - NERC Spare Equipment Database³²** — Consider contributing spare high-voltage transformer data as part of the NERC Spare Equipment Database program being implemented in 2012.

Key Recommendation #17 | Short-term and Long-term System Planning

Consider the spare equipment critical to BPS restoration and ways to improve availability of these spares.

³² Ref. NERC Spare Equipment Database <http://www.nerc.com/filez/sedtf.html>

Use of Rights-of-Way

Utilities that operate in areas prone to tornados recognize the possibility of simultaneous loss of all transmission lines on a single right-of-way. Other Severe Events such as earthquakes, unusually extreme ice storms, and physical or cyber attacks may also threaten multiple facilities using a common right-of-way.

- While it is common practice to concentrate multiple circuits onto a single right-of-way, consider minimizing the impact of a single mode failure on the facilities should be considered. For example, single circuit towers may be less vulnerable to disruption and facilitate energization when crews are working on adjacent structures.
- Some circuits could be built underground to reduce the vulnerability of all circuits along the right-of-way.

Station Design

The implementation of the NERC Critical Infrastructure Protection (CIP) standards³³ have helped enhance physical and cybersecurity at substations. However, many substations are often not staffed and monitoring is limited to visual security cameras and alarms and control devices used for electrical operation. Suggestions to improve resilience include:

- Install electronic surveillance to facilitate remote visual inspection and assist in setting priorities for operation, repair, and identifying alternatives for restoration.
- Harden structures and control houses to minimize damage and improve restoration efforts.
- To reduce exposure to explosions, use physical separation or blast containment techniques.
- Standardize the use of protection and control devices and schemes to ease repair or replacement. Consider using alternate technologies for backup systems that are simple yet effective.

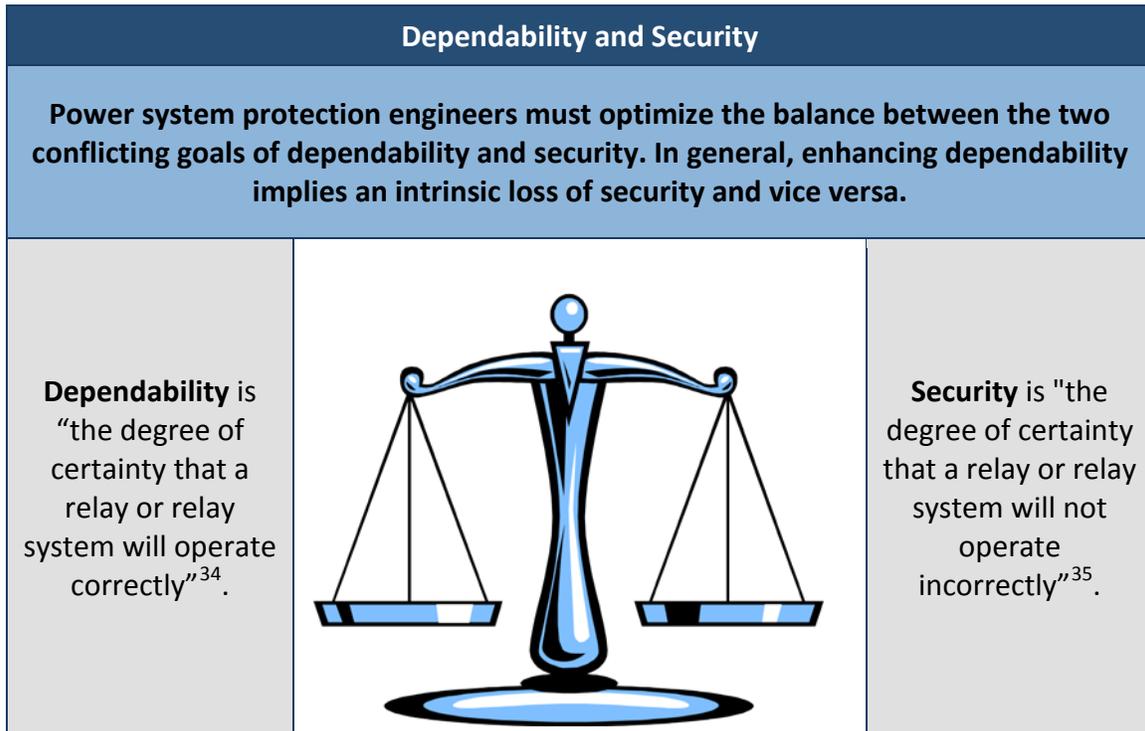
Use of Modular Control Houses by American Electric Power

AEP is working with suppliers to develop modular control houses with Faraday cage shielding of devices and protection cables that would harden critical cyber assets serving large metropolitan areas.

³³ NERC CIP-002 – CIP-009: <http://www.nerc.com/page.php?cid=2|20>

7.0 Protection and Control

This section identifies challenges associated with protection and control systems used to support the reliable operation of the BPS following a Severe Event and a prolonged period of New Normal operation. It is important to understand the differences between a power system protection engineer's two competing objectives.



Protection and control plays a major role in BPS reliability. An analysis of historical NERC outage reports indicates that hidden failures³⁶ are involved in over 70 percent of cascading outages. The probability of a hidden failure occurring is likely greater under the stressed system conditions following a Severe Event. Therefore, the severity of the event and the prolonged duration of the New Normal justify a thorough assessment of protection and control systems to help ensure reliable operation.

Protection schemes depend entirely on the local configuration of the BPS and vary significantly from utility-to-utility and region-to-region. While this section does not provide step-by-step

³⁴ Ref. IEEE Standard for Relays and Relay Systems Associated With Electric Power Apparatus," *IEEE Std C37.90-2005 (Revision of IEEE Std C37.90-1989)*, pp. 0_1-19, 2006.

³⁵ Ibid.

³⁶ A hidden failure is defined as a permanent defect on a relay system that will cause the incorrect removal of a circuit element as a direct consequence of another event [2] Tamroglak, "Analysis of Power System Disturbances due to Relay Hidden Failures," ECE, Virginia Tech, Blacksburg, VA, 1994. As conveyed by the definition, hidden failures remain dormant until a particular event causes its manifestation and associated relay miss-operation.

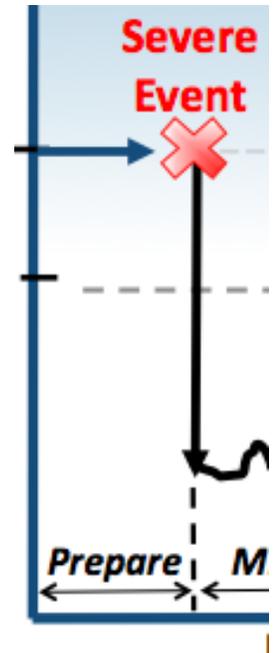
instructions or guidance on specific protection schemes, it does emphasize key considerations and potential mitigation actions to enhance reliable protection and control systems.

7.1 Preparation Phase

The NERC cybersecurity standards³⁷ require that critical cyber assets such as certain protection and control devices and systems be protected. The following offers industry practices best employed prior to a Severe Event.

Physical and Cybersecurity

- Instead of using manufacturer default passwords, consider using strong³⁸ passwords, change them periodically, and use different passwords for each control house and/or each protection relay.
- Consider performing periodic comparisons between “as-left” relay setting files in the field with setting files at the main office.
- Consider monitoring access into substation, control house, and protection relays.
- Consider enhancing physical security of equipment in the switchyard.
- Emphasize “need-to-know” and restrict access to critical assets and information.
- Consider encrypting communications of all critical data.
- Consider having redundant secure communication paths to critical assets to decrease the impact of denial of service attacks and to provide an alternative path for alarm and mitigation action.
- Consider developing procedures to disable bi-directional data flow in substations to prevent network access to protection relays. The intent is to prevent intruders from being able to remotely log into relays and alter relay settings, yet still allow the relays to perform their normal protective function. The procedure should not compromise SCADA data; disable communications from the communication processor to relays, and therefore only allow uni-directional data flow from the relays to the communications processor.



Power Supply to Protection and Auxiliary Systems

- Determine battery backup power requirements for substation loads such as the control house and station service under a Severe Event scenario.
- Consider installing permanent or portable backup generation to charge batteries at critical substations.

³⁷ NERC Cybersecurity standards CIP-002 – CIP-009 <http://www.nerc.com/page.php?cid=2120>

³⁸ US-CERT Cyber Security Tip ST04-002 <http://www.us-cert.gov/cas/tips/ST04-002.html>

- Understand the interdependencies between stored energy in circuit breakers and substation off-site power. For example, spring-spring circuit breakers have stored energy for an open-close-open (O-C-O) operation. The motor to charge the spring mechanism may be AC or DC driven, or both. If the motor is AC driven and the station service transformer is out of service, then only an O-C-O operation is allowed.

Communications Infrastructure

- It may not be possible to operate equipment remotely. Consider the logistics required to dispatch staff to multiple critical substations to monitor and manually operate equipment.
- Understand the interdependencies between protection systems and the communication infrastructure. As an example, consider a Direction Comparison Blocking (DCB) scheme. If the communication between substations is compromised, the scheme will lack security, i.e., the relay may misoperate for a fault outside the protected zone. However, the dependability of the scheme will not be affected.

Control House

- Consider a mobile control house for rapid restoration of critical substations [3]. The design of a mobile control house should address transportation, flexibility to adapt to multiple protection schemes, battery and generator backup power, test and control switches, communication equipment, etc.

Organizational Resilience:

- Consider developing contacts and communication protocols to request the assistance of relay technicians and engineers from neighboring utilities that may not be as affected.
- Consider developing procedures to designate responsibilities to optimize protection and control under the New Normal. Consider tasks such as:
 - Creating a new system model for protection studies.
 - Identifying personnel to assess the adequacy of protection settings considering local circumstances under the New Normal.
 - Identifying personnel to update relay settings.
 - Developing a priority list for protection relays.
- Ensure that appropriate communication channels exist between protection systems engineers and power system operators.

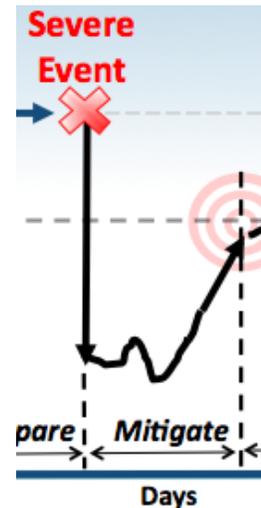
Particular Considerations

- Assess the potential impact of a geomagnetic disturbance on protection schemes. Harmonic distortion³⁹ may cause misoperations [4]. For example, certain shunt capacitor unbalance protection schemes may misoperate as a result of system harmonics. A potential mitigation is to use a voltage differential scheme to protect shunt capacitor banks. Consider the impact on the security-dependability balance on schemes that utilize harmonic restraint; e.g. transformer differential.
- Consider the potential impact of harmonic distortion on power system equipment such as harmonic filters, capacitor banks, SVC, communication equipment, generators.
- Assess the vulnerability of communications infrastructure to ensure data availability, integrity, and confidentiality: point-to-point fiber, power line carrier, synchronous optical networking (SONET) ring, third party provider network, etc.

7.2 Mitigation Phase

Immediately following the Severe Event, protection systems will respond according to predefined settings; adjusting protection relay settings as the event is evolving is not feasible. Response may be limited to confirming the status of protection systems.

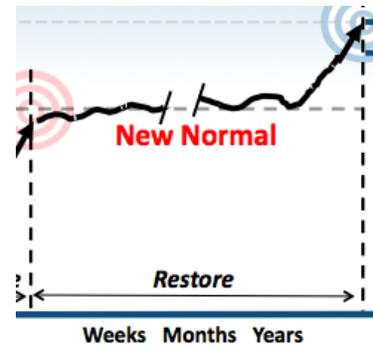
- If a cyber attack is suspected, compare “as-left” setting files in the field with setting files at the main office.
- Taking into consideration potential new islanded configurations, prioritize assessments at critical substations and generation facilities (ref. *Operations, Island Stability* section).



³⁹ Consider the operating quantity measured by protection relays: fundamental component (digital vs. analog filter), RMS values, etc.

7.3 Restoration Phase

Due to the severity of the event under consideration, a highly stressed system should be expected; e.g., potential islanded operation, rotating blackouts, lower system inertia and higher network impedance (i.e., reduced synchronizing torque), different short circuit currents and critical clearing times, reduced stability margins. Through the New Normal, protection relay settings may not be optimal and unwanted operations may occur.



System Restoration and Control

- Consider station service at substations along restoration paths to be critical loads.
- Assess physical damage on protection and control communication channels: wave traps, fiber channels, microwave, etc. Non-pilot distance protection of transmission lines may become primary protection until infrastructure for pilot schemes (that require a communications channel) is provided.
- Remote power system control may be compromised. Dispatch personnel to critical substations for manual operation of equipment.
- Assess physical damage to substation control houses. Ensure adequate protection relay equipment is readily available.
- No damage to protection relay devices is expected after a GMD event. Current transformers may have remanence flux, which can shorten the time-to-saturation; this should not be a problem for high speed protection [4].
- If traditional telemetry or access to SCADA/EMS is compromised, consider utilizing monitoring and control capabilities embedded in microprocessor-based protection relays.

Reliability of Protection Schemes

- Consider revisiting protection settings to enhance the security-dependability performance of the protective equipment. Protection relay settings are developed based on an assumed system state. Such settings may become unreliable under the New Normal; critical clearing times may be reduced, short circuit currents may change, and stability margins may be reduced. It may be possible to optimize the reach of protective zones.
- Consider a reliability bias towards security [7]. Traditionally, protection systems have been biased towards dependability. Under normal conditions, system topology and good stability margins justify such a design. For example, multiple transmission lines provide a number of alternate paths for power to flow and the BPS can withstand losing a single line as a result of conservative protection security provided the remaining transmission lines have sufficient loading margins. Under such conditions, not clearing a fault with primary protection has a greater impact on the system than a relay misoperation due to lack of security. However, under New Normal conditions, the power system may be in a highly "stressed" state. Unnecessary line trips may further

exacerbate system conditions, contribute to the geographical propagation of the disturbance, and may even lead to cascading events and subsequent blackout.

- Consider studying cascading outages. The BPS may not be secure enough to withstand the next contingency (N-1); consider reviewing existing and developing new SPS and RAS schemes.
- If rotating blackouts are implemented, consider studying the impact of cold load pick-up on distribution protection with Distribution Service Providers.
- Assess source strength for distribution circuits. If short circuit currents do not allow protection coordination, consider implementing voltage supervision.
- With stability margins significantly reduced, under frequency load shedding (UFLS), under voltage load shedding (UVLS), and special protection schemes (SPS) may be essential to ensure a reliable operation of the power system. Review and ensure the appropriateness of existing UFLS, UVLS, and SPS schemes [8-14]. Consider deploying additional schemes to better suit the prevailing system state. The main three parameters involved in designing UFLS and UVLS schemes are:
 - When to shed load (threshold setting).
 - How much load to shed.
 - Where to shed load.

Importance of Relay Setting Parameters

All three parameters are important. During the July 1996 WSCC blackout, [12] load was shed at the power sending side which caused several tie-lines to become overloaded which in turn led to a loss of synchronism. In the 1977 New York blackout [15] generator excitation protection tripped several machines after a voltage rise caused by load shedding.

Key Recommendation #18 | Protection and Control

Consider ways to implement large-scale changes in system protection schemes to support islanded operation and changing BPS configurations, and what decision points would be needed.

Key Recommendation #19 | Protection and Control

Consider ways to quickly reconfigure relay settings in the event large-scale changes are needed.

Distribution System Impacts and Mitigations

Impacts and mitigation on protection and control on distribution systems⁴⁰ have been considered in this section.

- Large magnitude geomagnetically induced currents are not expected to flow in the distribution system. However, the impact of harmonic distortion should be considered.

7.4 Training

Due to the challenges posed by operating the power system under the New Normal, personnel training is a critical factor to ensure a resilience power system. Training opportunities may include:

- Consider cross training between distribution and transmission relay technicians and engineers to allow flexible reallocation of personnel.
- Consider developing an instruction manual describing the system protection philosophy. The intent is to facilitate the learning process in case system protection personnel are shared among utilities. The manual should address protection scheme designs, protection relays used, communication equipment needed, etc.
- Before attempting to synchronize islands, ensure that mechanisms are in place to identify and coordinate any changes to protection systems (i.e., SPS, UFLS, UVLS schemes) that could affect neighboring entities.

References

- [1] "IEEE Standard for Relays and Relay Systems Associated With Electric Power Apparatus," *IEEE Std C37.90-2005 (Revision of IEEE Std C37.90-1989)*, pp. 0_1-19, 2006.
- [2] Tamroglak, "Analysis of Power System Disturbances due to Relay Hidden Failures," ECE, Virginia Tech, Blacksburg, VA, 1994.
- [3] R. Mazzatto, M. Leschuk, R. Glass, R. Brown, and D. Schmidt, "Case Study: Mobile Protection Unit for Rapid Power Restoration," *65th Annual Georgia Tech Protective Relaying Conference*, May 2011.
- [4] "Geomagnetic disturbance effects on power systems," *Power Delivery, IEEE Transactions on*, vol. 8, pp. 1206-1216, 1993.
- [5] UCTE, "Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy," ed, 2004.
- [6] NERC, "Final Report on the August 14, 2003 Blackout in the United States and Canada," ed, 2004.
- [7] E. Bernabeu, "Methodology for a Security-Dependability Adaptive Protection Scheme based on Data Mining," Ph.D., ECE, Virginia Tech, Blacksburg, VA, 2009.
- [8] NERC, "Assessment of the Design and Effectiveness of UVLS Program," 2005.

⁴⁰ In general, non-pilot schemes (fuses, sectionalizers, reclosers, over-current relays, etc) are used in distribution systems. The size and radial characteristic of distribution systems dictates such protection philosophy.

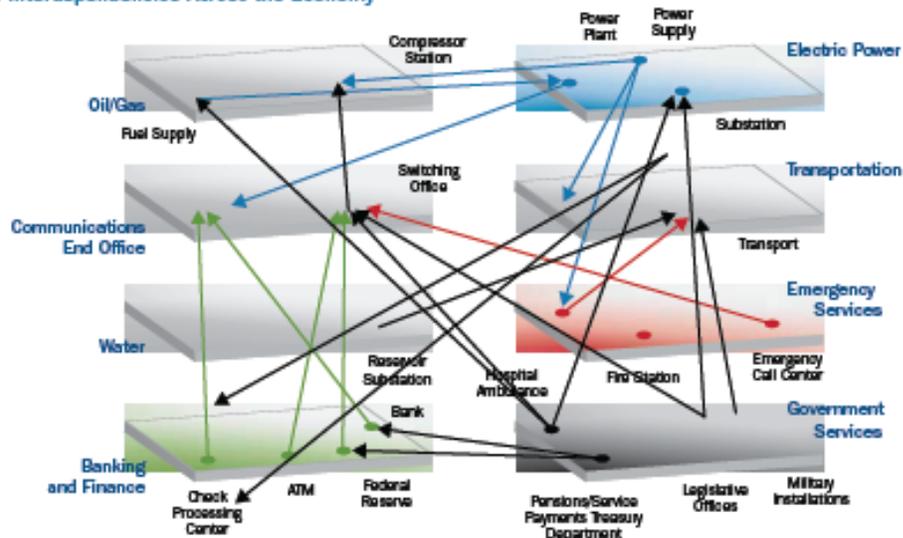
- [9] NERC, "UVLS System Maintenance and Testing," 2005.
- [10] NERC, "Assuring Consistency with Regional UFLS Program Requirements," 2005.
- [11] NERC, "Underfrequency Load Shedding Equipment Maintenance Programs," 2005.
- [12] NERC, "Review of Selected 1996 Electric System Disturbances in North America," 2006.
- [13] NERC, "Under-Voltage Load Shedding Program Data," 2006.
- [14] NERC, "Under-Voltage Load Shedding Program Performance," 2006.
- [15] FERC, "The Con Edison power failure of July 13 and 14, 1977: final staff report," ed. Washington, 1978.

8.0 Interdependencies with Other Critical Infrastructures

A Severe Event that broadly affects the BPS will in all likelihood have a significant impact on other critical infrastructures that depend on the reliable and continuous supply of electricity. Similarly, the BPS relies on other critical infrastructures that are necessary to support BPS restoration and operation. This section considers both aspects of these interdependencies.

- **Figure 6: Critical Infrastructure Interdependencies**⁴¹

Figure 1-8: Interdependencies Across the Economy



The U.S. and Canadian governments have programs in place to encourage greater protection and resilience of our nations' critical infrastructures. In Canada, "The *National Strategy and Action Plan for Critical Infrastructure*⁴² establishes a risk-based approach for strengthening the resiliency of Canada's vital assets and systems such as our food supply, electricity grids, transportation, communications and public safety systems". Similarly, in the United States, the *National Infrastructure Protection Plan*⁴³ prepared by the U.S. Department of Homeland Security identifies 18 critical infrastructures.

⁴¹ Source: Department of Energy, Energy Sector Specific Plan <http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf>

⁴² Public Safety Canada: <http://www.publicsafety.gc.ca/prg/ns/ci/index-eng.aspx>

⁴³ DHS Critical Infrastructure: http://www.dhs.gov/files/programs/gc_1189168948944.shtm

The table below illustrates the extent to which electricity is interdependent with many other infrastructures. These are discussed more fully in later sections.

Table 5: Key BPS Interdependencies		
Critical Infrastructure	BPS Depends on Infrastructure for:	Infrastructure Depends on Electricity for:
Banking and Finance	Funds transfer	Funds transfer, cash distribution, functioning of the economy
Communications	Voice and data services	Voice/data centers and networks, internet providers
Dams (hydroelectric)	Energy source	Station service
Defense Industrial Base	-	Military bases and defense production facilities
Energy – Coal, Oil & Natural Gas	Electricity generation fuel source Backup generators, service vehicle fuel	Fuel production and transportation (pumping)
Energy – Electricity	Station service	Station service
Food and Agriculture	Food production (staff well-being)	Irrigation and food production
Government Facilities	-	Facility service
Healthcare	Staff well-being	Facility service
Information Technology	Automated tools	Facility service
Nuclear	Electricity generation fuel source	Station service, including safety systems
Transportation	Staff and equipment transportation	Communications and control systems operation
Water	Electricity generation cooling Staff well-being	Pumping and processing

The following describes some of the significant dependencies of the BPS on other critical infrastructures needed to support mitigation and restoration through a Severe Event.

8.1 Communications Sector

In addition to affecting the BPS, a Severe Event may also degrade the communications infrastructure. System operators may not be able to rely on telephone, cellular, email or dedicated broadband networks to communicate with entity staff, other entities, and key stakeholders. Alternative communications facilities need to be in-place and tested in advance of a Severe Event.

Effective BPS restoration and continued operation is highly dependent upon the ability to communicate, both voice and data, at all times. The highly interdependent aspect of BPS recovery and the communications infrastructure cannot be over-emphasized. Communications infrastructure and protocols are discussed in further detail in the Communications section.

Recommendations:

Entities should work closely with their communications service-providers to better understand mutual dependencies, identify priorities, and seek ways of mitigating the impact of severe disruptions.

- Identify specific interdependencies between telecommunication infrastructure and BPS infrastructure, such as voice and protection circuits, SCADA, remote terminal units and smart grid devices, necessary for BPS operations (e.g. key telecommunications facilities and their power system restoration paths and priorities).
- Ensure that critical telecommunications users are registered for priority wireless and land-line services such as:
 - U.S. Government Emergency Telecommunications Service⁴⁴ (GETS).
 - U.S. Government Wireless Priority Service (WPS)⁴⁵.
 - Industry Canada's Wireless Priority Service⁴⁶ (WPS).
- Identify risks and hazards such as failures, attacks, High Impact Low Frequency Events and/or congestion etc., that could impair the quality of service continuity, readiness, performance and time response of telecommunications.
- Explore opportunities and needs associated with emerging technologies (e.g., future 700 MHz, 1.8 GHz bandwidth frequencies, WIMAX, wireless priority services).
- Take mitigation measures (e.g., operational procedure changes, changes to priorities and procedures in restoration plans, design considerations, inter-entity information exchange).

⁴⁴ U.S. GETS <http://gets.ncs.gov/>

⁴⁵ U.S. WPS <http://wps.ncs.gov/use.html>

⁴⁶ Canadian WPS http://www.ic.gc.ca/eic/site/et-tdu.nsf/eng/h_wi00016.html

Key Recommendation #20 | Interdependencies with other Critical Infrastructures

Consider working with communications service providers to identify which of their facilities are critical to BPS operations. Determine which BPS and distribution facilities supply them and what backup power capacity is in-place (e.g., batteries, standby generators).

8.2 Dams (hydroelectric) Sector

Hydroelectric dams provide substantial generation in many regions of North America, and often provide critical blackstart services, as well as control water flows for irrigation, navigation, and elevation. Failure of key dams could have a significant effect on BPS operations.

Recommendations:

- Operators should develop a comprehensive understanding of the location and characteristics of hydroelectric facilities in their area and consider their ability to restart these facilities following a blackout.
- Some dams may be of more critical importance in their role of navigation, such as enabling coal supply via barge to key generating stations. Operational plans should identify the generators dependent upon navigable inland waterway supply for fuel transport or cooling water.

8.3 Energy Sector

The energy sector, in addition to electricity, includes natural gas, petroleum, and coal. Disruption to any of these fuel infrastructures could seriously impede BPS restoration.

Recommendations – Coal

- According to the U.S. Energy Information Administration, coal currently accounts for almost half of U.S. electricity generation⁴⁷. Coal-fired generators are dependent upon frequent, in some cases daily, supply of coal from mine to power plant.
- Operators should ascertain and maintain cognizance of on-hand fuel supplies and storage capacity at coal fired generators.
- Operators should understand the coal transport routes in their area, consider possible supply disruption points, and explore alternate routes or transport modes.
- Operators should develop contingency plans around “out of fuel” scenarios in the coal fleet. What would New Normal operation look like in a short coal supply scenario?

⁴⁷ <http://www.eia.gov/energyexplained>

Recommendations – Natural Gas

- Entities should understand⁴⁸ the gas pipeline networks and arrangements in place to supply gas-fired generators in their footprint (e.g., gas-fired generators and pipelines that supply them, communications protocols during normal operations and emergencies).
- System operators should know which pipeline compressor facilities are gas versus electric powered and what gas pressure drops might be in the event of a sustained BPS outage. System operators will need to work with gas counterparts to understand power outage impacts on gas supply, and vice versa, and identify which are priority loads.
- In the event of a physical or cyber attack on gas infrastructure (including gas SCADA systems), system operators should consider the impact on gas-fired generation, and encourage their gas counterparts to share their plans to respond and restore operation.
- System operators should coordinate with gas operations personnel concerning their load shedding priorities.

Recommendations – Oil

- Oil is a relatively minor fuel source for the BPS, however system operators should assume these units will be unavailable due to unprecedented demand for diesel and gasoline fuel for standby and backup generators.
- Diesel fuel is needed for emergency standby generators at all critical BPS facilities that are without a reliable supply of power from the BPS during restoration. Entities should review contractual arrangements and establish priorities with fuel suppliers.
- Diesel and gasoline fuel is needed for transportation purposes. Regional Entities may wish to consider establishing regional fuel reserves for use in severe emergencies when normal fuel delivery channels may not be available for extended periods or when competing fuel demands (e.g., National Defense) take precedence for available supplies.

Key Recommendation # 21 | Interdependencies with Other Critical Infrastructures

Consider alternate suppliers, transportation paths, and agreements to support generating station fuel supply chains (e.g., coal, natural gas).

8.4 Information Technology Sector

Reliable operation of the BPS is highly dependent on the IT sector. IT is in turn heavily dependent upon electricity. Over the past decade, many entities have chosen to purchase or lease commercially available IT⁴⁹ systems and networks rather than build and support their own. Cyber attacks continue to increase in frequency and sophistication. System operators should be aware of the extent to which they rely on IT infrastructure, and should develop plans

⁴⁸ Ref. NERC Natural Gas and Electric Power Interdependency report http://www.nerc.com/files/Gas_Electric_Interdependencies_Phase_I.pdf

⁴⁹ In the context of this section, IT refers to entity business systems, rather than operational EMS or SCADA systems.

and procedures to enable recovery and New Normal operations in the event of significant disruption to the IT infrastructure.

Recommendations:

- Operations staff should work with entity IT staff to develop a comprehensive understanding of the IT infrastructure on which BPS operations are dependent. Consider elements of the infrastructure outside entity direct control, network interfaces (if any) with operational systems such as EMS and SCADA, redundant systems and backup plans.
- Consider developing detailed operational plans in the event of major disruption to the internal or external IT infrastructure and Internet.
- Develop backup plans for telemetry that is critical to BPS operations in the event of a major IT infrastructure disruption.

Key Recommendation #22 | Interdependencies with Other Critical Infrastructures

Consider working with information technology service providers that are critical to BPS operations and consider augmenting the subject matter expertise of staff and suppliers to support these systems.

8.5 Nuclear Sector

Nuclear power plants are of course a key part of the generation infrastructure, providing 20 percent of electricity in the U.S. and about 15 percent in Canada. This segment of the power sector has long been heavily regulated from a safety and security perspective. Because of its unique nature and national security importance, the nuclear sector was designated as its own critical infrastructure by the U.S. Department of Homeland Security, and has its own Sector Specific Plan under the National Infrastructure Protection Plan (NIPP). System operators are well versed in handling nuclear plant outages, and in the dependence of nuclear plants on BPS-supplied electricity. However, recent incidents, such as Fukushima, have focused renewed attention on the interdependencies of nuclear plants, the grid, backup fuel supply for cooling, and the transportation infrastructure to move that fuel. BPS restoration and New Normal operation should take into account the disruption of and potential long-term unavailability of key nuclear power plants.

Recommendations:

- The industry is extensively studying the lessons learned from Fukushima. These lessons should be incorporated into BPS restoration and recovery plans.
- Nuclear plant operators and system operators should carefully calibrate plans and procedures⁵⁰ in the event of major disruption to either infrastructure.

⁵⁰ NERC standard NUC-001 Nuclear Plant Interface Coordination <http://www.nerc.com/page.php?cid=2|20>

- As we have seen from recent history, emergency cooling for nuclear plants highlights several key interdependencies: water, fuel, and transportation. Recovery plans and procedures should take account of these infrastructure interdependencies.
- Once off-line, nuclear plants can be out of service for extended periods. Recovery and New Normal operational plans should consider these implications carefully, particularly if nuclear generation provides a substantial source of energy to the area.

Key Recommendation #23 | Interdependencies with Other Critical Infrastructures

Consider alternate means to supply BPS power to nuclear plants and confirm these loads as critical to restoration and public safety.

8.6 Transportation Sector

The transportation infrastructure is highly complex. It includes rail, waterborne transport, surface transport, and aviation as well as pipelines that transport natural gas, crude oil, petroleum products, and water. All of these infrastructures are critically important to BPS operations. Almost half of generation is dependent upon coal that is transported via rail and barge. (Barge transport can be very dependent upon river/navigation conditions, including flooding, low water, and accidents.) Pipelines move the natural gas that fuels a quarter of the generation fleet, and is forecast to increase over time. Surface transport moves fuel for backup generation and mobility. In the future, electric vehicles will introduce new interdependencies as they consume electricity and may provide new demand response opportunities. Disruptions to any of these infrastructures can heavily impact BPS restoration and New Normal operations.

Recommendations:

- Emergency plans should be developed that “work backward” to inventory the transport dependencies affecting BPS operations, including basic requirements such as transporting workers to and from work locations.
- Emergency plans should identify suppliers of diesel fuel and gasoline for service vehicles and emergency backup generation and review how these supplies will be prioritized through a Severe Event.
- Backup and re-routing plans should be developed in the event of major disruption to primary transport networks. This could include secondary and tertiary routing plans to move coal, gas, and petroleum products. Disablement of a key river lock or railroad bridge, or key pipeline, could seriously affect BPS restoration. Alternative routing/sourcing should be planned for in advance.
 - In addition to evaluating existing stockpiles at generating stations, Operators should consider re-establishing coal inventory needs if operating in an islanded configuration for a considerable period of time, and consider if coal can be re-dispatched to more critical generators.
 - Operators should work with rail service providers and government to consider how to prioritize the shipment of coal or other fuels to priority generators.

- Operators should consider consulting with government to consider establishing strategic reserves of key fuels to be used in the event of significant supply disruption. This could be a shared regional system, modeled on the U.S. Strategic Petroleum Reserve.
- Transportation dependencies go beyond fuels. The transportation of key pieces of equipment, such as transformers⁵¹, and other spare parts essential to BPS restoration. The same planning should be considered for these other items, to include alternative sourcing and transport mechanisms.

8.7 Critical Infrastructure Sectors that Depend on Electricity

All critical infrastructures depend on electricity to varying degrees. System operators, working in consultation with other critical infrastructures and possibly local, state/provincial, or federal government authorities will need to prioritize loads and understand the extent to which they will be supplied through the mitigation and restoration phases following a Severe Event. Some of these infrastructure sectors and their importance in a Severe Event are briefly described below.

- **Government and Emergency Services:** In a Severe Event affecting the BPS, priority loads may include certain government loads, particularly those with no backup emergency power source. This may include police/fire, emergency services, command centers, and key military facilities. This will be critical to ensuring law and order and effective governance.
- **Defense Industrial Base:** Should a Severe Event be associated with an act of war, or a substantial threat to the National Security, supplying key elements of the defense community and its industrial base would become a priority load.
- **Water:** Water is essential for life. Failure to treat wastewater could result in widespread disease. Hence, supplying electricity for water and wastewater treatment plants and pumping stations will likely be a high priority load for restoration.
- **Healthcare:** Hospitals and healthcare facilities are always a high priority in an outage situation, and will be in any Severe Event to handle injuries or disease.
- **Agriculture and Food:** Food supply will be an important priority in a Severe Event. Electricity for irrigation pumping, food processing, and related purposes will be essential.
- **Banking and Finance:** An important priority will be to restore and maintain commerce. Thus the banking sector will be a priority load.

System operators should work with government authorities and other stakeholders to develop a plan for addressing these critical infrastructure sectors in the event of a severe BPS disruption. Most operators know their critical and priority loads under normal recovery operations, such as hurricanes and ice storms. However, new protocols may need to be

⁵¹ Ref. NERC's Spare Equipment Database program <http://www.nerc.com/filez/sedtf.html>

developed to address these loads in the context of BPS restoration and New Normal operation after a Severe Event.

Training and Exercises

Training will be an absolutely critical element for personnel at all levels in order to gain an understanding of what types of conditions may be encountered in all phases of an emergency, and what the key interdependencies could look like. System Operators, field, and support staff will need this training as will senior management and other key stakeholders, including Government officials, law enforcement, defense, etc. Representatives of interconnected infrastructures should also be included so that information can be shared on key interdependencies and likely response patterns (this can avoid recovery procedures working against each other). The concept of a multi-sector New Normal should be a main theme of this training.

The training cannot envision every possibility. A major part of the training (like survival training) is to engender resourcefulness and flexibility in operational personnel. They understand the outlines of the problem and can then react to the situations at hand.

Realistic exercises should be a key part of the program. Exercises should include BPS personnel at all levels, plus key government representatives, and subject matter experts from other critical infrastructures. The exercises should be carefully documented and thorough after action reports prepared so that learning can be factored into planning and continuous improvement.

These activities should also be coordinated with the National Infrastructure Protection Plan, the National Response Plan and similar coordination elements of the federal and state/provincial governments of both countries.

9.0 Coordination with Government

Local, state/provincial and federal governments (government authorities) are key stakeholders in the electricity industry's response to a Severe Event. These government authorities are responsible for emergency planning and response, developing energy security and reliability policies. In the event of a Severe Event that spans a broad geographic area, government authorities – and perhaps the military – will have a large role to play. Just as the response by electricity entities to any Severe Event will be driven through local and regional entities first and foremost, the response from government will also likely be foremost a local and state/provincial response. As such it is important to be prepared to work with government authorities at all levels:

- Plan for a Severe Event, share your plan with government authorities, and know their plans.
- Understand local and state/provincial government concerns and provide them with information that will help address these concerns.
- Understand in advance how government may be able to assist during a Severe Event. Government authorities may be able to assist by providing resources or information.

This section provides a number of recommendations to enhance communication and coordination on the following topics:

- Overview of government authorities
- Coordination and communications prior to a Severe Event: planning, exercising, and training
- Initial communication and coordination
- Coordination and communication during restoration

9.1 Overview of Government Authorities

In order for entities to determine the government agencies they will need to coordinate with, entities need to understand the roles that government and first responders play, as well as their authorities and legal responsibilities. This will avoid potential conflicts, enhance coordination, and help each other understand respective needs. Entities charged with directing response and restoration should be familiar with government procedures for declaring emergencies at the local, state/provincial and federal levels. The laws, regulations, and plans for declaring emergencies and invoking emergency authorities are readily available on government websites. Entities should review the relevant emergency-related legislation and plans, understand the roles and responsibilities, and determine in advance of a Severe Event their points of contact with the appropriate government authorities. Involving these points of contact in entity emergency exercises will enhance entity understanding of the role of government authorities and help build positive relationships.

Some examples of government authorities involved in managing emergencies include:

- **Local and state/provincial emergency management agencies** and first responders, who prepare for and respond to all emergencies, especially those with responsibilities for the energy sector. These organizations are on the front line of emergency response at the local and state/provincial levels.
- **The lead authority for emergencies (usually activated at the Emergency Operations Center).** State/provincial governments have a designated primary contact for managing emergencies.
- **State Governors** and provincial Premiers possess emergency authorities that they can exercise to mitigate the impacts of emergencies. Increasingly, state/provincial authorities (eg. **State Homeland Security Directors**) have protection and vulnerability assessment programs in place involving the critical infrastructure sectors.
- **State/Provincial regulators, such as public utility commissions,** who oversee and regulate multiple sectors and systems, such as natural gas, telecommunications, and water systems, as well as important elements of the transportation infrastructure. This provides them with the capability to connect information between interdependent systems, and may also provide a nexus of infrastructure information that crosses a number of sectors at once. **State/provincial energy offices** typically serve many energy-related functions at the state/provincial level, including coordinating responses to energy emergencies, developing state energy emergency plans, and developing practices to improve energy security and reliability at the state-level.

Key Recommendation #24 | Coordination with Government

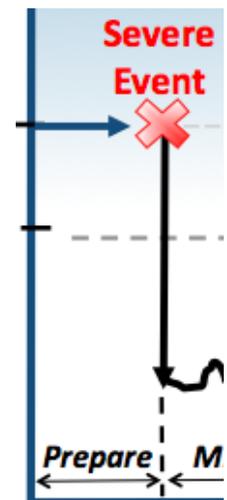
Confirm the roles, authorities, and points of contact between BPS entities and as appropriate, local, state/provincial, and federal governments.

9.2 Coordination and Communications Prior to an Event: Planning, Exercising, and Training

Critical and priority loads: Entities should work with government at all levels to inform them of the power system loads considered critical to power system restoration. Entities should also consult with government to identify priority loads that are essential to public health and safety. Establishing a common understanding of these loads prior to a Severe Event will help provide a basis to confirm or adjust these priorities, depending on the specific circumstances following a Severe Event.

Key Recommendation #25 | Coordination with Government

Coordinate with local and state/provincial government authorities and consumer stakeholders to identify priority loads to mitigate the impact on public health and safety.



Requesting regulatory exemptions and waivers: Entities understand that its operations need to comply with all applicable international, federal, state/provincial, local laws, standards (e.g., NERC Reliability Standards, OSHA, and Department of Transportation), codes, executive orders and regulations. However, during a Severe Event, entities should consider seeking exemptions from certain regulations if this helps improve overall public safety.

Entities should identify waivers they may request from state/provincial and federal agencies to continue operations under stressed conditions (e.g., environmental emissions, truck driver hours). Identify entity and agency emergency contact information and know each waiver's limitations (i.e. expiration and renewal terms). Work with government authorities to confirm detailed procedures. Keep any required forms available and completed in advance to the extent possible, and review them annually.

Key Recommendation #26 | Coordination with Government

Consider developing a list of regulatory exemptions or waivers that will materially improve restoration and operation (e.g., plant emissions, truck driver hours) and consult with state/provincial and federal agencies.

Credentialing: Government first responders (e.g., police, fire, ambulance) have become more aware in recent years of the need to provide access to critical infrastructure work crews. Access to the affected area will be important as soon as it can be provided safely. If possible, access policies should be established with government authorities prior to a Severe Event. Areas with a history of reliance on mutual assistance for recurring disasters (such as for hurricane response) may have protocols in place; in the event of a Severe Event some protocols (depending on communications systems that may not be operational) may need to be available for use without transmittal, or a working access and credentialing protocol may be needed.

Recommendations:

- Consider consulting with government authorities to understand what access policies may be in place during a Severe Event.
- Consider having entity staff meet with local law enforcement personnel to discuss access requirements and build a cooperative relationships.

Considerations:

- Do you know what kind of documentation would be needed to reenter affected areas?
- Is there a plan in place to procure and disseminate the necessary documents if communications systems are down?
- Have you discussed an access plan with government authorities that cover you, your mutual aid, and contractors? Consider alternatives in case information technology is compromised.

Building Trust with Decision Makers: Realistic exercises that involve entity personnel at all levels, key government staff, and other critical infrastructures are essential to preparedness. Following exercises, participants should identify action items and next steps for future planning and continuous improvement.

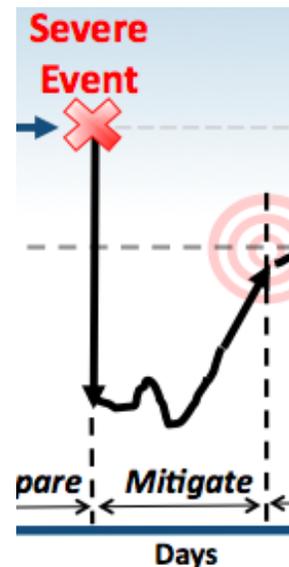
Budgets: Governments have the means to declare a state of emergency and invoke the authorities needed to respond to the situation. Entity emergency management plans should recognize government roles and responsibilities when they exercise that authority, and how they will become aware of changes that may impact entity operations. Entities should engage with government to help ensure a common understanding of mutual needs.

9.3 Initial Communication and Coordination

It will be very important that entities begin communicating with the appropriate government authorities at a very early stage of a Severe Event to provide updates both on a scheduled basis, and as urgent developments occur. This will help ensure that decisions are made using the best available information.

Some of the key issues that should be communicated with government authorities, especially with local and state/provincial emergency operations centers, include:

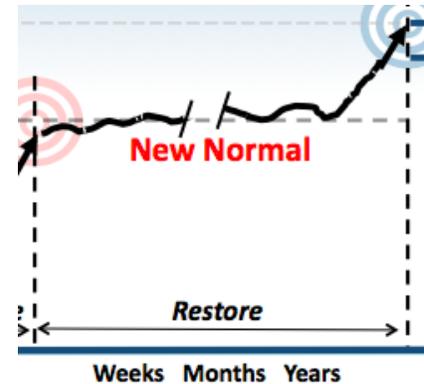
- Restoration assessment and prognosis
- Share needs and priorities
- Coordinate with other critical infrastructures
- Coordinate public announcements and schedules for voluntary and mandatory load shedding, including rotating blackouts
- Requests for protection and security



Recommendation: Entities should consider establishing crisis management teams that consist of broad stakeholder and technical representation and establish clear lines of communication with government. Similar to what many entities do during major weather events entities should consider co-locating at their state/provincial emergency operations centers around-the-clock for as long as necessary.

9.4 Coordination and Communication During Restoration

Restoration and operation through the New Normal period will require scarce resources to be continuously reprioritized and reallocated. Government is ultimately the locus for determining public health and safety priorities for resource allocation, and as such, government authorities will need information about what supplies, resources, and materials are available, as well as the prospects and progress of restoration in order to make informed decisions.



Electricity entities in Canada and the U.S. have a long history of sharing resources and work crews to aid restoration following hurricanes and severe floods. In an effort to facilitate crossing the U.S. and Canadian border during emergencies, the Canadian Electricity Association is working with the Canadian Border Security Agency and the U.S. Department of Homeland Security. A *Cross-Border Mutual Aid Assistance Agreement* has been prepared and is expected to be implemented in the near future.

Government authorities and electricity entities should have primary, alternate, and possibly tertiary contacts and means of contact, including provisions for around-the-clock contact. Hard-copy contact information lists should be maintained and reviewed at least annually.

Entities need to be familiar with government emergency management structures. For examples, entities in the U.S. should be familiar with the government’s Incident Command System [ICS]/National Incident Management System [NIMS] principles⁵². Requests by entities should be referred through the appropriate channels.

Continual Review of Legal Authority: Legislation and supporting regulations define the role of government agencies during emergencies. Entities should be familiar with these and understand how emergency authorities may affect entity operations. During a Severe Event, government may revise these or enact new authorities. Entities will need to stay abreast of these changes, understand how they may affect the entity, and have mechanisms in place to communicate them quickly across the entity as appropriate.

Understanding Impacts: It is important for the government to understand the role played by BPS entities and vice versa. Requests for information should not distract or impede those who are engaged in operational roles such as restoration and crisis response. It is also important that government understand the actions that asset operators will be taking, and that actions will be underway independent of any emergency declaration by government. However, as the days add up to weeks after a Severe Event, decisions regarding changing priorities will be required.

⁵² Ref. <http://training.fema.gov/IS/NIMS.asp>

Recommendation: Government authorities and electricity entities should coordinate closely so they are prepared to explain the actions they are taking or are about to take, and why. Decision-makers will need to understand the second and third order effects of making such priority selections. For example:

- The sequence of electricity service restoration to consumers in different geographical areas or regions will vary depending on circumstances such as the availability of resources and the nature of any damages to equipment.
- If the cause of the Severe Event is continuing, restoration may need to be halted, or re-started.
- If fuel is not prioritized to communications facilities, the ability to operate portions of the BPS will be severely limited.

References

- <http://disaster.ifas.ufl.edu/PDFS/CHAP03/D03-07.PDF>
- <http://www.nyu.edu/intercep/businesscase/index.html> - New York University / International Center for Enterprise Preparedness
- <http://www.fema.gov/privatesector/preparedness/>
- http://www.oe.energy.gov/our_organization/iser.htm - Department of Energy
- http://www.fema.gov/pdf/about/stafford_act.pdf
- <http://www.naruc.org/cipbriefs/> - NARUC briefs on critical infrastructure protection
- <http://www.naseo.org/eaguidelines/> - NASEO and NARUC Energy Assurance Planning guidance

10.0 Taking Care of People

The electricity sector has extensive experience planning for emergencies. While these plans often focus on repairing or replacing physical assets and taking the necessary operating actions, success is highly dependent on our most important asset – knowledgeable, capable, and available personnel. Without question, a Severe Event will put great stresses on personnel throughout the New Normal period.

This section provides guidance on topics that should be included in an entity's disaster recovery plan or business continuity plan. Much of this information is based on past experience in disaster response operations and also includes lessons learned in everyday operations. While many of the suggestions might seem obvious, past experience indicates they may not be achievable if not planned in advance of an event. This guidance is provided in the context that can easily be modified for inclusion in entity plans.

This section discusses the following topics that should be considered as part of an entity's plans.

- Accommodation
- Safety considerations
- Employee and family Issues
- Respite facilities
- Counseling

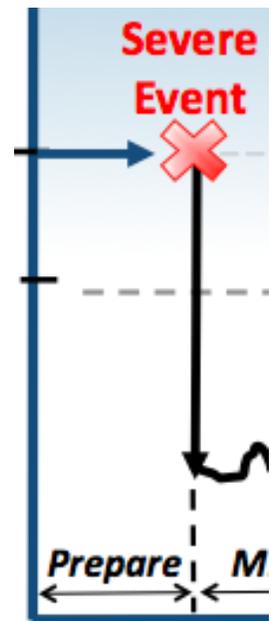
10.1 Accommodation

Consider alternate housing arrangements that would be suitable during the Mitigation Phase as well as the longer Restoration Phase. Traditional support infrastructure such as hotels, restaurants, and grocery stores will most likely not be available or unable to support the influx of personnel and displaced residents of the affected areas.

An example of an extended restoration event is the recovery of Entergy's system after the catastrophic damage caused by Hurricane Katrina and the subsequent failure of the levy system around New Orleans. Because of its experience, Entergy modified its existing plans to include many of the recommendations provided in this section.

Recommendations

Housing options could include rental housing, apartments, hotels, tent cities, campgrounds, employee travel trailers or campers, cruise ships or military vessels, and federal, state/provincial shelter facilities. Identify points of contact to determine how these options would be acquired and implemented.



10.2 Safety Considerations

Maintaining operations through the New Normal period can be stressful and hazardous. There is never a good time for an accident or operating error, but this is especially true during a Severe Event. Paradoxically, experience has shown that safety rates can be better during major disaster response and restoration than during routine operations. This may in part be due to the initial increase in adrenalin and commitment to tasks that are of immense value to their peers and the general public. But it is not reasonable to assume that this will continue through the weeks or months of a Severe Event. The onset of fatigue and stress will contribute to increased errors. Accidents or operating errors can delay or even halt restoration efforts.

For entity incident and disaster planning, safety for personnel families and personnel performing operational restoration is a primary consideration. While many of these apply to “normal” emergencies, they can become particularly important during a Severe Event.

Entergy’s Experience from Hurricane Katrina

Entergy’s headquarters and nearly 1,000 employee homes were initially uninhabitable. Entergy secured office space to replace its New Orleans area work locations and arranged interim housing for displaced employees for 7 months. Entergy has since implemented long-term office relocations as an integral part of its disaster recovery strategy.

Recommendations

- **Advanced warning** – If the Severe Event is preceded with advance warning, provide guidance on when and where to evacuate.
- **Proper permits** – Many entities require specific certifications and permits. Procedures should be documented on what permits and certifications may be waived through a Severe Event.
- **Safety teams to oversee work conditions** – Safety teams should monitor for signs of fatigue and stress and have the authority to stop work when conditions are unsafe. This may require an increased role for the entity’s internal health and safety oversight organization.
- **Transportation** – Transporting personnel safely and reliably between work and rest centers will decrease stress.
- **Stock of supplies** – For shorter-term events, experts recommend having a minimum of a seven-day supply that will need to be adjusted for a Severe Event, but the same considerations for health and nutrition are applicable. Entities should consider stocking non-perishable foods and food in pouches; proteins, fruits and vegetables; and foods that do not require extra cooking and can be eaten cold if necessary. Store water, at least one gallon per person per day. Remember to have on-hand manual can openers, cooking utensils, pots and pans. Include aluminum foil, paper towels, garbage bags and disposable cleaning wipes. Have sufficient rotated stocks of batteries for flashlights and radios. Make up a good first aid kit and stock up on cleaning supplies, especially bleach, gloves and heavy-duty garbage bags. Keep freshly stocked emergency kits with vitamins and over-the-counter medications that might be needed, such as pain relievers, antacids and cold-relief medications.

- **Notification of well-being** – Entities should provide communication options to allow personnel to contact family. Personnel should be patient as communication systems are likely to be disrupted. Typically, personnel will establish a family communication plan that establishes a time frame for contacting family after the event.
- **Encourage personnel to develop an individual or family Emergency Medication Plan** – Entities could develop and provide a sample plan to its employees. This may include the following:
 - Consult an individual’s healthcare provider, especially for complicated or difficult-to-administer medications, such as those requiring pumps or nebulizers.
 - All medications should be kept in one location in the home, to expedite any evacuations or ease in retrieving medications after an event. Along with your prescription identification card, individuals should keep a list of their medications and those of other family members, including drug name, strength, dosage form and frequency.
 - If there is a shortage of medications for personnel, entities may consider helping to secure medications or work to have key personnel placed on a priority list for medications.
 - Keep the names and phone numbers of your doctor and the pharmacy that filled your prescriptions in your wallet. If possible, the entity should work with a local pharmacy or its mail-order service to help personnel address any prescription needs.
- **Personal protective equipment** – Ensure that an entity has and provides to field personnel the appropriate personal protective equipment.
- **Personnel in new roles** – When redirecting personnel into new roles which require more physical effort, leaders must take into consideration any health issues a staff member may have been able to control in under normal circumstances, but may be further exacerbated after a Severe Event.
- **Plan for medical response** – Enhance first-aid packs, and prepare for on-site medical care teams.
- **Worker rest** – Manage worker rest based on conditions and tasks. Ensure appropriate rest time between and during work shifts and provide safe, comfortable, and quiet facilities.
- **Security** – Provide security in areas where potential civil unrest may erupt that includes personnel guidance on how to manage such unrest.

10.3 Employee and Family Issues

Every employee and his family should have a personal emergency plan that recognizes and mitigates the risks faced in a given community. An entity’s business continuity or disaster recovery plan should identify the relative criticality of each job function and inform employees potentially affected. As part of this planning, the entity should clearly communicate the level of support it will provide in situations covered by business continuity plans or disaster recovery plans so that employees in non-critical job functions may also plan appropriately. Employees who do not fill critical job functions should be instructed to check-in for reassignment.

During an event, health and safety concerns are a primary consideration. During a Severe Event, this concern extends to all personnel and their families. The success of restoration for an entity could hinge on whether the families of employees are safe and able to get back to some semblance of a normal set of activities.

Recommendations

Some key topics that should be considered in disaster recovery plans that may need to be in place for months following a Severe Event include the following:

- Supplies and respite
- Communications
- Transportation
- Safety
- Education
- Child/elder care
- Secure homes
- Relocating employee's family to safety as necessary
- Food & necessities
- Continuity of pay and banking services

Operating Iraq's Grid in an Unstable Security Environment
With Iraq's unstable security situation and a shortage of system operators, generation, transmission and distribution station staff were expected to live on site. Given the high levels of sectarian and personal violence many families of staff were moved into the stations as well. Often the station staff would provide the residents surrounding the station with scarce electricity and create a friendly buffer around the station.

10.4 Respite Facilities

Immediately following a Severe Event, basic needs need to be met to help reduce personnel and family stress. Although the following recommendations appear to address the immediate need after a Severe Event, the human factor related to respite to prevent burn-out is something that will need to be addressed throughout the New Normal period.

Recommendations

Rest Area

- Provide an area that is covered and dry.
- The area should contain heating and cooling with good ventilation.
- Provide for personnel to sit or lie down.
- Provide an area suitable for activities and discussions, and a separate quieter area for rest.

Water

- Ensure personnel stay well hydrated.

Respite Facilities following the 9/11 Terrorist Attacks
During the search and rescue and the subsequent clean-up at Ground Zero after the 9/11 terrorist attacks on New York, respite centers remained in the work-zone for an extended period of time.

- Reserve potable water for the essentials of drinking and food preparation. Other treated water may be suitable for showering and hand washing.
- Ensure water is treated and managed properly; serious diseases can be transmitted by untreated water.
- Properly dispose of or recirculate gray water to protect the potable water supply.

Food

- Ensure adequate supplies of healthy food. Consider long shelf-life foods, stock-piled in advance.
- Maintain clean and comfortable meal facilities.
- Store perishable foods below 45 °F and serve heated food above 140 °F.
- Dispose of perishable foods not properly stored after 4 hours.
- Consider weather conditions and temperatures to determine whether hot or cold foods should be served.

Hygiene

- Provide hand washing or disinfecting facilities at all food service areas, rest rooms, and disposal areas. Disinfecting and hand washing is the single-most important measure in preventing food-borne illness and must be enforced at all times.
- Provide individual hand cleansers and liquid hand sanitizing gel to personnel.
- Provide for bathing and clothes washing at respite facilities.

Rest Rooms and Waste Disposal

- Ensure portable latrines are available, cleaned regularly, and located in appropriate areas.
- Ensure waste is managed appropriately and designate storage locations away from living and work areas.

10.5 Counseling

Everyone involved in maintaining operations during an event are dealing with increased stress and anxiety. In certain events, there is a potential of the tragic loss of life and material possessions that will affect each person involved. Personnel must seek care from a stress management team or other options provided by the entity when they feel overwhelmed or unable to cope with maintaining operations. Many times during stressful situations personnel need someone to talk to that is not involved in the situation so they are not burdening their relationships with others close to them.

Recommendations

During normal business operations, Human Resource (HR) departments usually have the responsibility of benefits that may include various types of counseling programs. HR may want to consider expanding their business continuity plan to include counseling programs for

incidents. An entity may consider establishing a counseling center at a respite location. Because situational stress and loss of life could include personnel (internal and external) and personnel's family members, the business continuity plan should establish a process to expand the needs of its typical employee assistance program to deal with needs of those individuals outside its organization. Remember personnel performance can be affected by the problems of an employee's immediate family members. In addition to the services provided by the entity, personnel may seek guidance from local religious leaders.

Key Recommendation #27 | Taking Care of People

Consider ways to support the health, safety, and well-being of personnel and their families in the face of extraordinarily demanding circumstances.

References

National Rural Electric Cooperative Preparedness Plans, Building Operations Plans

Communities of the National Capital Region, Be Ready Make a Plan, www.makeaplan.org

PUBLIC ASSISTANCE PROGRAM (Public Assistance, Emergency, Fire Suppression)
DCA/DEM/BRM Recovery Office STANDARD OPERATING GUIDLINES the Florida Division of
Emergency Management web site is: <http://www.FloridaDisaster.org>

Preparing Makes Sense Get Ready Now Brochure, United States Department of Homeland
Security www.ready.gov/.../Ready_Brochure_Screen_EN_20040129.pdf

A Guide to Business Continuity by James C. Barnes, 2001, Wiley Press, ISBN: 0-471-53015-8.

Security Planning & Disaster Recovery by Eric Maiwald and William Sieglein, 2002, McGraw-Hill/Osborne Press, ISBN: 0-07-222463-0

Business Continuity Planning edited by Ken Doughty, 2001, Auerbach Publications, ISBN: 0-8493-0907-7

Business Resumption Planning by Edward S. Devlin, Cole H. Emerson, Leo A. Wrobel, Jr, and Mark Desman, 2001, Auerbach Publications, ISBN: 0-8493-9945-9

11.0 Logistics and Self Sustained Operations

This section identifies the challenges associated with the logistics of acquiring, delivering, and replacing or repairing assets damaged in a Severe Event and provides guidance on effective logistics to support operations through the New Normal period.

The key to identifying the best use of resources is dependent on the entity's ability to respond and think "outside the box" of normal planning for emergencies. Many of the items suggested are counter-intuitive to operating in a normal environment. Of necessity, many decisions will be spur of the moment decisions and may have un-intended consequences later as restoration progresses from the New Normal period to pre-event reliability. For example, suppose early in the restoration process a decision is made to cannibalize a substation for parts to rebuild other substations. As load continues to be restored over the New Normal time period, eventually the substation that was cannibalized will need to be rebuilt.

Decision-makers will need to understand the current operating situation and prioritize logistical needs in the absence of much of the information normally available. Initially, the efforts will focus on dispatching existing inventory to restore the critical loads essential to BPS restoration. Efforts will then rapidly shift to dispatching inventory to support priority loads, many of which will be on the distribution network.

Procurement processes suitable for normal operations to meet an entity's policies or government requirements may need to change to provide the flexibility and responsiveness needed during a Severe Event.

11.1 Specialized Equipment

Specialized equipment such as high voltage transformers, circuit breakers, turbines, phase shifters, and series capacitors often take a year or longer to procure and build. Consider the following:

- Participate in spare equipment consortiums that allow the use of other's spare inventory (e.g., NERC's Spare Equipment Database program⁵³).
- Locate spare equipment at a site that is more secure than the sites where they may be needed.
- Develop agreements with other utilities to share spare or redundant equipment. If agreements already exist, discuss the implications of a Severe Event with the participating entities and consider how decisions would be made to appropriately allocate spare equipment. This is important because those owning the spare equipment will increase their operational risk by releasing spares.

⁵³ Ref. NERC Spare Equipment Database <http://www.nerc.com/filez/sedtf.html>

- Maintain a list of suppliers and service level agreements for highly specialized installation or transportation equipment such as cranes for heavy equipment and Schnabel rail cars for large high voltage transformers.
- As opportunities arise to replace transformers that are aging or have insufficient capacity, convert substations operating at non-standard voltages to more common voltages.

11.2 Standard Equipment

While standard equipment such as structures, hardware, insulators, distribution components, etc. may be more readily available; replacement inventory will still be constrained. Consider the following:

- Compile a list of regional and national suppliers with around-the-clock contact information, and ensure the list is readily accessible during a Severe Event.
- Review existing spare equipment and material inventories under a Severe Event scenario and identify opportunities to improve these inventories.
- Create a salvage control center which could amass materials to be re-dispersed to key restoration areas. Cannibalize spare parts from damaged equipment or from less critical plants and substations.
- Siphon fuel from inoperable equipment.
- Re-allocate tools such as compressors, chargers, lifts from in-operable equipment.
- Re-allocate redundant equipment to facilities that need them.
- Use temporary design standards that use less material (e.g., wood and steel beams in lieu of concrete foundations, increase span distances between towers without sacrificing public safety).
- Remove obstacles from beneath transmission lines to increase clearance. Increase clear-cut corridors to manage vegetation growth with fewer resources.

Wal-Mart and Home Depot Hurricane Response

Wal-Mart and Home Depot, valuable sources of many different consumables that may be required, have emergency response plans that have proven very effective during hurricane response.

11.3 Fuel for Transportation and Backup Generators

Entities have contracts in place with suppliers to provide fuel for vehicles and generators. However, during a Severe Event the fuel suppliers may also be impacted and normally used delivery systems or routes may be unavailable. Entities should enhance their arrangements with suppliers in advance of a Severe Event to consider alternative delivery systems. Regardless, entities need to consider how they would prioritize their allocation of limited fuel supplies.

Table 6: Sample Fuel Priorities for Critical Equipment	
Critical Load	Rationale for Priority
Backup generators at nuclear stations	In the event of a loss of BPS power supply, enhance recovery, prevent extended unavailability, or maintain safe shutdown.
Backup generators at non-nuclear generating stations	In the event of a loss of BPS power supply, enhance recovery and prevent extended unavailability.
Backup generators at transmission substations	Supply station service auxiliaries (e.g., compressed air for breaker operation, protection systems, station monitoring devices and systems).
Backup generators power plant and system control centers	Supply critical operations at Reliability Coordinators, Transmission Operators, Generator Operators.
Backup generators at telecommunications centers	Supply communications facilities and systems needed to operate the BPS.
Vehicles	Transport personnel and resources needed for BPS restoration and supply to critical loads and priority loads.

Key Recommendation #28 | Logistics and Self-Sustained Operations

Consider with fuel suppliers ways to prioritize the supply and delivery of fuel for emergency standby generators and essential work vehicles.

11.4 Transportation Routes

Evaluate alternative transportation routes. It is likely that the transportation sector (e.g., airlines) would be heavily impacted. This occurred with September 11th and with recent volcano eruptions shutting down air traffic into Europe, South America, Australia, and New Zealand. Natural disasters combined with terrorist activity could easily impact the railroad or highway system to large parts of the continent.

Seasonal issues such as ice storms, blizzards, hurricanes, and flooding can compound the impact of the severe Event on transportation. Consider alternate transportation modes (e.g., rail, air, water, truck) that may not be appropriate during normal circumstances.

Establish contact with and develop relationships with state and local government transportation authorities who can help identify transportation routes and approve any transportation permits that may be required by utilities, transportation service-providers, or mutual assistance partners.

11.5 Personnel and Facility Resources

Whether using entity employees or external resources, a Severe Event will strain the entity's ability to respond to a Severe Event. Planning to effectively utilize human resources during a Severe Event will optimize the utility's ability to respond.

Entity Employees

Business continuity and disaster recovery plans should identify the key personnel needed to restore and maintain critical operations, and recognize the increased intensity associated with filling these roles through the New Normal period. Plans should address scheduling additional personnel to assume these critical roles or provide operational support. Plans should address issues related individuals who are unwilling or unable to report for work. The plans should also consider how to supplement these key roles with personnel who can be shifted from lower priority work and quickly trained to fill critical roles. For every critical role, there should be at least one individual with primary responsibility and a fully trained and experienced backup. Identify, train, and explicitly recognize individuals to fill these roles.

Plans should identify the initial work shift hours and team or crew composition. For example, during the first few days of an event shift durations may be different than later in the event when circumstances may be more predictable. Consider changes that may be required to employee work arrangements (e.g., collective agreements) such as work schedules and alternate roles and responsibilities.

- **Management Personnel** – Management will need to be ready to make important decisions to support personnel operating in unusual situations, including working out of their normal scope of responsibilities or levels of authority.
 - With the necessary refresher or certification training, a manager with experience in the field and technical trades could assist as an equipment operator, control center operator, or foreman.
- **Field Personnel** – Field personnel will play front-line operational roles to identify damage and repair or replace damaged equipment.

- With suitable training, a groundman may perform certain duties as a line hand on a de-energized line.
- Journeymen linemen may provide support in roles such as relay technician assistants or substation assistants.
- Warehouse staff may provide groundman support for line crews.
- **Operating Personnel** — Operating personnel are typically the first to recognize an event has occurred and are instrumental in activating their entity's plans. They will need to maintain situational awareness, make decisions and direct operations clearly and concisely at all times.
 - Back office engineering staff may support system operator functions.
- **Office Personnel** — Office personnel will not likely be directly involved in the front-line of restoration activities, yet the most important aspects of their roles will still need to be carried out and they may be re-deployed to new tasks.
 - Engineering or office staff may fill needed roles in logistical operations such as procurement or warehousing.

Leadership and Succession Planning

During a Severe Event, it is particularly important that personnel know at all times the manager or supervisor who will provide them with direction and operational support. Circumstances will require these leaders to change roles through the New Normal period, and succession planning will be a critical element of an entity's strategic direction and operational success. It is vital that leaders at all levels continue to find, assess, develop, and monitor the personnel resources needed to manage New Normal conditions. As the New Normal period progresses, working conditions may become more stable, and entity leaders may resist losing competent personnel to other roles, and having to train their replacements. Leaders themselves may be reluctant to move into new areas of responsibility. Leaders need to understand that succession planning must continue to match rapidly evolving organizational needs with employee competencies and capabilities. Effective succession planning will form the basis for continued success through the New Normal period. The succession planning process for the organization should:

- Define the skills and competencies needed through the New Normal period.
- Identify leadership and personnel competency gaps.
- Observe and periodically assess how leaders and personnel are coping in their roles.
- Identify personnel who are demonstrating an ability to assume increased responsibilities.
- Foster a growing sense of responsibility for personnel to display leadership characteristics at all levels in the organization.

Clearly Define the New Roles

It is important that personnel understand their new roles and who their manager or supervisor is at all times. Personnel need to know who provides them with technical direction and who they can rely on when they need to seek help or advice. Personnel roles and responsibilities should be clearly defined and documented and include:

- **Reporting structure** — present and new role, new work locations, new manager or supervisor, working hours and shifts
- **Expectations of the new role** — personal equipment provided by the individual (e.g., tools, personal protective equipment), equipment that will be provided at the work location, professional qualifications, certifications, or licenses required.

External Resources (Contractors, Mutual-Aid providers)

Entities often rely on externally contracted resources to fill roles similar to those of entity employees, for example for major projects. Entities need to consider that these contracted resources may not be available during a Severe Event, as other entities will have similar incremental needs to respond to the Severe Event. Prior to a Severe Event, entities should consider establishing contracts with these resources that explicitly address what may or may not be provided through a Severe Event (e.g., force majeure).

Mutual aid arrangements with other entities allow entities to quickly supplement their existing workforce. Recognizing that neighboring entities may be similarly stressed, consider making arrangements with a number of geographically dispersed entities to help ensure that assistance can be obtained from areas outside the affected region. Similarly, consider how you may be able to assist other entities, particularly with personnel other than the work crews historically familiar with working in new work locations (e.g., system operators, system planners, control room support staff). The terms of these arrangements should be reviewed periodically.

Key Recommendation #29 Logistics and Self-Sustained Operations
Consider how your business continuity or disaster recovery plan would change if you are unable to rely on mutual support arrangements.

Alternate Work Locations

During a Severe Event, it is possible that the primary work location may be unavailable and personnel will need to work from backup or other temporary locations. Personnel should be trained on how to deploy to the alternate location and start work safely and efficiently.

Alternate work locations, which may include fields for staging work, empty warehouses, or schools should be identified and tested periodically. Plans should consider:

- Alternate backup facilities if both primary and backup operations centers are unavailable.
- A communications plan to quickly and reliably direct personnel to backup facilities.
- Van pools to safely transport employees and conserve fuel.
- If working from home is viable, ensure personnel have the tools to effectively work prior to any event.

12.0 Preventing and Responding to Physical Attacks

While this report provides generally applicable guidance for entities to prepare, mitigate, and respond regardless of the cause of the Severe Event, this section specifically addresses a coordinated physical attack scenario.

It is impossible to completely prevent a determined physical attack on BPS infrastructure. However, steps can and should be taken to prepare to make such an attack more difficult and/or less effective.

This section discusses the following topics:

- **Challenges** – The challenges of preventing and preparing for physical attacks.
- **Prevention** – Steps that should be considered to protect facilities in a way that will discourage attacks, make attacks more difficult to accomplish, or minimize the damage.
- **Preparation** – Steps that should be considered in advance, to prepare to respond to a physical attack.
- **Response and Recovery** – Steps that should be considered to effectively respond to a physical attack, and how security might change to support operations through the New Normal.

Assumptions

This section assumes the following scenario:

- A simultaneous and coordinated physical attack directly impacts the BPS. Equipment at multiple generating stations and high voltage transmission substations are severely damaged.
- Subsequent attacks days or weeks later will continue to impact BPS equipment and place field personnel at risk. Law enforcement and National Guard support to protect field personnel and equipment is very limited due to the priority to protect the communities they serve.
- Voice and data communications are disrupted due to equipment damage (microwave towers, fiber cuts, etc.). Cell phone systems are jammed due to excess traffic.
- Transportation is disrupted due to widespread power outages.

12.1 Challenges to Protecting the BPS

In order to provide some insight into why some prevention and preparation strategies are suggested and others are not, the following provides context for subsequent sections.

Asset Protection

BPS assets are dispersed widely across the continent, usually in remote areas, making complete protection infeasible. Protection is often limited to fencing and padlocks at facilities that are operated remotely and not staffed.

Mixed Environments

Some BPS assets are in rural, remote locations while others are in urban, densely populated areas. This makes protection difficult and the resulting procedures complex.

Multi-Jurisdictional

Because service territories rarely align within a single municipality, it is typical for entities to need to deal with many different local law enforcement agencies to address security issues. This multi-jurisdictional nature is not limited to the geographic location of the assets, but also involves understanding the various different government agencies and their roles.

Replacement Assets

Many BPS assets are difficult to replace or repair – some require purchasing lead-time of many months. This suggests that greater protection is needed for these assets.

Ease of Asset Identification

Due to the size, accessibility, and visibility of high voltage power lines, identifying equipment that is part of the BPS is relatively easy.

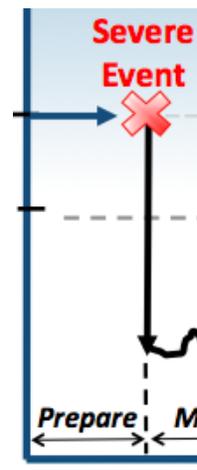
12.2 Recommended Prevention Strategies

While it is impossible to completely prevent a determined physical attack on BPS infrastructure, actions should be considered to implement prevention measures that will deter or limit an attack by making it difficult to locate, enter, and damage a facility.

Obfuscation

A facility that 'blends' into its surroundings is more difficult to identify and decreases the chance it will be targeted. This can be accomplished by:

- **Security by Environmental Design** — Where possible, establish visual barriers such as trees, mounds, and bushes.
- **Security by Architectural Design** — Where possible, use matching building material that blends the asset into the neighboring buildings.
- **Fly Zones** — Do NOT identify locations as 'no fly zones' to the Federal Aviation Administration and Transport Canada. The resulting maps available to all pilots are widely published and will clearly identify the location of the facilities.



Hardened Facilities

Design facilities, particularly those that are critical assets, to increase the effort required to damage the facility or make it difficult to gain access. Install equipment to detect and report a security breach. This can be accomplished using:

- Basic construction techniques, such as:
 - Higher and stronger walls
 - Fewer windows and doors
 - Reinforced gates
- Install monitoring and sensing equipment, such as:
 - Cameras
 - Vibration Detection
 - Motion Detection
- Involve the local community, for example by enhancing Neighborhood Watch programs to raise awareness regarding the local BPS facilities that they rely on.

Key Recommendation #30 | Preventing and Responding to Physical Attacks

Consider actions that can be taken to protect BPS assets by involving local communities and law enforcement (e.g., reinforcing their awareness of BPS facilities that are critical to operations).

Key Recommendation #31 | Preventing and Responding to Physical Attacks

Consider ways to improve security when designing or refurbishing existing BPS facilities.

12.3 Recommended Preparation Strategies

The strategies suggested in this section pertain to preparatory actions that may be taken prior to an attack to manage likely consequences. These actions will help ensure that assets are prioritized, vulnerabilities and risks are understood, law enforcement support is coordinated, and plans and teams have been developed and exercised.

Consequence Assessments

Consider conducting consequence assessments to evaluate and prioritize BPS assets. Consequence assessments should consider the impact on the entity, as well as impacts on society and other critical infrastructures within the entities footprint of operation. Criteria to identify critical assets for NERC Reliability Standard CIP-002-1 are provided in the *NERC Security*

*Guideline – Identifying Critical Assets*⁵⁴. Additional information is available in Section 3 of the DHS National Infrastructure Protection Plan⁵⁵ that provides a generic methodology for consequence assessments.

Physical Vulnerability Assessments

Conduct physical vulnerability assessments to identify threats, vulnerabilities, loss impacts, prioritize risks, and identify cost effective controls. Assume that critical assets will be targeted.

Strategies

Identify strategies for emergency response, operations recovery, and system restoration.

Site Security Plans

Develop, exercise and maintain site security plans that provide for the protection of assets and personnel from physical attacks. Site security plans should be based on the results of consequence assessments as well as risk and vulnerability assessments. The countermeasures documented in the plans should be implemented according to the alert levels declared by the entity.

Emergency Response Plans

Develop, exercise, and maintain incident and emergency response plans that provide for life safety (e.g., evacuation, shelter-in-place, bomb threat) and limit initial property damage.

Business Continuity Plans

Develop, exercise, and maintain business continuity plans that initially recover business operations to minimally acceptable levels for the New Normal period, then later resume operations to normal business operation levels.

Incident Management Plan

Develop, exercise, and maintain an incident management plan that addresses command, control, communications, and coordination with entity operational response, crisis communication (e.g., media, consumers), and government.

Training

Train and exercise teams in the activation and execution of the above plans and other response, recovery, and restoration strategies.

Local Law Enforcement Agency Days

Collaborate with local law enforcement agencies to build relationships. Foster an environment of cooperation and participate in joint exercises. Coordinate planning and preparedness activities with local and state/provincial government.

⁵⁴ NERC Security Guideline – Identifying Critical Assets

http://www.nerc.com/fileUploads/File/Standards/Critical_Asset_Identification_2009Nov19.pdf

⁵⁵ Ref. NIPP, [National Infrastructure Protection Plan](#)

Key Recommendation #32 | Preventing and Responding to Physical Attacks

Consider ways to improve local coordination and cooperation with local/state/provincial law enforcement.

Replacement Equipment

Essential equipment that is difficult to obtain should be identified, acquired, and stored in secure locations. See the *Logistics and Self-sustained Operations* section of this report for additional information.

Adaptability and Continuous Improvement

Periodically perform post-exercise reviews to identify and document preparedness successes, areas for improvement, and lessons-learned. Develop an action plan for improvements, develop enhancements, and implement identified improvements.

Possible Threats

Physical attacks on the BPS may appear in several forms. Threats could come from internal (e.g., disgruntled employee, contractors) or external (e.g., disgruntled customer, terrorist) sources. The table below shows possible threats that should be considered when performing a risk assessment. The threats shown could be part of the initial attack or could be part of subsequent attacks designed to stop, slow, or divert response and recovery efforts.

Controls Overview

Controls (countermeasures, safeguards) may come in many forms. Before an appropriate control can be identified the nature of the threat must be understood as well as the vulnerability of the asset being protected. Threat and vulnerability information is identified and documented in a risk assessment. When assessing controls it is useful to classify them into 'control types'. The table below shows possible controls separated into control types. The examples shown are not limited to a physical attack scenario.

Table 7: Control Types and Examples		
Control Type	Definition	Control Examples
Prepare	Controls that prepare for threat occurrence or expected losses.	Risk assessments, impact assessments, plans (response, recovery, restoration, preparedness), backup data, alternate sites, backup equipment, awareness, training, exercises, drills, control maintenance
Prevent	Controls that prevent threat occurrence or resulting losses.	Prevention procedures, site security plans, fences, access control, passwords, safety measures, fire prevention measures, hide asset, security guards
Detect	Controls that detect threat occurrence or resulting losses.	Smoke detectors, heat detectors, motion sensors, vibration sensors, cameras, security guards
Minimize	Controls that reduce or minimize losses as the threat occurs.	Activate emergency response procedures, water sprinklers, CO2, halon, fire extinguishers, exit signs, stairwells, emergency lighting, first-aid kits, flood wall, deterrence measures, security guards, backup generators
Recover	Controls that recover resources, operations, and reputation lost as a result of threat occurrence.	Activate business recovery and restoration procedures, heal/replace injured personnel, rebuild/replace damaged equipment and facilities, restore data from backups

12.4 Recommendations for Response and Mitigation Strategies

The strategies suggested in this section pertain to actions taken immediately after the physical attack to notify appropriate response teams, assess the nature and magnitude of the attack, and review the status of BPS assets in order to make decisions on the physical security and incident management actions to be implemented.

Site Security Plans

Activate appropriate site security plans according to the alert levels (e.g., Elevated, Imminent per U.S. National Terrorism Advisory System⁵⁶) to protect critical assets and personnel from additional attacks.

Emergency Response Plans

Activate appropriate emergency response plans (evacuation, shelter-in-place, bomb, threat, etc.) that provide for life safety and limit initial property damage.

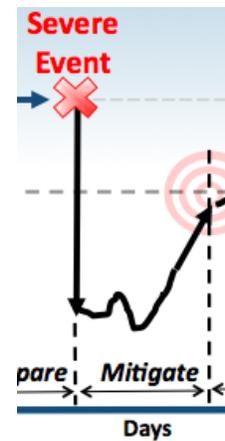
Business Continuity Plans

Activate appropriate business continuity plans that recover time-sensitive, high priority business operations to minimally acceptable levels for the New Normal period.

Incident Management

Activate an incident management system that includes the execution of crisis management plans, the activation of emergency operations centers and incident command posts, as well as the coordination of emergency response and business continuity. Also, activate crisis communication plans, and coordination with government and industry authorities.

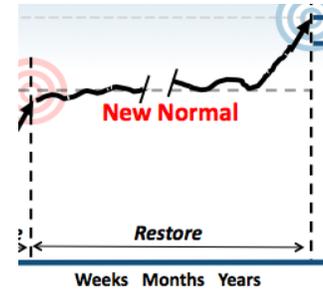
Additional response actions are shown in the Mitigations for Physical Attack section in *Appendix 3* of this report.



⁵⁶ Ref. NTAS <http://www.dhs.gov/files/publications/ntas-public-guide.shtm>

12.5 Recommendations for Restoration Strategies

The strategies suggested in this section pertain to actions that should be taken after response actions are underway to notify appropriate recovery and restoration personnel, implement the incident management system, recover business operations according to prioritized lists of BPS assets, and implement physical security plans and procedures.



Site Security Plans

Continue implementation of site security plans according to the alert levels (e.g., Elevated, Imminent per U.S. National Terrorism Advisory System⁵⁷) to protect critical assets and field personnel from additional attacks.

Business Continuity Plans

Continue implementation of business continuity plans that recover time-sensitive, high priority business operations. Activate plans to recover less time sensitive, lower priority business operations to minimally acceptable levels. Later, resume operations to normal business operation levels.

Incident Management

Operate an incident management system where crisis management teams in emergency operations centers and incident command teams in the field provide command, control and coordination of restoration activities, communication, physical security, and coordination with government and industry authorities.

Adaptability and Continuous Improvement

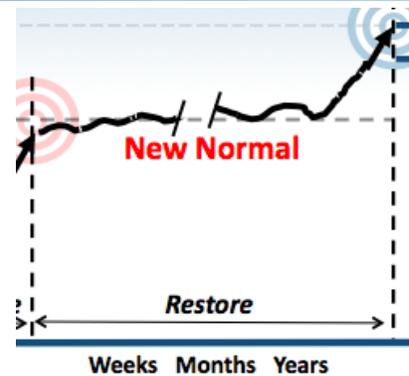
Perform after action reviews to identify and document successes, failures, and lessons-learned. Develop an action plan for improvements; follow the action plan, and implement actions to improve preparation, response, and restoration plans and procedures. Share non-proprietary after action review results with NERC, as appropriate.

Additional restoration actions are shown in the *Mitigations for Physical Attack* section in *Appendix 3* of this report.

⁵⁷ Ref. NTAS <http://www.dhs.gov/files/publications/ntas-public-guide.shtm>

13.0 Financing Emergency Operations

During a routine emergency and recovery (e.g., storm damage), entities normally have sufficient cash and related financial mechanisms in the form of reserves, lines of credit or other financial instruments to deal with immediate needs. Consumer rates approved through the tariff approval process and various forms of industrial insurance are used to finance restoration work and the return to normal operations is possible through rate recovery. A more serious event⁵⁸ can be financially devastating.



A Severe Event will certainly have financial impacts that exceed anything that North America has experienced. The recent nuclear tragedy in Japan hints at the seriousness of the potential problem. This is a look into crippling financial problems as severe as the event itself.

The requirement for cash immediately after the event and for months during recovery through the New Normal period will be significant. Conservative estimates may place this cash requirement at ten times that of normal operations. Given this cash flow requirement, the duration of liquidity is short lived. An entity's ability to acquire and properly allocate funds will largely influence the degree to which recovery is successful, or even possible. Effective cost-tracking and audit processes will still need to be in place to demonstrate that restoration actions are financially prudent under the circumstances.

Each entity will react somewhat differently to the financial reality of a Severe Event. For example, a private investor owned utility will see their stock drop to nothing and credit rating go to junk just before their cash flow slows to zero. Lines of credit will dry up within weeks. State and federal intervention will be inevitable.

The goal of this section is to provide guidance and information to all entities faced with these financial challenges under the following assumptions.

- The Severe Event is regional and affects several BPS entities.
- Existing Banking and Insurance Intuitions are still functioning, but are outside the area affected by the Severe Event.
- The entity's executive and financial functions are able to operate.

⁵⁸ Ref. Edison Electric Institute, *After the Disaster: Utility Restoration Cost Recovery*
http://www.eei.org/ourissues/electricitydistribution/Documents/Utility_Restoration_Cost_Recovery.pdf

13.1 Getting Prepared for Emergency Financing

Some would argue there is little that can be done in advance to prepare for emergency financing that would be required through a Severe Event. Increasing consumer electricity rates through the normal tariff and regulatory approval process would be extremely difficult if not impossible. The carrying cost for large lines of credit is similarly difficult to secure and would soon become unsustainable. It is expected that the need to manage costs will place increased pressures on everything from staffing levels to warehouse inventories and reduce bench strength of needed equipment and resources.

However, much can be done to prepare to manage the financial pressures that would arise soon after a Severe Event. Entities should consider bringing together those responsible for financial matters to discuss the issue. The insurance, procurement, risk management, and financial functions share a significant part of the responsibility and may already have much of the information needed to prepare a plan. Discussions with suppliers, financial institutions, and labor unions will increase awareness of the challenges that would be faced in a Severe Event, and help identify options to address them.

Key Recommendation #33 | Emergency Financing

Consider how extreme financial challenges will be addressed in consultation with financial institutions, suppliers, and government agencies.

The following links provide references that may aid these discussions.

Public Safety Canada: <http://www.publicsafety.gc.ca/prg/em/index-eng.aspx>

- Resources for Emergency Management Planning.
 - Emergency Management Planning Guide to support the Federal Policy for Emergency Management and the Emergency Management Act (2007).
 - All-Hazards Risk Assessment.
- Emergency Preparedness.
 - Canadian Emergency Management College.
 - Guides for business and first responders.
 - Joint Emergency Preparedness Program.
- Joint Emergency Preparedness Program (JEPP).
<http://www.publicsafety.gc.ca/prg/em/jepp/index-eng.aspx>

Canadian Centre for Emergency Preparedness: <http://www.ccep.ca/>

U.S. Federal Emergency Management Agency (FEMA):
<http://www.fema.gov/privatesector/preparedness/>

- References, news and information

- Robert T. Stafford Relief and Emergency Assistance Act
http://www.fema.gov/pdf/about/stafford_act.pdf

U.S. Department of Energy: http://www.oe.energy.gov/our_organization/iser.htm and
<http://energy.gov/oe/office-electricity-delivery-and-energy-reliability>

University of Florida: <http://disaster.ifas.ufl.edu/PDFS/CHAP03/D03-07.PDF>

- Outlines the role of U.S. government agencies in a disaster
 - Describes the difference between a Declaration of an Emergency and a Declaration of a Major Disaster.
 - Outlines the types of assistance that a state governor may request.
 - Describes the role of FEMA if engaged.

New York University, International Center for Enterprise Preparedness:
<http://www.nyu.edu/intercep/businesscase/index.html>

- Provides links to research papers on the financial impacts of emergency preparedness:
 - Corporate balance sheet, impact on assets and liabilities.
 - Profit and loss, impact on revenue and expenses.

U.S. Emergency Management Assistance Compact: <http://www.emacweb.org/>

- State-to-state mutual aid system

Public Entity Risk Institute:

https://www.riskinstitute.org/peri/index.php?option=com_bookmarks&task=detail&id=588

Appendix 1: Task Force Scope

Purpose

This document defines the scope, objectives, organization, deliverables, and overall approach for the SIRTF.

The purpose of the SIRTF is to provide guidance and options to enhance the resilience of the bulk power system to withstand and recover from severe-impact scenarios, specifically:

- Coordinated physical attack.
- Coordinated cyber attack.
- Geomagnetic disturbance.

Background

The NERC and DOE *High Impact, Low Frequency Risk to the North American Bulk Power System* report described a number of severe-impact scenarios and their potential impact on the reliability of the bulk power system. Subsequent to this report, the Electricity Sub-sector Coordinating Council's (ESCC) *Critical Infrastructure Strategic Roadmap* identified a number of strategic initiatives to mitigate these impacts. Several of these initiatives (i.e. items E, F, H, L, and P) identify the need to assess the current capability of the bulk power system to withstand these severe-impact scenarios and to enhance restoration plans and procedures.

NERC staff and the leadership of the NERC technical committees (Planning, Operating, and Critical Infrastructure Protection Committees) have developed a Coordinated Action Plan to address the initiatives identified in the Strategic Roadmap. This scope document elaborates on the Coordinated Action Plan to establish and provide direction to the SIRTF.

Scope

The SIRTF will provide guidance and options to enhance the resilience of the bulk power system to withstand and recover from three severe-impact events as described in the Coordinated Action Plan.

- Coordinated physical attack.
- Coordinated cyber attack.
- Geomagnetic disturbance.

The SIRTF will propose approaches, practices, and plans to reduce the impact of these events through effective emergency operations and timely restoration of the BPS.

The SIRTF will consider what aspects of emergency operation and restoration will be particularly challenged through these severe-impact events, and consider options to enhance the resilience of the BPS. Preferred solutions will be flexible and based on heuristic methods applicable under a wide variety of circumstances, as opposed to fixed procedures. The SIRTF

will recommend solutions for broad implementation across the electricity sector, and propose drills or exercises to reinforce this capability. These solutions could be in the form of industry guidelines that describe practices that may be used by individual entities according to local circumstances.

The SIRTf may consider establishing sub-teams to address the planning /operational and tools/systems issues that may be unique for each of the three severe-impact scenarios.

Assumptions and Limitations

The three scenarios described in the Coordinated Action Plan are intended to describe extreme conditions that would make operation and restoration much more challenging than would normally be considered by electricity entities through their usual planning and preparedness activities. While solutions that offer material improvements are preferred, it is recognized that more modest enhancements that are readily implemented are also valued.

It is expected that any solutions proposed to enhance existing capabilities would be broadly applicable to other severe-impact scenarios, and certainly applicable to smaller scale events.

Goals and Objectives

Goals	Objectives
Review current situation and capabilities	<ol style="list-style-type: none"> 1. Recognizing that priorities will vary depending on local circumstances, consider priorities to restore critical power system loads along restoration paths (e.g. communications, nuclear units), and priority customer loads (e.g. oil refineries, military bases, hospitals, water treatment plants, public telecommunications). Consider how these priorities might differ through a range of outage durations (e.g. days, weeks, and longer). 2. Consider operating capabilities and voice and data communications tools and energy management systems, with a focus on identifying minimum essential functional needs for reliable operation. 3. Consider restoration plan elements such as black start, islanded operation, synchronization, rotational load shedding. 4. Assess operational staffing levels and unique safety considerations under these scenarios.
Perform needs assessment	<ol style="list-style-type: none"> 5. Identify elements of current operating and restoration capability that would be particularly challenged under these severe-impact scenarios.
Develop alternative solutions	<ol style="list-style-type: none"> 6. Propose a range of alternative solutions and options to enhance current operating and restoration capability, including estimated costs and effort to develop and

	maintain this capability. Identify the residual risks that may be associated with each of these solutions.
Coordinate Solutions	7. Coordinate with NERC staff to integrate these solutions with the NERC Crisis Response Plan with special emphasis on areas where local, state, and Federal resources may be required to support such efforts.
Recommend solutions	8. Recommend specific practices or programs for use by NERC or individual entities. Create scalable drill templates that registered entities could utilize to train personnel and enhance current restoration and operating protocols through existing drill and exercise programs.

Task Force Reporting Structure and Coordination with Other Related Initiatives

The Task Force will:

- Report to the Operating Committee. Seek Planning Committee endorsement prior to Operating Committee approvals.
- Provide periodic status reports to the Operating Committee and Electricity Sub-Sector Coordinating Council.
- Coordinate closely with the Critical Infrastructure Protection Committee that will provide expertise to address Coordinated Action Plan Item F – Protect Critical Equipment.
- Coordinate closely with the Spare Equipment Database Task Force.
- Coordinate with other NERC and industry resources that may be able to contribute, such as the, Reliability Coordinator Working Group, North American Transmission Forum.
- Leverage from other recent initiatives in this area (e.g. the National Infrastructure Advisory Council’s Stress Test exercise).

Resources Required

The Task Force requires expertise in the following areas:

- Experience with the real time operation of the bulk power system, including the communications and energy management systems and tools typically used by reliability coordinators, transmission operators, and generator operators.
- In-depth experience with bulk power system restoration plans and procedures, including designing and conducting restoration drills and exercises.
- Familiarity with developing situation assessment reports used to inform senior management or government.

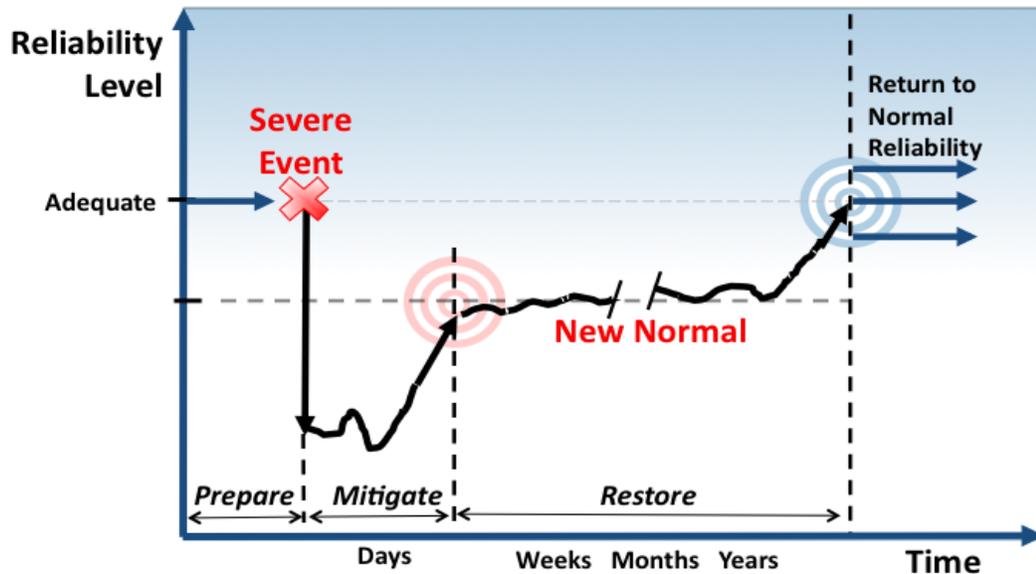
It is anticipated that two conference calls per month, and a total of four face-to-face meetings will be required, in addition to the time required to contribute to this effort. This work is expected to begin in December 2010 and end by December 2011.

References

Name	Link
DOE/NERC HILF “ <i>High Impact, Low Frequency Risk to the North American Bulk Power System</i> ” report	http://www.nerc.com/files/HILF.pdf
<i>Critical Infrastructure Strategic Roadmap</i>	http://www.nerc.com/docs/escc/ESCC_Critical Infrastructure Strategic Roadmap.pdf
NERC Technical Committees’ Report – <i>Critical Infrastructure Strategic Initiatives Coordinated Action Plan</i>	http://www.nerc.com/docs/ciscap/Critical Infrastructure Strategic Initiatives Coordinated Action Plan BOT Apprd 11-2010.pdf

Appendix 2: Mitigations for Monitoring the BPS

This Appendix builds on the recommendations in the *Monitoring the BPS* section of this report and highlights the different actions that may be taken, prior to, during, and after a severe event.



MONITORING Resilience Considerations	Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
	Robustness The ability to absorb shocks and keep operating	Resourcefulness The ability to manage a disruption as it unfolds	Rapid Recovery The ability to get back to Normal as quickly as possible
Generator Output			
1.	Fixed Schedules	Develop and Modify as required MW and MVAR output schedules of available units	As the situation becomes more stable the variability and flexibility of the schedules will be broader.
2.	Block Loading	Using a block loading schedule reduce the need for communications	

MONITORING Resilience		Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
3.	Operating Ranges	Review with GOP’s particular operating ranges that if a directive is outside of the GOP needs to confirm the directive with its own call	Within the response and New Normal adjust and communicate new ranges as required by the new system.	
LIMITS				
4.	Hard Copies of Limits	On a periodic basis print out BPS limits and maintain copies in primary and back-up control centers	During a cyber event routinely sample displayed limits with printed limits	
5.	Referencing Guides	Consider developing distribution factor spreadsheets that act as quick references to better understand the effects of possible actions and contingencies	After an event and particularly in islanded operations and when PSSE tools are not available these tables may need to be recalculated.	
6.	Standing Orders and Temperature Sets	Consider a standing order which states following an event to ease communications particular triggers will be used to go from one temperature set to another.	Based on communications capabilities may want to go to a seasonal set of ratings – making it easier to ensure all parties are always using the same set of ratings	
7.	Conservative Limits	Define a conservative set of limits which could be implemented after a large event (could be as simple as a percent back-off)		As the system becomes more stable and operators will need to continually reassess if these limits are too conservative for the community’s needs.

MONITORING Resilience		Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
8.	Revisit Design Assumptions		A continual re-assessment and implementation cycle of adjusting operating limits to the realities of the current topology and not the original design assumptions. As islands are interconnected these differing operating assumptions will need to be communicated to the joining entities.	
9.	Operate to the Most Conservative Limit	Have discussions with operators and engineers when operating to the most conservative reading may not be in the best interest of reliability.	Continually work with other critical infrastructures to determine whether operating to a less conservative rating is in the greater good of keeping multiple critical infrastructures available.	
MONITORED FLOWS ON BPS FACILITIES				
10.	Prepare for Large Amounts of Data Loss	<ol style="list-style-type: none"> 1. Conduct studies of the minimum amount of data needed. 2. Assess how greater aggregation might reduce some of the reliance on this data. 3. Develop practices for operating without any SE/SA capability for months. 4. Develop a list of the most critical data points. 	Based upon the list of most critical data points prioritize which stations will be staffed with the communications available at that time.	Train additional personnel to assist in the 24/7 needs to report data.
11.	Loss of Primary & Back-Up EMS	Understand which portions of your system are independently monitored by neighbors.	Consider how off-line study packages and applications (operator training simulator) could be leveraged.	

MONITORING Resilience		Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
12.	Phasors	Continue to develop the operational capabilities of the PMUs. As these capabilities and systems are developed, consider keeping their data feeds and platforms independent of EMS capabilities.	<ol style="list-style-type: none"> 1. Redefine the operating parameters of the PMU applications as procedures/decision points may be based upon pre-crisis topology. 2. Continue to evolve operating procedures around operating experience. 	
Loss of Both Control Centers				
13.	Back Up Location Considerations	Consider both sites are sufficiently distant so as not to be affected by single events which would render a control center unusable.	Backup sites should have considered the issues of personnel feeding, hygiene, security, backup power, and transportation needs.	Recovery from an event would be facilitated if a common event would not render both primary and backup control centers unusable.
14.	Agreements with Others	Consider if other entities might be able to share control centers and telemetry.	Contracts should be in place for security, fuel delivery, sewage, and food supplies. Following an event prioritize contacting these suppliers and arrange deliveries.	Contract revisions will be necessary during the period of reconstruction. In some cases assistance from neighboring utilities may be necessary.
15.	Diversely routed telemetry	Design and plan telecommunications paths such that both sites are not exposed to single points of failure.	Multiple telemetry routes should be available from all sources, especially the RC, as operation from the alternate could extend for a significant time.	Diversely routed telemetry would more readily enable operation for an extended duration after the event is over while the previously disabled or destroyed control centers are rebuilt.

MONITORING Resilience		Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
16.	Use of EOC or OTS as possible tertiary sites	Anticipate possible use of emergency operations centers (EOC) or operator training simulators (OTS) as backup control centers and design them with the appropriate telemetry.	Dispatcher familiarity with the EOC and OTS from drills & exercises should facilitate and help recognize the need for various facilities for long term operation.	An EOC or OTS are more likely to have the necessary facilities to operate for an extended duration during the New Normal.

		Preparedness: Prior to Event	Mitigation: During an Event	Recovery: After an Event
		Robustness The ability to absorb shocks and keep operating	Resourcefulness The ability to manage a disruption as it unfolds	Rapid Recovery The ability to get back to Normal as quickly as possible
Communicate				
1.	ES-ISAC	Develop and maintain procedures to report suspicious activity to ES-ISAC.	Report incidents to the ES-ISAC and monitor ES-ISAC alerts or advisories.	Continue updating ES-ISAC as appropriate.
2.	Local, State Authorities	Develop, maintain, and exercise communication plans with local, state authorities.	Communicate with local, state authorities during response.	Continue communicating with local, state authorities during recovery.
3.	NERC	Share prevention and preparedness phase lessons-learned.	Share mitigation phase lessons-learned.	Share recovery phase lessons-learned.
4.	Alternative Communications	Develop, maintain alternative communication methods.	Execute alternative communication methods, as required.	Continue execution of alternative communication methods, as required.
5.	Crisis Communication Plan	Develop, maintain, and exercise Crisis Communication Plan.	Activate Crisis Communication Plan.	Continue execution of Crisis Communication Plan.
6.	Public Reporting	Develop, maintain, and exercise communication with the media to share information with the public in order to increase observations in the field (the public reporting strange happenings/sightings).	Use communication with the media to share information with the public in order to increase observations in the field (the public reporting unusual events).	Continue using communication with the media to share information with the public in order to increase observations in the field (the public reporting unusual events).
7.	Reliability Coordinator (RC)	Utilities develop, maintain, and exercise communication plans with relevant RC.	Execute communication plans with relevant RC. Rapidly share lessons-learned with other entities.	Continue execution of communication plans with relevant RC, as required.
Monitoring & Situational Awareness				

8.	Vulnerability Assessments	Perform risk/vulnerability assessments and review at least annually.	Implement lessons-learned from other entities into security or operations plans.	Review vulnerability assessments for ability to estimate the actual threat, vulnerabilities, and impacts experienced.
9.	Controls	Install, maintain, test, and monitor controls. For example: <ul style="list-style-type: none"> • fences, gates, walls, berms • access control systems/methods • make assets less visible • security guards and patrols • smoke/heat detectors, motion sensors, cameras, etc. 	Increase and adapt monitoring of implemented controls. Consider random changes to security plans to reduce predictable actions.	Continue increased monitoring of implemented controls.
10.	Law Enforcement/Military	Develop and maintain coordination.	Increase coordination and adapt to current situation.	Continue increased coordination.
11.	SCADA Monitoring	Review expansion of use of SCADA to monitor and report inappropriate activity.	Use SCADA to monitor and report inappropriate activity. Work with IT to monitor SCADA for possible disruption.	Continue use of SCADA to monitor and report inappropriate activity.
12.	Situational Awareness by the Public	Develop and implement programs to support situational awareness of facilities by the public.	Remind public of situational awareness and where to submit reports, provide for disruptions in routine communications.	Continue reminding public of situational awareness and where to submit reports. Share intelligence and lessons-learned with communities.
13.	Monitoring Plans	Train, exercise, maintain plans and teams to perform monitoring.	Activate appropriate monitoring plans and teams.	Continue execution of appropriate monitoring plans and teams.

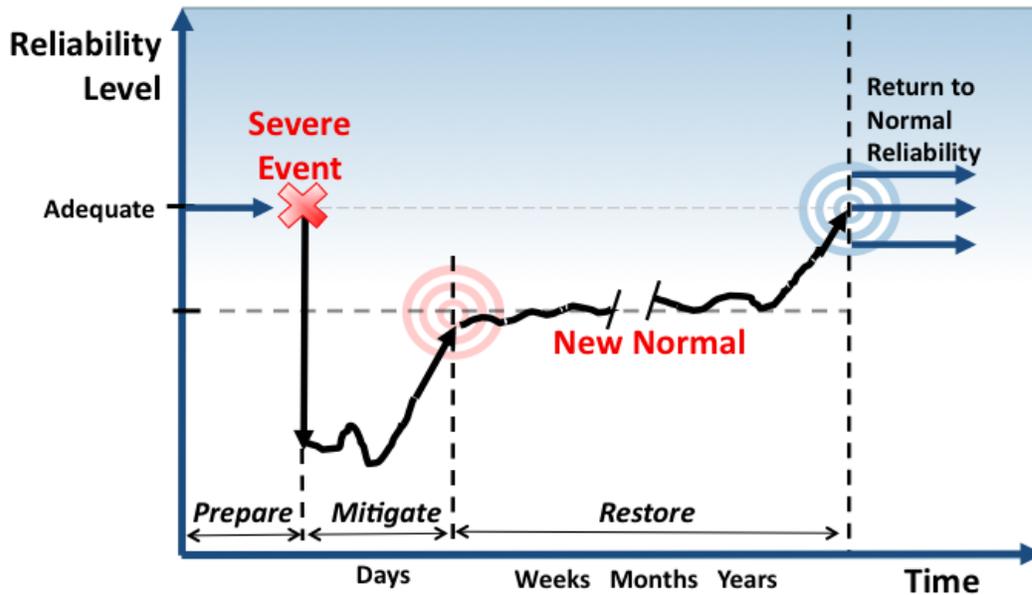
14.	Intelligence	Implement thorough intelligence gathering and reporting. (e.g., through ES-ISAC, RCs)	Increase intelligence gathering and reporting.	Continue increased intelligence gathering and reporting.
15.	Security Threat Levels	Develop, maintain, and exercise a system of Security Threat Levels which is compatible with the National Terrorism Advisory System . Have procedures to be prepared to move to a different level based on perceived threats; and report the current level to authorities as appropriate.	When credible, <u>specific, and impending</u> terrorist threats to electric infrastructure becomes evident, change the Security Threat Level to IMMEDIATE and activate appropriate response and crisis management plans. When a credible terrorist threat becomes evident, change the Security Threat Level to ELEVATED, and monitor threats as appropriate. Report the current level to authorities as appropriate.	Continue monitoring threats and the current situation. Change the Security Threat Level, as appropriate. Report the current level to authorities as appropriate.
Command & Control, Operate				
16.	Incident Response Plans	Develop, maintain, and exercise Incident Response Plans.	Activate appropriate Incident Response Plans to protect facilities and personnel.	Continue execution of appropriate Incident Response Plans to protect facilities and personnel.
17.	Crisis Management Plan	Develop, maintain, and exercise crisis management plans and crisis communication plans.	Activate crisis management plans and crisis communication plans.	Continue execution of crisis management plans and crisis communication plans.

18.	Crisis, Operations, Incident Teams	Train, maintain, and exercise crisis management, crisis communication, emergency operations, and incident response teams. Align and train teams in the National Incident Management System (NIMS) and the Incident Command System (ICS) .	Activate appropriate crisis management, crisis communication, emergency operations, and incident response teams.	Continue activation of appropriate crisis management, crisis communication, emergency operations, and incident response teams.
19.	Protect Critical Infrastructure	Develop, maintain, and exercise response plans with law enforcement to have them protect critical infrastructure when initiated by the operator owner.	Activate appropriate response plans to have law enforcement protect critical infrastructure. Inform law enforcement as priorities regarding critical assets change.	Continue execution of response plans to have law enforcement protect critical infrastructure.
20.	Protect Field Personnel	Develop, maintain, and exercise plans for the protection of field personnel after an attack. Protection strategies could include: <ul style="list-style-type: none"> • Protection provided by local and state law enforcement and the National Guard • Protection provided by a contractor with armed personnel • Protection provided by field personnel themselves (armed?) 	Activate appropriate plans for protection of field personnel after an attack.	Continue to implement and update plans for protection of field personnel during recovery and restoration.

21.	Mobile Control Center	Develop, maintain, and exercise a mobile control center for use by security and crisis/incident management teams. Could be used as a security control center, emergency operations center, and/or incident command post.	Deploy and protect mobile control center where needed.	Continue deployment and protection of mobile control center where needed.
-----	------------------------------	--	--	---

Appendix 3: Mitigations for Physical Attacks

This Appendix builds on the recommendations in the *Preventing and Responding to Physical Attacks* section of this report and highlights the different actions that may be taken, prior to, during, and after a Severe Event.



Appendix 4: Resilience Discussion Worksheet

Introduction

The SIRTF report provides a framework to help entity management and subject matter experts review their plans and preparations and consider a Severe Event that is much greater in terms of impact and duration than current plans envision.

This Appendix provides a worksheet that could be used by business continuity and emergency preparedness personnel, system operators, and management to prompt creative thinking about the possible challenges they might face through a Severe Event. The worksheet builds upon the ideas and recommendations found within the SIRTF report and poses questions that may prompt new resilience ideas, mitigation responses, and other courses of action. The worksheet is not intended to require that a new and detailed response plan be developed for a severe event; instead, personnel are encouraged to challenge themselves to consider substantially worse scenarios to help ensure they and their organization will be in a better position to respond.

As such, the SIRTF recommends that entities use this worksheet to facilitate discussions involving personnel at all levels, including executive leadership, to enhance the entity's overall crisis preparedness and response capability. This worksheet is not exhaustive, and entities are encouraged to build further on the concepts and ideas offered.

Decision Making

1. If many members of the organization's senior leadership team were unavailable because of travel restrictions, communications failures, or other post event challenges how would decision making authority be established?

Possible Challenges Requiring Decisions	If this decision should fall to a few people – who?	If this decision should be made up of a team, who should comprise this team?
Priority Load Designation		
Changes to Operating Limits		
Procurement Decisions		
External Communications (Messaging)		
Reassignment of Personnel		

2. What might be the triggers for re-evaluating certain decisions or the assumptions or both underlying these types of decisions?

Decisions which may require periodic reevaluation:	What are the Triggers for reevaluation? (i.e., Time Based, Changes in Operating State, External Requirements)
Priority Load Designation	
Changes to Operating Limits	
Procurement Decisions	
External Communications (Messaging)	
Reassignment of Personnel	

Business Continuity and Restoration Plans

3. How would your current **Business Continuity plans** be disrupted if your organization had little to no communications? Which of these disruptions most troubles the following personnel?

	What is most troublesome?	What makes this concern so critical?	What are possible mitigations?
System Operator			
Field Personnel			
Procurement Team			
Executive Leadership			

4. How would your current **Restoration plans** be disrupted if your organization had little to no communications? Which of these disruptions most troubles the following personnel?

	What is most troublesome?	What makes this concern so critical?	What are possible mitigations?
System Operator			
Field Personnel			
Procurement Team			
Executive Leadership			

5. Another way of examining the critical communications interdependence is to list each of your communication capabilities and prioritize the importance of these capabilities to your business continuity or restoration plans or both. Walk through how your organization would adapt its plans if you were to lose these capabilities, from the most critical to the least.

Communications Capability	Possible Mitigations
Phone Lines	
EMS/GMS Signals	
Cell Phones	
Satellite Phones	
Internet	
Radio	
Hand-Carried Messages	
Other	

6. What resource limitations create time constraints for portions of your business continuity or restoration plans or both?

Possible Examples of Time Restraints	Possible Mitigations
Nuclear Power BPS-supplied Power (six hours)	
Nuclear Power Back-up Diesels (7 days)	
Control Room Back-Up power (3 days?)	
Data Aggregation Points	
Communications Repeating Stations	
Sub-station Breakers	
Other	

7. For energy-related limitations how could the investment of renewable generation (e.g., wind, solar) extend these time restrictions? What would be other financial justifications beyond greater system resilience for making such an investment?

Operations

1. If only limited data points are available, how would studies be performed?
2. If the BA and TO no longer have visibility of their systems:
 - a. Who would become the new system operator and how would this be established?
 - b. How would the extent (boundaries) of any resulting islands be determined?
 - c. How would you implement the system restoration plan?
 - d. What independent actions would equipment operators take? How are these actions known, coordinated and trained?
 - e. What system information (e.g., generator characteristics, load characteristics, limits) would be shared with the new system operator and how?
 - f. What communication methods and protocols would be used to keep the Reliability Coordinators, Balancing Authorities and Transmission Operators updated on local system conditions and restoration progress?
 - g. How will variable generation resources be managed during restoration and New Normal timeframes?

3. How would the following system parameters be managed immediately following the Severe Event and during the New Normal?

Challenge	Possible Mitigations to deremine MW, MVAR output and resulting frequency
BA has No Communications with Market/Generation Operation (MOC/GOP) Centers	
BA has no communications with units but can communicate with MOC/GOP	

4. How would your organization consider its operating assumptions and limits? At what point is it appropriate to revisit, and possibly revise, protection settings on relay settings, UFLS and other protection schemes?
5. What rules of thumb should be provided to system operators for operating in the New Normal?
6. Assuming a total blackout with no outside assistance and no expectation to interconnect in the near term:
 - a. What units are most essential to the restoration plans?
 - b. How many days of fuel do these essential units typically have on hand? Are there contracts in fuel on hand. How does such a number of MWh define the load to be served, the rotating blackout schedule, and the amount of reserves carried?
 - c. What concerns do you have about units that do not have station power and lighting needs served?
 - How many days before a unit might be damaged? What ways could resources be committed to protect such units?
 - What if the severe event prevents BPS supply to the nuclear units and is expected to last beyond the technical specification requirement to have seven days fuel on hand for the back-up diesels?
7. How will new load patterns be established?
8. Will Operating reserve requirements be met by load shedding or by reserving generation capacity? Why? What are factors that may change this assessment?

9. In the event that there are no market mechanisms and tools available to dispatch generation, what alternative mechanisms can be used?
 - a. place (i.e. black start agreements) governing minimum fuel supply?
 - b. What are the critical and priority loads that need to be served? Do these change based on different event outcomes and timeframes? If so why?
 - c. What loads are not essential and do not need to be supplied over the long term?
 - d. Assuming no fuel resupply and half of the load in your typical operating zone calculate how many MWh of energy is available today with a typical amount of

Logistics and Interdependencies

10. What infrastructures are your critical facilities most dependent on?

Critical Infrastructure	What is most troublesome?	What makes this concern so critical?	What are possible mitigations?
Communications			
Energy			
Water & Dams			
Information Technology			
Other			

11. Of these infrastructures, which have critical facilities (those facilities essential to bulk power system operation) within your zone (and maybe in your neighbors' zones)?

Facility & Contact Info	Critical Infrastructure	Location	Impacts & Time to Impact
1.			
2.			
3.			
4.			
5.			

12. What are the energy needs of these critical facilities?
13. How would a total blackout restoration plan address these facilities' energy needs?

14. What hard-stop time limits can these facilities endure without power before there is damage or second or third order impacts to other infrastructures and/or the bulk power system. How are these time limits factored into your own plans?

People

1. For each of the major functions within your organization related to the reliability of the bulk power system, which are most critical?

Critical Organizational Function	Point or Primary Person/Department	Secondary Person/Department	Tertiary Person/Department
1. Operations			
2. Communications - Hardware			
3. Communications - Messaging			
4. Emergency Liaison			
5.			

2. Based on the assessment of critical functions, how would personnel within these functions be directed?
 - a. When should they report to work following a Severe Event?
 - b. Do they all report at once, and then a schedule is created, or is there a standing set of instructions?
 - c. How would transportation challenges be addressed under the following scenarios?
 - State/provincial or local travel restrictions
 - Gas pumps are not working, and personnel’s private vehicles have insufficient fuel to get to work.
 - Consumers wanting to know when their power will be restored routinely interrupt and delay utility personnel engaged in restoration efforts.
 - d. How would you address personnel concerns about their families?
 - In the first couple of days following a Severe Event
 - Ten days after a Severe Event
 - One – six months after a Severe Event
 - e. How would you house, feed, and care for these personnel?

Financing

1. How can each corporate function best prepare and respond to a severe event?

Critical Organizational Function	What can you do to prepare for a severe Event? What resources are available?	How will you function during the new normal?	How will your area facilitate the return to normal BPS reliability levels?
1. Insurance			
2. Procurement			
3. Risk Management			
4. Finance			
5. Collections			
6. Labor Relations			
7.			

Appendix 5: Severe Event Response Checklist

This Appendix provides a checklist of questions that may be used by entities through a Severe Event to periodically assess the situation and decide new courses of action as system conditions and circumstances evolve through the New Normal period.

Date: _____

Time: _____

System Topology

What are the current island boundaries?

1. Are these being operated in an unstudied state?
2. Depending on the electrical configuration of the island(s), which operating security limits may no longer be appropriate?
 - a. Why are these limits inappropriate?
 - b. Conversely, why are other limits still appropriate?
 - c. Of those limits which require additional study
 - Which limits should be prioritized?
 - What decision criteria are used to determine this priority?
3. Is the system configuration suitable for restoration?
 - a. How do we know this?
 - b. Have breakers been opened along the restoration path?
 - c. Have entities initiated their independent actions?
 - d. Who is working on this confirmation?
4. Will the current protection schemes/SPS/UFLS/UFLS settings impede or assist with the current system's operations?
 - a. What protection changes are practical at this time?
 - b. How are the decision criteria for "practical" defined?
 - If changes are merited, with the limits in the current workforce, communications, and other resources how will the priority of these changes be determined?
 - How will these changes be coordinated as connections are made with other islands?

Generation

1. What generation is damaged and what is fully capable and available?
 - a. What is keeping the unavailable units in this state?
 - b. Are the fixes that are required under the organization's control, or what assistance is needed?
2. Which units in the island are blackstart capable and available?
3. What is the fuel availability for each unit within the island?
4. Do any of these units have regulatory restrictions that are limiting their capacity?
 - a. How can these restrictions be addressed?
 - b. Who is the decision maker?

Transmission Lines and Substations

1. What is the status of key substations?
 - a. How critical is the key substation in the current system configuration?
 - b. What is the status of key elements within the substation (transformers, busses, breakers, reactive elements)?
 - c. Can the substation be reconfigured to utilize good equipment and bypass bad equipment
2. What equipment can be cannibalized to restore key substations?
 - a. Can redundancy (per standard requirements) be minimized/eliminated to provide a larger restoration footprint such as moving redundant transformers to key substations or creating radial configurations on breaker and a half configurations to free up additional breakers for key substations)?
 - b. In what timeframe can the cannibalization occur?
 - c. What is the availability of specialized equipment (railcars, cranes etc.)?
3. What is the status of key transmission lines?
 - a. Breaker status, operable, etc.
 - b. If line is out of service, has a line inspection been completed and any potential faults resolved?
 - c. Can lines be re-configured to by-pass damaged substations?

Key Equipment

1. What is the status of key equipment?
 - a. Damaged equipment (repairable or not)
 - b. Replacement equipment
 - c. Cannibalization

Load

1. What are the critical loads needed to operate the bulk power system?
 - a. Within an island?
 - b. Beyond the island, that may drive restoration priorities
2. What are the priority loads needed to support public health and safety?
 - a. Within an island?
 - b. Beyond the island that may drive restoration priorities
 - c. What are the decision criteria for ranking these priority loads?
 - d. Who are the decision makers for the current priorities?
 - Are we able to communicate with these decision makers?
 - If there are no communications with this decision maker, who will make the decision?
 - How do we share and coordinate these priority load decisions?

Communications

1. Who am I able to talk to in my role as a _____?
2. Who must I talk with in my role as a _____?
3. What are the means to mitigate these communication gaps?

People

1. Are key personnel available to perform their role?
 - a. How can they best be utilized?
 - b. What key personnel gaps need to be filled, and from where?
2. What extraordinary safety concerns need to be addressed?
 - a. How will personnel be kept informed of any security-related risks?
 - b. How will field changes be documented so field operating and system operators are kept informed?

Monitoring

1. What is the organization's situational awareness of the current island?
2. Why can this situational awareness be trusted?
3. Are there other entities that might help provide additional situational awareness?
4. Based upon current topology – what are the most essential data points
 - a. Which of these essential data points is missing?
 - b. What are the possible mitigations to acquire these essential data points?
5. What other mechanisms can be used to gain some visibility of the system, no matter how limited or rudimentary?

Financing

1. What funding is available to support continued operations in the short term? How will operations be funded in the long term?
2. What funding can be shifted away from low and medium priority projects given the new normal configuration?
3. How will employees be paid if electronic transactions are not available?
4. How will customers pay bills if electronic transactions are not available?
5. How will your revenue stream be impacted? Will customers be willing to pay given the expected decrease in reliability? Will customers be able to pay given the expected economic impacts?
6. How widespread is the event? How much state or provincial aid will be available? Is federal assistance available?

Appendix 6: NERC SIRTF Roster

Chairman	Tom Bowe Executive Director of Compliance	PJM Interconnection, L.L.C. 955 Jefferson Avenue Valley Forge Corporate Center Norristown, Pennsylvania 19403-2497	(610) 666-4776 (610) 666-4287 Fx bowet@pjm.com
Vice Chairman	Paul B. Johnson, P.E. Managing Director - Transmission Operations	American Electric Power 8400 Smith's Mill Road New Albany, Ohio 43054	(614) 413-2200 (614) 413-2652 Fx pbjohnson@aep.com
	Sandy Bacik Principal Consultant	EnerNex Corp 6008 Tundra Lane Fuquay Varina, North Carolina 27526	(865) 696-4470 sandy.bacik@enernex.com
	Emanuel Bernabeu Engineer III	Dominion Technical Solutions, Inc. 2400 Grayland Avenue Richmond, Virginia 23220	(804) 432-8780 emanuel.e.bernabeu@ dom.com
	Julie Couillard Director	CTC Cable Corporation 2026 McGaw Avenue Irvine, California 92614	(949) 428-8500 (949) 428-8515 Fx jcouillard@ctccable.com
	Sean Eagleton Section Manager	Con Edison 4 Irving Place New York, New York 10003	(212) 460-2898 (212) 529-4828 Fx eagletons@coned.com
	Ian S Grant Senior Manager, NERC Planning Coordinator	Tennessee Valley Authority 1101 Market Street MR-5G-C Chattanooga, Tennessee 37402-2801	(423) 751-8721 isgrant@tva.gov
	David Grubbs Director of Regulatory Affairs and Compliance	City of Garland 217 N. 5th St. Garland, Texas 75040	(214) 802-9045 (972) 205-2822 Fx dgrubbs@garlandpower- light.org
	Jose Guzman Junior Policy Analyst - Government Services Division	Schweitzer Engineering Laboratories, Inc.	(703) 647-6241 (703) 647-6259 Fx jose_guzman@selgs.com
	Frederick P. Heller Engineer/Analyst	U.S. Department of Defense 18372 Frontage Road Suite 318 Dahlgren, Virginia 22448	(540) 653-2929 (540) 284-0143 Fx frederick.heller@navy.mil
	Bradley Hofferkamp Senior Analyst	PJM Interconnection, L.L.C. 955 Jefferson Avenue Norristown, Pennsylvania 19403	(610) 666-4688 (610) 666-4287 Fx hoffeb@pjm.com

Nicholas Ingman Manager, Operational Excellence	Independent Electricity System Operator 655 Bay Street Suite 410 Toronto, Ontario M5G 2K4	(905) 855-6108 (905) 855-6129 Fx nicholas.ingman@ieso.ca
Wallace Jensen Director Electrical Engineering	Emprimus 1660 South Highway 100 Minneapolis, Minnesota 55416	(651) 341-2090 (952) 545-2216 Fx wjensen@emprimus.com
Michael D. Johnson Lead Engineer	Florida Power & Light Co. 700 Universe Boulevard TLD/JB Juno Beach, Florida 33408	(561) 691-7548 (561) 694-4161 Fx mike_johnson@fpl.com
Miles Keogh Director of Grants and Research	National Association of Regulatory Utility Commissioners 1101 Vermont Avenue N.W. Suite 200 Washington, D.C. 20005	(202) 898-2217
Matthew Light Infrastructure Systems Analyst	Department of Energy 1000 Independence Ave., SW Washington, D.C. 20585	(202) 316-5115 matthew.light@hq.doe.gov
Toni Lineberger NERc CIP Program Manager	U.S. Bureau of Reclamation P.O. Box 25007 (84-45000) Denver, Colorado 80225-0007	(303) 445-2912 (303) 445-6573 Fx tlineberger@usbr.gov
Matthew Luallen Consultant	Sph3r3, LLC 19873 Oakwood Drive Suite A Bloomington, Illinois 61705	(312) 375-4715 m@sph3r3.com
Michael Lynch Chief Security Officer, Corporate Security and Investigations	Detroit Edison Company One Energy Plaza Detroit, Michigan 48335	(313) 235-7733 (313) 965-3853 Fx lynchm@dteenergy.com
Patricia E Metro Manager, Transmission and Reliability Standards	National Rural Electric Cooperative Association 4301 Wilson Blvd. Mail Code EP11-253 Arlington, Virginia 22203	(703) 907-5817 (703) 907-5517 Fx patti.metro@nreca.coop
Philip Mihlmester Senior Vice President	ICF International 9300 Lee Highway Fairfax, Virginia 22031	(703) 934-3560 (703) 934-3968 Fx pmihlmester@icfi.com
John G. Mosier, Jr. Assistant Vice President of System Operations	Northeast Power Coordinating Council, Inc. 1040 Avenue of the Americas, 10th Floor New York, New York 10018-3703	(212) 840-1070 (212) 302-2782 Fx jmosier@npcc.org

	Gale Nordling President/CEO/Consultant	Emprimus 1660 S. Hwy 100, Sutie 130 Minneapolis, Minnesota 55416	952-545-2051 952-545-2216 Fx gnordling@emprimus.com
	Steven Norris Director Transmission Operations	APS 502 S. 2nd Avenue M.S. 2259 Phoenix, Arizona 85003	(602) 250-1644 (602) 250-1155 Fx Steven.Norris@aps.com
	Thomas V. Pruitt Consulting Engineer	Duke Energy Carolina 526 South Church Street Charlotte, North Carolina 28202-1006	(704) 382-4676 (704) 382-3230 Fx tom.pruitt@duke- energy.com
	Michael L. Puscas Manager Critical Infrastructure Protection	Northeast Utilities 107 Selden Street Berlin, Connecticut 06037	(860) 665-2615 (860) 665-6001 Fx puscaml@nu.com
	Ken Shortt Director, Compliance	PacifiCorp 70 N. 200 East American Fork, Utah 84003	(801) 756-1237 (801) 756-1318 Fx ken.shortt@pacificorp.com
	Michael T. Tallent Manager Cyber Security Solutions	Tennessee Valley Authority 1101 N. Market Street Chattanooga, Tennessee 37402	(423) 751-3413 mttallent@tva.gov
	Terry Volkmann Consultant	Volkmann Consulting, Inc. 14240 55th Street, NE St. Michael, Minnesota 55376	(612) 419-0672 terryvolkmann@gmail.com
	Luke Weber Project Manager Operational Support	We Energies W237 N1500 Busse Road Waukesha, Wisconsin 53188	(262) 544-7393 (262) 544-7099 Fx luke.weber@ we-energies.com
	Charles A. White Vice President SCE&G Electric Transmission	South Carolina Electric & Gas Co. 220 Operations Way Cayce, South Carolina 29033	(803) 933-7242 (803) 933-7242 Fx cwhite@scana.com
	Bruce Wollenberg Professor	University of Minnesota Keller Hall 200 Union Street S.E. Minneapolis, Minnesota 55455	(612) 625-4583 (612) 625-4583 Fx wollenbe@umn.edu
	Bradley C. Young	LG&E and KU Services Company TBD Lexington, Kentucky 40507	(859) 367-5703 (502) 217-2249 Fx Brad.Young@lge-ku.com
Observer	David Batz Manager, Cyber & Infrastructure Security	Edison Electric Institute 701 Pennsylvania Ave NW Washington, D.C. 20004	(202) 508-5064 (202) 508-5445 Fx dbatz@eei.org

Observer	Steven Belle Power Supply Reliability Specialist	South Carolina Electric & Gas Co. 601 Old Taylor Road Cayce, South Carolina 29033	(803) 217-1978 steven.belle@scana.com
Observer	Stuart J. Brindley President	S. J. Brindley Consulting Inc. 4177 Vermont Cr. Burlington, Ontario Canada L7M 4A6	(905) 464-4211 stuart.brindley@gmail.com
Observer	Larry Camm Policy Analyst	Schweitzer Engineering Laboratories, Inc. 500 Montgomery Street Suite 400 Alexandria, Virginia 22314	(703) 647-6221 (703) 647-6259 Fx larry_camm@selgs.com
Observer	David A. Casey Security Lead	Consumers Energy 1935 West Parnall Road Jackson, Mississippi 49201	(517) 788-0956 dacasey@cmsenergy.com
Observer	Carl J. Eng Manager, System Operations-Engineering	Dominion Virginia Power Innsbrook Technical Center - 2 North 5000 Dominion Boulevard Glen Allen, Virginia 23060-3308	(804) 273-3305 (804) 273-2405 Fx carl.eng@dom.com
	Thomas R. Flowers President	Flowers Control Center Solutions 9338 Clark Road Todd Mission, Texas 77363	(936) 894-3649 flowersccs@att.net
Observer	Jeffrey Fuller Corporate Security/CIPManager	Dayton Power & Light Co. 1065 Woodman Drive Dayton, Ohio 45432	(937) 259-7144 jeffrey.fuller@dplinc.com
Observer	John Helme Technical Analyst	Utility Services, Inc. 25 Crossroads Suite 201 Waterbury, Vermont 05676	(802) 552-4022 (802) 214-8632 Fx john.helme@utilitysvcs.com
Observer	Charles John Hookham Vice President	HDR Engineering, Inc. 5405 Data Court Ann Arbor, Michigan 48108	(734) 332-6496 (734) 761-9881 Fx chuck.hookham@hdrinc.com
Observer	Jennifer Hubbs Infrastructure Policy Analyst	Homeland Security Infrastructure and Reliability Division Public Utility Commission of Texas	Jennifer.Hubbs@puc.state.tx .us
Observer	Anthony Jankowski Manager, Electric System Operations	We Energies W237 N1500 Busse Road Waukesha, Wisconsin 53188	(262) 544-7117 (262) 544-7099 Fx tony.jankowski@we- energies.com
Observer	Jack Kerr Consulting Engineer	Dominion Virginia Power 5000 Dominion Blvd. IN-2N Glen Allen, Virginia 23060	(804) 273-3393 (804) 273-2405 Fx jack.kerr@dom.com

Observer	Paul D. Kure Senior Consultant, Resources	ReliabilityFirst Corporation 320 Springside Drive Suite 300 Akron, Ohio 44333	(330) 247-3057 (330) 456-3648 Fx paul.kure@rfirst.org
Observer	Michael Mertz FERC Regulatory Compliance	PNM Resources Alvarado Square Albuquerque , New Mexico 87158	(505) 241-0676 michael.mertz@pnmresources.com
Observer	Melvin Miller IASO/Wireless Analyst	Nulink Wireless, LLC 15483 Murray Hill Detroit, Michigan 48227-1945	(313) 350-9129 (313) 838-6669 Fx techservices@nulinkwireless.com
Observer	Thomas Pearce Senior Utility Specialist	Public Utilities Commission of Ohio 180 East Broad Street Columbus, Ohio 43215	(614) 466-1846 (614) 752-8353 Fx thomas.pearce@puc.state.oh.us
Observer	Alan J Rivaldo Cyber Security Analyst	Public Utility Commission of Texas 1701 N. Congress Ave. Austin, Texas 78711-3326	(512) 936-7162 (512) 936-7328 Fx alan.rivaldo@puc.state.tx.us
Observer	Michael Sanders Manager, Energy Management Systems Engineering	Southern Company 600 North 18th Street 758220 P.O. Box 2641 Birmingham, Alabama 35291	(205) 257-3388 msander@southernco.com
Observer	Dan R Schoenecker Vice President of Operations	Midwest Reliability Organization 2774 Cleveland Avenue North Roseville, Minnesota 55113	(651) 855-1753 (651) 632-8572 Fx dr.schoenecker@midwestreliability.org
Observer	Jason Shaver Reliability Standards and Performance Manager	American Transmission Company, LLC W234 N2000 Ridgeway Pkwy. Ct. Waukesha, Wisconsin 53187-0047	(262) 506-6885 jshaver@atcllc.com
	Robert V. Snow, P.E. Senior Electrical Engineer, Office of Electric Reliability	Federal Energy Regulatory Commission 888 First Street, NE Room 91-13 Washington, D.C. 20426	(202) 502-6716 robert.snow@ferc.gov
Observer	Ed Tymofichuk Vice President, Transmission	Manitoba Hydro 820 Taylor Avenue P.O. Box 7950 Winnipeg, Manitoba R3C 0J1	(204) 360-4280 (204) 360-6149 Fx tetymofichuk@hydro.mb.ca
Observer	Scott Watts Senior Compliance Specialist	Duke Energy Carolina 526 South Church Street Mail Code: EC02A Charlotte, North Carolina 28202	(704) 382-2260 (704) 382-6938 Fx scott.watts@duke-energy.com

Observer	Bruce D. Wertz Senior NERC Compliance Consultant	Public Service Electric and Gas Co. P.O. Box 54865 Hurst, Texas 76054	(817) 498-0310 (801) 383-9772 Fx brucewertz@sbcglobal.net
Observer	Daniel J. Zaragoza Director - Electric Distribution Operations	San Diego Gas & Electric P.O. Box 129831 San Diego, California 92112-9831	(619) 725-5171 (619) 725-5196 Fx dzaragoz@semprautilities.com
NERC Staff	Brian M. Harrell Manager of CIP Standards, Training, and Awareness	North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, D.C. 20005-3801	(202) 393-3998 (202) 393-3955 Fx brian.harrell@nerc.net
NERC Staff	Jordan Erwin	North American Electric Reliability Corporation 3353 Peachtree Rd, NE Suite 600 Atlanta, GA	Jordan.Erwin@nerc.net
NERC Staff	Larry J Kezele Manager of Operations	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx larry.kezele@nerc.net

Appendix 7: NERC SIRTF Report Drafting Team

2

Chairman	Tom Bowe Executive Director of Compliance	PJM Interconnection, L.L.C. 955 Jefferson Avenue Valley Forge Corporate Center Norristown, Pennsylvania 19403-2497	(610) 666-4776 (610) 666-4287 Fx bowet@pjm.com
Vice Chairman	Paul B. Johnson, P.E. Managing Director - Transmission Operations	American Electric Power 8400 Smith's Mill Road New Albany, Ohio 43054	(614) 413-2200 (614) 413-2652 Fx pbjohnson@ aep.com
	Sandy Bacik Principal Consultant	EnerNex Corp 6008 Tundra Lane Fuquay Varina, North Carolina 27526	(865) 696-4470 sandy.bacik@ enernex.com
	Emanuel Bernabeu Engineer III	Dominion Technical Solutions, Inc. 2400 Grayland Avenue Richmond, Virginia 23220	(804) 432-8780 emanuel.e.bernabeu@ dom.com
	Ian S Grant Senior Manager, NERC Planning Coordinator	Tennessee Valley Authority 1101 Market Street MR-5G-C Chattanooga, Tennessee 37402-2801	(423) 751-8721 isgrant@tva.gov
	David Grubbs Director of Regulatory Affairs and Compliance	City of Garland 217 N. 5th St. Garland, Texas 75040	(214) 802-9045 (972) 205-2822 Fx dgrubbs@ garlandpower-light.org
	Bradley Hofferkamp Senior Analyst	PJM Interconnection, L.L.C. 955 Jefferson Avenue Norristown, Pennsylvania 19403	(610) 666-4688 (610) 666-4287 Fx hoffeb@pjm.com
	Nicholas Ingman Manager, Operational Excellence	Independent Electricity System Operator 655 Bay Street Suite 410 Toronto, Ontario M5G 2K4	(905) 855-6108 (905) 855-6129 Fx nicholas.ingman@ ieso.ca
	Miles Keogh Director of Grants and Research	National Association of Regulatory Utility Commissioners 1101 Vermont Avenue N.W. Suite 200 Washington, D.C. 20005	(202) 898-2217

Michael Lynch Chief Security Officer, Corporate Security and Investigations	Detroit Edison Company One Energy Plaza Detroit, Michigan 48335	(313) 235-7733 (313) 965-3853 Fx lynchm@dteenergy.com
Sean Eagleton Section Manager	Con Edison 4Irving Place New York, New York 10003	((212) 460-2898 (212) 529-4828 Fx eagletons@coned.com
Michael D. Johnson Lead Engineer	Florida Power & Light Co. 700 Universe Boulevard TLD/JB Juno Beach, Florida 33408	(561) 691-7548 (561) 694-4161 Fx Mike_johnson@fpl.com
Patricia E Metro Manager, Transmission and Reliability Standards	National Rural Electric Cooperative Association 4301 Wilson Blvd. Mail Code EP11-253 Arlington, Virginia 22203	(703) 907-5817 (703) 907-5517 Fx patti.metro@nreca.coop
Philip Mihlmester Senior Vice President	ICF International 9300 Lee Highway Fairfax, Virginia 22031	(703) 934-3560 (703) 934-3968 Fx pmihlmester@icfi.com
Steven Norris Director Transmission Operations	APS 502 S. 2nd Avenue M.S. 2259 Phoenix, Arizona 85003	(602) 250-1644 (602) 250-1155 Fx Steven.Norris@aps.com
Thomas V. Pruitt Consulting Engineer	Duke Energy Carolina 526 South Church Street Charlotte, North Carolina 28202-1006	(704) 382-4676 (704) 382-3230 Fx tom.pruitt@ duke-energy.com
Michael L. Puscas Manager Critical Infrastructure Protection	Northeast Utilities 107 Selden Street Berlin, Connecticut 06037	(860) 665-2615 (860) 665-6001 Fx puscaml@nu.com
Ken Shortt Director, Compliance	PacifiCorp 70 N. 200 East American Fork, Utah 84003	(801) 756-1237 (801) 756-1318 Fx ken.shortt@pacificorp.com
Luke Weber Project Manager Operational Support	We Energies W237 N1500 Busse Road Waukesha, Wisconsin 53188	(262) 544-7393 (262) 544-7099 Fx luke.weber@we- energies.com

	Bradley C. Young	LG&E and KU Services Company TBD Lexington, Kentucky 40507	(859) 367-5703 (502) 217-2249 Fx Brad.Young@lge-ku.com
Observer	Stuart J. Brindley President	S. J. Brindley Consulting Inc. 4177 Vermont Cr. Burlington, Ontario Canada L7M 4A6	(905) 464-4211 stuart.brindley@gmail.com
Observer	Jennifer Hubbs Infrastructure Policy Analyst	Homeland Security Infrastructure and Reliability Division Public Utility Commission of Texas	Jennifer.Hubbs@puc.state.tx.us
Observer	Jack Kerr Consulting Engineer	Dominion Virginia Power 5000 Dominion Blvd. IN-2N Glen Allen, Virginia 23060	(804) 273-3393 (804) 273-2405 Fx jack.kerr@dom.com
NERC Staff	Jordan Erwin	North American Electric reliability Corporation 3353 Peachtree Rd, NE Suite 600 Atlanta, GA	Jordan.Erwin@nerc.net
NERC Staff	Larry J Kezele Manager of Operations	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx larry.kezele@nerc.net

Cyber Attack Task Force Report

Action

Review and accept the *Cyber Attack Task Force* report prepared as part of the *Coordinated Action Plan*¹ to address high-impact, low-frequency (HILF) risks.

Background

To help the electricity industry better understand the HILF risks, NERC and the U.S. Department of Energy (DOE) issued a report titled, "*High-Impact, Low-Frequency Event Risk to the North American Bulk Power System.*"² In November 2010, the NERC Board of Trustees approved a Coordinated Action Plan under the leadership of the NERC Technical Committees to establish four task forces to address this work. One of these task forces, the Cyber Attack Task Force addressed a coordinated cyber attack scenario.

The *Cyber Attack Task Force Report* describes what aspects of cybersecurity would be particularly challenged through a coordinated cyber attack and provides options to protect the assets, systems, and networks that are critical to the reliable operation of the bulk power system. The report provides recommendations to help entities prevent, deter, detect, and respond to a coordinated cyber attack and further enhance the resilience of the bulk power system. Chapters include:

- Adversaries, motivations and capabilities
- What a coordinated attack looks like?
- Detection capabilities
- Deterrence and defensive capabilities
- Responses to attack

While many of the recommendations are intended for entity consideration, the NERC Critical Infrastructure Protection Committee has identified several requiring further development. These activities will be coordinated with the other Technical Committees and the Electricity Sub-sector Coordinating Council.

The Cyber Attack Task Force report has been reviewed and approved by the Critical Infrastructure Protection Committee. The Operating Committee, Planning Committee, and Electricity Sub-sector Coordinating Council have also endorsed the report.

¹ Ref. Coordinated Action Plan http://www.nerc.com/docs/ciscap/Critical_Infrastructure_Strategic_Initiatives_Coordinated_Action_Plan_BOT_Apprd_11-2010.pdf

² Ref. High Impact Low Frequency report <http://www.nerc.com/files/HILF.pdf>

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Agenda Item 12
Attachment 1
Board of Trustees Meeting
May 9, 2012

Cyber Attack Task Force

Final Report

March 2012

RELIABILITY | ACCOUNTABILITY



3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC's Mission

The North American Electric Reliability Corporation (NERC) is an international regulatory authority established to enhance the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; assesses adequacy annually via a ten-year forecast and winter and summer forecasts; monitors the BPS; and educates, trains, and certifies industry personnel. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the U.S. Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada.¹

NERC assesses and reports on the reliability and adequacy of the North American BPS, which is divided into eight Regional areas, as shown on the map and table below. The users, owners, and operators of the BPS within these areas account for virtually all the electricity supplied in the U.S., Canada, and a portion of Baja California Norte, México.

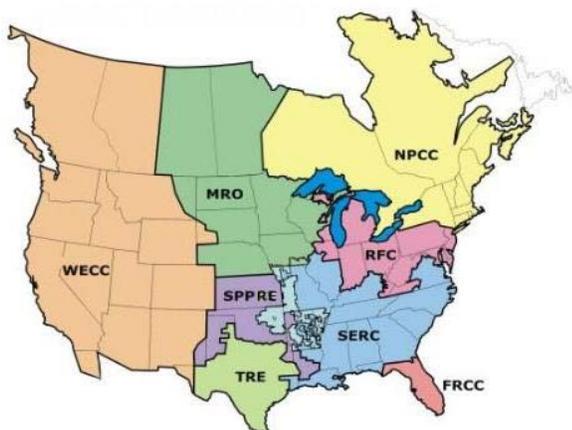


Table A: NERC Regional Entities

FRCC Florida Reliability Coordinating Council	SERC SERC Reliability Corporation
MRO Midwest Reliability Organization	SPP Southwest Power Pool, Incorporated
NPCC Northeast Power Coordinating Council	TRE Texas Reliability Entity
RFC ReliabilityFirst Corporation	WECC Western Electricity Coordinating Council

Note: The highlighted area between SPP and SERC denotes overlapping regional area boundaries: For example, some load serving entities participate in one region and their associated transmission owner/operators in another.

¹ As of June 18, 2007, the U.S. Federal Energy Regulatory Commission (FERC) granted NERC the legal authority to enforce Reliability Standards with all U.S. users, owners, and operators of the bulk power system, and made compliance with those standards mandatory and enforceable. In Canada, NERC presently has memorandums of understanding in place with provincial authorities in Ontario, New Brunswick, Nova Scotia, Québec, and Saskatchewan, and with the Canadian National Energy Board. NERC standards are mandatory and enforceable in Ontario and New Brunswick as a matter of provincial law. NERC has an agreement with Manitoba Hydro making reliability standards mandatory for that entity, and Manitoba has recently adopted legislation setting out a framework for standards to become mandatory for users, owners, and operators in the province. In addition, NERC has been designated as the “electric reliability organization” under Alberta’s Transportation Regulation, and certain reliability standards have been approved in that jurisdiction; others are pending. NERC and NPCC have been recognized as standards-setting bodies by the Régie de l’énergie of Québec, and Québec has the framework in place for reliability standards to become mandatory. NERC’s reliability standards are also mandatory in Nova Scotia and British Columbia. NERC is working with the other governmental authorities in Canada to achieve equivalent recognition.

Table of Contents

Table of Contents.....	iii
Executive Summary.....	1
Defining a Coordinated Cyber Attack	2
Enhancing Resilience.....	2
Key Recommendations	4
Introduction	1
Approach.....	1
Adversaries, Motivations, and Capabilities.....	3
Insiders.....	9
What a Coordinated Attack Looks Like	10
Prerequisites of an Attack.....	11
Coordinated Cyber Attack Scenario and Assumptions:.....	12
Detection Capabilities	14
Global Monitoring of Internet Activity	15
Federal Initiatives.....	15
Peer Groups	15
Alerts.....	16
Precursors and Local Indicators	16
Deterrence / Defensive Capabilities	18
Education / Training.....	20
Incident Response Plans	20
Information Sharing	23

Post-event analysis (Lessons Learned)	25
Procurement Language.....	26
Independent Testing of Systems and Equipment.....	26
Responses to Attack.....	27
Background	27
Isolation and Survivability.....	28
Restoration	29
Forensics	29
Recommendations	33
Outreach	38
References	40
Appendix A: Introduction to Attack Trees	42
Appendix B: Resources.....	44
Appendix C: Cyber Event Scenarios for System Operators.....	46
Overview	46
Social Engineering – false request or information to operator	47
Description	47
Implementation	47
Recognition	47
Response.....	47
Denial of Service – EMS network.....	48
Description	48
Implementation	48
Recognition	48
Response.....	48

Denial of Service – EMS applications halted.....	49
Description	49
Implementation	49
Recognition	49
Response	49
Spurious Device Operations.....	50
Description	50
Implementation	50
Recognition	50
Response	50
Realistic Data Injection	51
Description	51
Implementation	51
Recognition	51
Response	51
Appendix D: Acronyms.....	53
Appendix E: Potential Responses to an Attack.....	55
Appendix F: Precursors and Local Indicators of an Unusual Event	59
Appendix G: Isolation and Survivability Tactics	61
Appendix H: Defensive Capabilities	63
Appendix I: CRPA Observations and Recommendations.....	65
Appendix J: Case Studies.....	69
Appendix K: Task Force Goals and Objectives	73

Executive Summary

The North American bulk power system (BPS) is one of the most critical of infrastructures and is vital to society in many ways. The electric power industry has well-established planning and operating procedures in place to address the “normal” emergency events (e.g., hurricanes, tornadoes, and ice storms) that occur from time to time and disrupt electricity reliability². However, the electricity industry has much less experience with planning for and responding to high-impact events that have a low probability of occurring or have not yet occurred.

To help the electricity industry better understand these low probability risks, in June 2010, NERC and the U.S. Department of Energy issued a report titled, “*High-Impact, Low-Frequency Event Risk to the North American BPS*”³. Subsequently, the NERC board approved a *Coordinated Action Plan*⁴ under the leadership of the NERC Technical Committees to establish four Task Forces needed to address this work. This report provides the conclusions of one of them – the Cyber Attack Task Force (CATF).

This effort has challenged the CATF in a number of ways.

- The industry already recognizes cybersecurity risks, in part by addressing the requirements of the NERC Critical Infrastructure Protection standards CIP-002 – CIP009. As a result, some entities may feel they are already prepared.
- While entities are challenged on a daily basis by new cybersecurity vulnerabilities and attempted intrusions, a successful coordinated cyber attack affecting the North American bulk power system has not yet occurred. Therefore, it is difficult to confidently determine the potential impact on the reliability of the bulk power system and what additional actions may need to be taken.
- Through the course of its work, the CATF shared sensitive information related to threats, vulnerabilities, and impacts. While this information was essential to develop the recommendations found in this report, the CATF could not include these details in this public report.

The CATF has recognized these challenges and through this report offers electricity industry owners and operators (entities) a number of suggestions and recommendations. The report highlights 8 key recommendations that will help entities prevent, deter, detect, and respond to a coordinated cyber attack and further enhance the resilience of the bulk power system.

² Ref. NERC Adequate Level of Reliability http://www.nerc.com/docs/standards/Adequate_Level_of_Reliability_Defintion_05052008.pdf

³ Ref. High Impact Low Frequency report <http://www.nerc.com/files/HILF.pdf>

⁴ Ref. Coordinated Action Plan

http://www.nerc.com/docs/ciscap/Critical_Infrastructure_Strategic_Initiatives_Coordinated_Action_Plan_BOT_Apprd_11-2010.pdf

Defining a Coordinated Cyber Attack

The CATF adopted an approach that assumed a coordinated cyber attack has occurred. It did not attempt to determine the likelihood of such an attack either today or at some time in the future. The CATF also did not attempt to determine which functional entities⁵ might be more susceptible or vulnerable to attack. The CATF determined that it was more important to assume that an attack has occurred, and consider what actions need to be taken to prevent, deter, detect, and respond.

The CATF adopted the following scenario to guide their work:

An organized cyber disruption disables or impairs the integrity of multiple control systems, or intruders take operating control of portions of the bulk power system such that generation or transmission system are damaged or operated improperly.

1. Transmission Operators report unexplained and persistent breaker operation that occurs across a wide geographic area (i.e., within state/province and neighboring state/province).
2. Communications are disrupted, disabling Transmission Operator voice and data with half their neighbors, their Reliability Coordinator, and Balancing Authority.
3. Loss of load and generation causes widespread bulk power system instability, and system collapse within state/province and neighboring state(s)/province(s). Portions of the bulk power system remain operational.
4. Blackouts in several regions disrupt electricity supply to several million people.

Enhancing Resilience

“Resilience” is generally defined as the ability to recover or adjust to misfortune or change.

More specifically, the ASIS SPC.1-2009 standard on Organizational Resilience⁶ defines, “Resilience is the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event.” In recent years, in the context of strategies needed to enhance the reliable operation of critical infrastructures, resilience has come to be valued as much as protection. But what exactly is meant by resilient critical infrastructures? How is resilience measured and how much is needed?

Infrastructure Resilience

Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.

⁵ E.g., Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator

⁶ ASIS SPC.1-2009, http://www.asisonline.org/guidelines/ASIS_SPC.1-2009_Item_No._1842.pdf

In October 2010, a study group⁷ of the National Infrastructure Advisory Council issued its report “A Framework for Establishing Critical Infrastructure Resilience Goals⁸”. The report provides a broader construct for resilience originally conceived by resilience expert Stephen Flynn. The construct is based on four features organized in a sequence of events prior to, during, and after a severe emergency event.

NERC’s Severe Impact Resilience Task Force⁹ has proposed a number of recommendations and considerations from the perspective of the reliable operation of the bulk power system, regardless of the cause of the emergency event. The CATF has focused its efforts on the measures that can be taken to prevent, deter, detect, and respond to a coordinated cyber attack from the perspective of the assets, systems, and networks used to monitor, operate and control the bulk power system such as Supervisory Control and Data Acquisition (SCADA), energy management systems (EMS), and generation management systems (GMS).

Prevent Deter	Detect	Respond
✓	✓	✓

⁷ The NIAC Study Group included a number of representatives from the electricity industry, including several members of the Electricity Sub-sector Coordinating Council.

⁸ Ref. <http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf>

⁹ Ref. report *Severe Impact Resilience: Considerations and Recommendations* <http://www.nerc.com/filez/sirtf.html>

Key Recommendations

The CATF has considered what aspects of cybersecurity would be particularly challenged through a coordinated cyber attack and considered options to protect the assets, systems, and networks that are critical to the reliable operation of the bulk power system. The following summarizes the key recommendations of this report that are described in the body of the report in further detail. While some of the recommendations identify areas that require further study coordinated through NERC's Technical Committees, others recommend that entities take certain actions to enhance their ability to prevent, deter, detect, and respond to a coordinated cyber attack.

1. **Continue Work on Attack Trees** – A separate working group under NERC's Critical Infrastructure Protection Committee (CIPC) should be established to further develop attack trees with the goal of populating the nodes, performing detailed analysis, and providing recommendations to industry from this analysis.

Prevent Deter	Detect	Respond
✓		

2. **Continue to Develop Security and Operations Staff Skills to Address Increasingly Sophisticated Cyber Threats** – Entities should develop strategies to attract cybersecurity talent and further develop the knowledge, skills, and abilities of existing staff to address increasingly sophisticated cyber threats and technology challenges that accompany grid modernization efforts.

Prevent Deter	Detect	Respond
✓	✓	

3. **Augment Operator Training with Cyber Attack Scenarios** – Several cyber attack scenario templates are included in Appendix C of this report. Entities should consider enhancing training to incorporate cyber attacks that raise operator awareness for a coordinated cyber attack.

Prevent Deter	Detect	Respond
	✓	✓

4. **Conservative Operations** – The *Severe Impact Resilience: Considerations and Recommendations* report prepared by the Severe Impact Resilience Task Force offers a number of recommendations regarding conservative operations. Entities should review this report and consider the practices that would apply to a coordinated cyber attack scenario.

Prevent Deter	Detect	Respond
		✓

5. **Conduct Transmission Planning Exercise** – Working with Department of Energy's national labs and a pilot group of electricity utilities, a transmission planning exercise should be coordinated by NERC to simulate a coordinated cyber attack that creates a cascading event and blackout. The event should attempt to

Prevent Deter	Detect	Respond
✓		✓

identify the point at which current transmission planning criteria is exceeded and allow for dynamic resilience and mitigation exercise.

6. Continue to Endorse Existing NERC Initiatives That Help Entities Prepare for and Respond to a Cyber Attack

– Entities should consider greater participation and support of NERC’s initiatives that can help the industry with cyber attack identification, defense, and response. Three examples are:

Prevent Deter	Detect	Respond
✓		✓

- Cyber Readiness Preparedness Assessments (CRPA)
- NERC Grid Security Exercise
- ES-ISAC portal and collaboration

7. Increase Awareness for Department of Energy Initiatives

– The Energy Sector Control Systems Working Group recently released the *Roadmap to Achieve Energy Delivery System Cybersecurity*. NERC’s Critical Infrastructure Protection Committee should review these initiatives and support further development and implementation of these initiatives to help ensure protection of critical systems supporting bulk power system.

Prevent Deter	Detect	Respond
✓		

8. Continue to Extend Public / Private Partnership

– Entities should review their cyber incident response plans to ensure an appropriate mix of operational, security, technical, and managerial staff are aware of how they need to evaluate, respond, and make timely decisions to slow or stop a coordinated cyber attack.

Prevent Deter	Detect	Respond
		✓

This could include participating in ES-ISAC and government sponsored programs to share security-sensitive or classified information regarding cyber threats and vulnerabilities. In the event standard information sharing protocols are unavailable (e.g. between utilities, ES-ISAC, etc), alternative methods need to be defined.

Introduction

A highly coordinated and structured cyber, physical, or blended attack on the bulk power system, could result in long-term, difficult to repair damage to key system components in multiple simultaneous or near-simultaneous strikes. Unlike “traditional,” probabilistic threats (i.e. severe weather, human error, and equipment failure), a coordinated attack would involve an intelligent adversary with the capability to bring the system outside the protection provided by current planning and operating practices. An outage could result with the potential to affect a wide geographic area and cause large population centers to lose power for extended periods.

Though no such attack has been successfully executed to date on the North American grid, the bulk power system remains an attractive target for acts of both physical and cyber terrorism. Goals of these adversaries are wide-ranging and could involve extortion, societal damage, and, in the case of state-sponsored attacks, acts of war.¹⁰

Security practitioners have always found it difficult to provide convincing demonstrations that the countermeasures they deploy are effective in preventing an attack. It is fundamentally difficult to provide conclusive proof of why an event did not happen.

The purpose of the Cyber Attack Task Force (CATF) is to consider the impact of a coordinated cyber attack on the reliable operation of the bulk power system, and identify opportunities to enhance existing protection, resilience, and recovery capabilities.¹¹

Approach

The scenario itself allows for a consequence driven approach. The premise is that the outcome of the attack has unacceptable consequences. It is impossible to consider and evaluate every type of risk to the bulk power system. As a result, we focus on the risks that matter as defined by consequences.

To address the objectives and goals the task force utilized a combination of industry expertise (both IT and operational), discussions with federal agencies and law enforcement, and incorporated lessons learned from current and past initiatives.

In addition, the task force attempted to capture and catalog different attack paths that could be utilized to create specific results from the given scenario. In other words, leverage intelligence from the community of interest to define what a coordinated attack would look like. We started to capture the many steps associated with different attack paths in what is called an Attack Tree.

Security practitioners have always found it difficult to provide convincing demonstrations that the countermeasures they deploy are effective in preventing an attack. It is fundamentally

¹⁰ High-Impact Low-Frequency Event Risk to the North America Bulk Power System (June 2010)

¹¹ NERC Scope – Cyber Attack Task Force

difficult to provide conclusive proof of why an event did not happen. This is one of the reasons that the task force did not focus on the adequacy of the NERC CIP standards to prevent a coordinated cyber attack. Instead the task force included references to the CIP standards, both approved and under development, along with other tools, processes and recognized standards and guidelines from ISA and NIST as part of the industry's defensive capabilities to combat a coordinated attack. This problem is exacerbated further when dealing with unprecedented or infrequent events. Yet the threat environment going forward is likely to demand and feature a capability to prevent attacks or mitigate their impacts through coordinated response and effective information sharing.

Attack Trees are constructed from the point of view of the adversary. Creating good Attack Trees requires *"we think like an attacker"*. The task force did not focus on how to defend a utility's systems when the model was originally started. Instead the task force thought about what an attacker wants to achieve and ways to accomplish it. In this case, the attacker wants to achieve blackouts in several regions disrupting distribution supply to several million people¹². This approach was useful as those engaged for the project have a very good understanding of the mechanics associated with the elements required to severely impact the bulk power system.

One of the constraints encountered by the task force is the sensitivity of the information being gathered and determining a way to translate from sensitive to public so the larger industry can benefit from subject matter expert recommendations. This situation manifested itself on numerous occasions from discussions with law enforcement and the intelligence community on threat actor capabilities to detailed steps captured in the Attack Trees.

¹² Ingoldsby, Terrance R., 2010 Amenza Technologies Limited: Attack Tree-based Threat Risk Analysis, page 2

Adversaries, Motivations, and Capabilities

In the cyber realm, the ability to climb the line of consequences versus likelihood is very different than physical risks. The resources and requirements to execute an attack that can cause a catastrophic effect are much more available, and is really a matter of how an adversary chooses to manifest attack type or target selection.

Attacker sophistication should be measured less in technical “craft” skills and more in terms of intent fitted to environment. Disrupting or hijacking system resources is one thing...destroying trust and confidence by poisoning data or compromising privacy information is another.¹³

The defense against a cyber attack scenario will include physical as well as cyber-based elements, some procedural and others involving strategic investments in physical infrastructure, capabilities, spares, and training.

There are a variety of interventions or attacks that adversaries might contemplate and each carries unique defensive planning and resource requirements. A holistic, tailored defensive posture prioritizes and balances these to achieve the optimal cost/benefit value delivery for the defender. The defense against a cyber attack scenario will include physical as well as cyber-based elements, some procedural and others involving strategic investments in physical infrastructure, capabilities, spares, and training.

There does not appear to be a universally accepted classification or grouping of advisories. Work done by the FBI, DHS, NERC, and security consulting groups with many years of experience do not all agree what the threat actor categories should be. In this report you will see references to Groups 1-3; High, Medium and Low Threat Actors; Criminals, Hackers, Hacktivists, Nation States, Organized Crime, Structured Criminals, Terrorists, and Foreign States. As you read about these groups from the different sources, the focus should be on intent and capabilities to conduct a coordinated cyber attack on the bulk power system. But also recognize that intent and capabilities can change very quickly.

Training offered as part of the Department of Homeland Security’s Control System Security Program (CSSP) discusses three categories of threat actors: Group 1 Main Stream Threats, Group 2 Organized Threats, and Group 3 Terrorist and Nation State Threats

Group 1 is the largest threat group although they are typically not organized. These types of threats often compete for notoriety, fame, or personal research and members of this group can be anyone. There is some element of minor organization in this group, but historically the members of this group are lone actors. Often, as they become better known, and there is an increase in the demand for their services, both legal and illegal, their activity increases. It needs to be understood that there are capabilities within this group that can be used in the activities performed by group 2 and group 3 threat actors. Just because group 1 actors are not organized

¹³ Likelihood and Consequences Chart – Mike Assante 2011

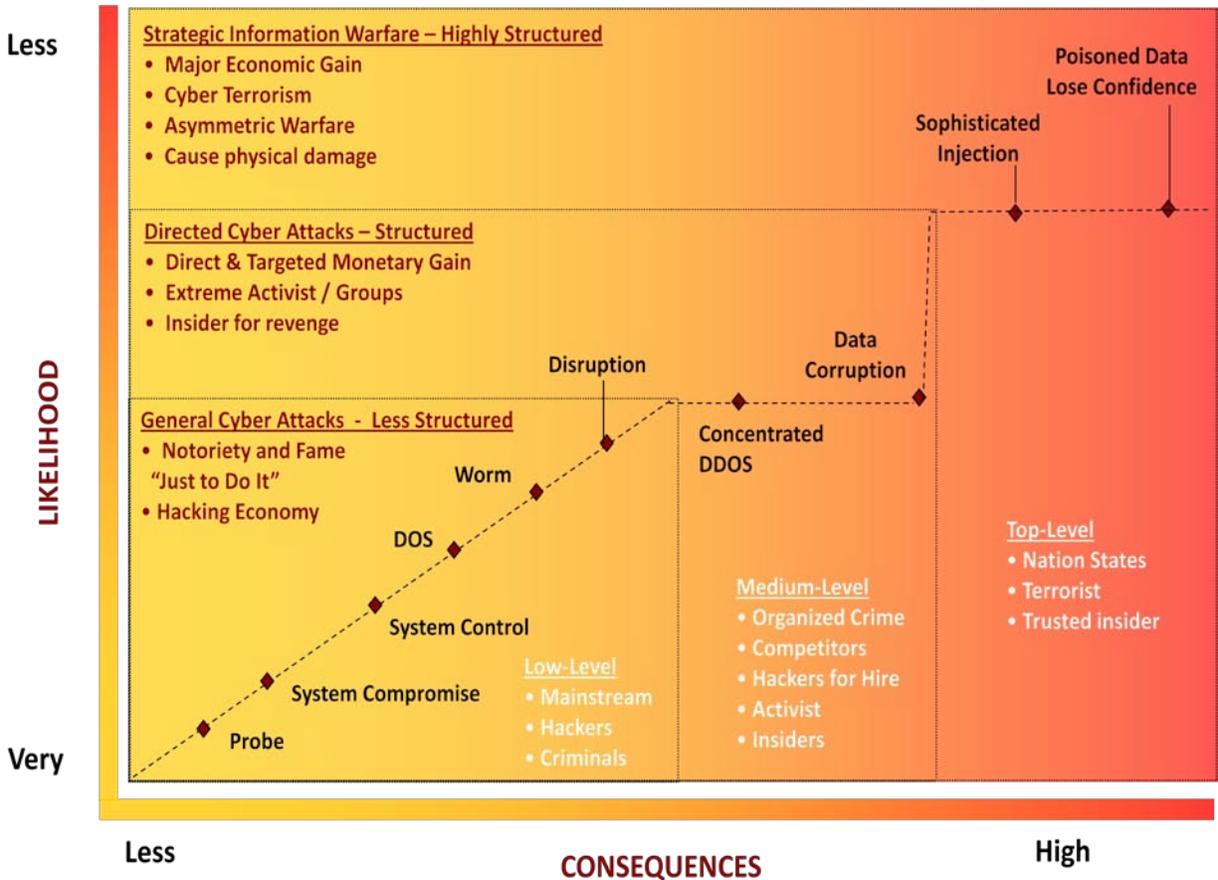
in numbers, and may not have a specific modus operandi or methodology, there is a good chance that unique capabilities exist that could be very useful in group 2 and group 3 activities.

Group 2 are more organized, and it is the organizational aspect that is cause for concern. By having a structure, this group can have membership elements that are diversified across a very large area, and may have access to disparate information systems that would normally be only accessible by a single actor. Often, collective intelligence is pooled together by group 2 members to help shape more effective and efficient attack strategies. Group 2 threats are most likely to develop specific target folders and use the information in those folders to plan, test, and perform targeted attacks.

The motivation for these attacks can be quite diversified, but it is generally observed that these attacks involve group level efforts supporting a common cause. Group 2 typically target a particular group or groups, and their motivation may be financial, revenge, theft of trade secrets or drawing attention to a cause (hacktivists). The capabilities in group 2 would be found useful in group 3 type activities, as group 2 factors often aggregate tools and methods to be more powerful. The end state of this aggregation may be attractive to group 3 actors (depending, of course, on what the goals are). Their attacks are more structured and sophisticated than group 1 attacks, but group 2 attacks often incorporate methods used by group 1. This would be expected considering that the attack lifecycle of target acquisition, system penetration, privilege escalation, and covert action is fairly ubiquitous across all group activities.

Group 3, asymmetric threats (often associated with terrorist or nation state), occurs when two forces of disproportionate size and capability are engaged in conflict. The goal of these types of attacks is to disrupt, terrorize or eliminate major aspects of society. Targets include financial institutions, political establishments, military organizations, and media outlets. Organizations involved in national security activities are also concerned about critical infrastructure, and how such threats could launch debilitating cyber attacks that include an impact on restoration and reconstitution activities. In addition to asymmetric threats, nation states that may have well-funded cyber warfare programs are also a concern.

Both asymmetric and nation state threats have significantly more resources than group 1 and 2 threats and as a result they can launch very sophisticated attacks. However, it should be understood that it is not unlikely for a group 3 actor to utilize tools, techniques, and procedures used by either group 1 or group 2. This reasoning could be extended to suggest that, when possible, group 3 actors will recruit the services of group 1 and 2 threat elements and capabilities. The impact or consequences of group 3's attack could be catastrophic.



The risk equation that is often most appropriate for critical infrastructure is one that involves threat, vulnerabilities, and consequence. Using what are commonly known as ‘threat curves’, we can plot different types of threats and their associated elements against the likelihood of such activities happening. In its simplest form, we can plot consequence against likelihood and then plot the activities of the three types of groups discussed earlier.

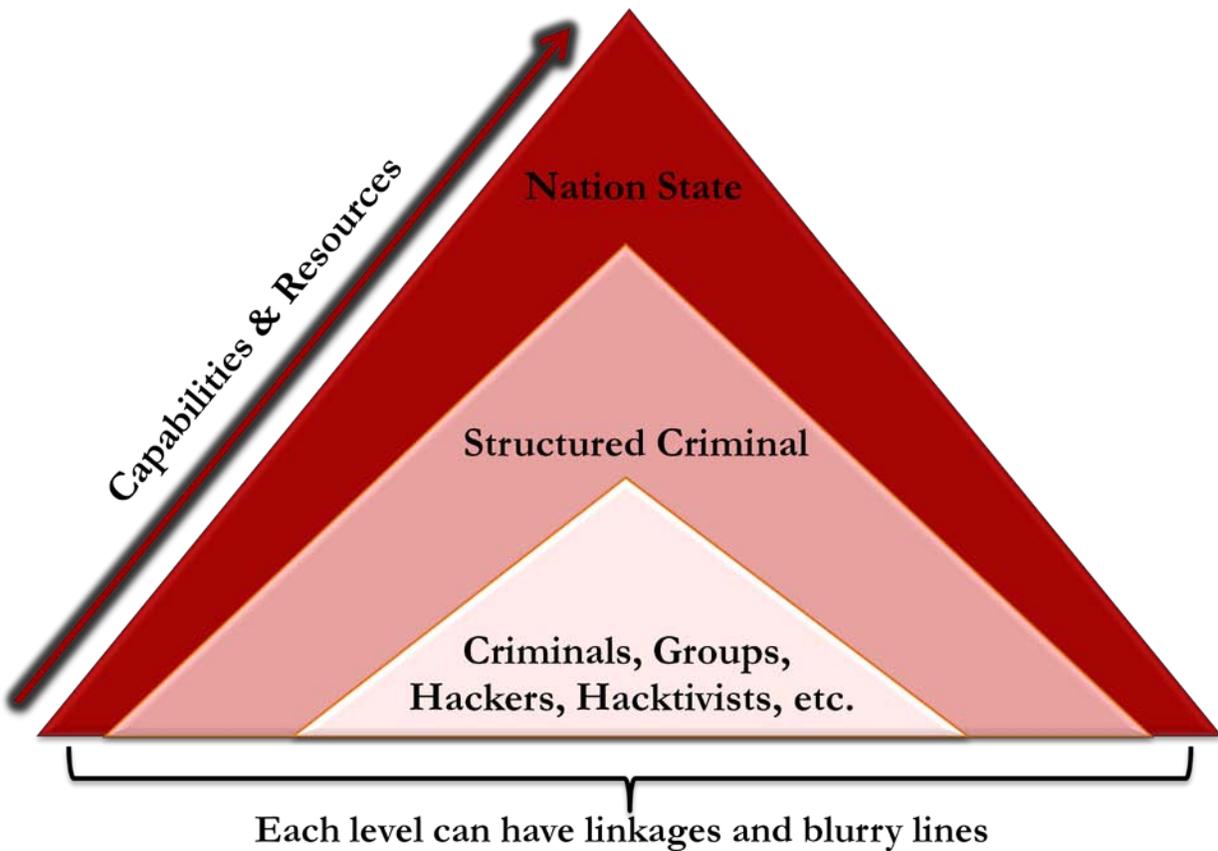
We notice from the graphic that the more benign activities would occur in the bottom left-hand corner of the graph with the most critical actions or consequences in the upper right. As the plot moves towards the top, the top right-hand element of the curve is referred to as the ‘high impact low frequency’ domain. This is the area of the graph containing the most severe consequences.

But looking at the way the curve starts in the bottom left-hand corner, we can see how the strategies of the group 1 actor curve up into the right. This is because we anticipate that the activities being performed in an attempt to generate greater consequence become more difficult to accomplish. Taking into consideration that group 1 type actors are usually lone actors, and if they do exist in small groups there is limited organization, the level of effort increases noticeably as they try to increase their attack complexity. This is not necessarily true if the lone actor is an insider. See the reference to insiders later in this document.

The curve flattens when it gets to the group 2 domain, the primary reason being that the characteristics of group 2 suggest that the organization and the cultural make up of the group

will have an ability to increase consequences without necessarily having any less likelihood of success. The reasons for this are many, but can include the fact that the group 2 structure facilitates for advanced reconnaissance and the development of target folders which would be used specifically to ensure there is enough intelligence to ensure successful attack. Group 2 may use elements and perhaps membership from group 1, but the motivations of group 2 combined with an advanced and collaborative technical capability results in an increase in consequence with no deterioration likelihood for success.

Lastly, group 3 is assumed to have very specific goals and intentions with regards to consequence. As these consequences are desired to be extreme, such as widespread economic impact and the degradation of recovery capabilities, the level of effort is significant. The interesting thing about group 3 activities in the high impact low frequency domain is that we could expect well-planned and well-funded cyber attacks to have cascading effects across critical infrastructure elements. Currently, there is an abundance of available information suggesting that national critical infrastructures have significant interdependencies and interconnectedness. The 2003 Blackout illustrated the interdependencies of critical infrastructure, and showcased how a catastrophic failure in one specific sector has extremely far-reaching results in others.



Low Level Threat

Criminals, Hackers, Hacktivists

- Can be less experienced
- Limited financial resources
- Opportunistic in nature
- Target known vulnerabilities
- Use packaged attack tools
- Can be motivated by bragging rights, theft, activism, and exploration
- Market provided defenses are usually effective

© Scipio Group, LLC 2011

Medium Level Threat

Structured Criminal

- Can be experienced and skilled
- Access to financial resources
- Targeted in their attacks
- Posses objectives
- Use a range of attack tools
- Can be detected
- Exploit known vulnerabilities very quickly

High Level Threat

Nation State

- Draw upon skilled people
- Demonstrate sophisticated tactics
- Deep financial resources
- Rely on recon and planning
- Target specific technologies & data
- Develop customized attacked tools
- Can exploit unknown vulnerabilities
- Well defined goals & objectives Difficult to detect & remove
- Can use insider access
- Access to supply chains

Attacker capabilities vary greatly based on skill level and resources. High Level Threat Actors have the capability to employ or exploit all of the following:

Network traffic capture and analysis

Intercept and modify data inputs and outputs

Inject values or data into bidirectional traffic (Man-In-The-Middle attacks)

Physical layer (tampering, inputs, and add-ons)

Data & datalink layer (MAC address spoofing, root bridge, enable unauthorized DHCP server, VLAN trunking, etc.)

Network layer (injecting blackhole, rerouting, route manipulation, inject packets and malformed packets, source route IP packets, etc.)

Application layer (DNS cache poisoning, web browser attacks, digital certificate impersonation, TCP session hijacks, injects)

System layer (Operating System attacks, privilege escalation, remote control, computer resource management, etc.)

Behavioral (people) layer (man-to-machine interface and process)

Compromising and owning a connected device with administrative privileges

Denial of service attacks (Complete, Selective, etc.)

Weak authentication/authorization

Buffer Overflows

Integer Over/Underruns

Format String Flaws

Use of fuzzers and other logic flaws

Operating System and application flaws (evaluate common code weaknesses/programming errors and IT vulnerabilities)

Connected devices, servers, and databases (injection attacks)

Access to computer resource management (the actual board)

Consider the process for updates (supply chain, vendor patches)¹⁴

Recent work by the FBI has classified threat groups into six major categories with references to methods of reaching their goal. Cyber Network Exploitation (CNE) is considered non-destructive while Cyber Network Attack (CNA) is destructive. CNE activity could be part of a long term effort to amass CNA capabilities with kinetic impacts, or generate new novel techniques, tactics, and procedures.

CNE may include expansion of threat actor understanding. CNE may also increase future CNA capability. For example, CNE in the form of exfiltration may be non-destructive in the present, but crucial to future destructive CNA capabilities or power projection.

CNA could be conducted as a means to an end in isolation, or as part of a larger, more complex effort to achieve broader goals beyond the effects of its own specific kinetic impacts. For example, CNA goals could extend to creating policy movement or fear among governments or populations.

¹⁴ Scipio Group, LLC 2011

Cyber Threat Group	Primary Motivation	What They Want	How They Get It
Foreign State	National Interest Warfare	Information Control	CNE CNA
Terrorists	Ideology	Attention	CNA
Criminal	Money	Personally Identifiable Information Ransom	CNE CNA
Hacker	Personal Interest	Methods	CNE
Hacktivist	Cause	Support	CNA
Insider	Anger Personal Enrichment	Revenge Information	CNA CNE ¹⁵

Insiders

Insiders pose the greatest threat, especially if they are working with a Foreign State or other High Level Threat Actors, because of their detailed knowledge of system operations and security practices. In addition, they have legitimate physical and electronic access to key systems and the controls designed to protect them. Insider individuals can provide qualitative, technical or physical assistance to the team requirements of sophisticated adversaries or pose a unique unilateral threat detection challenge, if acting alone.

Individuals with the highest level of access pose the greatest threat. Furthermore, an individual with access to grid infrastructure could unwittingly or inadvertently introduce malware into a system through portable media or by falling victim to social engineering e-mails or other forms of communication.¹⁶

¹⁵ FBI Presentation, NERC CIPC meeting, September 14, 2011, "US Electricity Sector Faces High Cyber Exploitation Threat, Low Cyber Attack Threat

¹⁶ Department of Homeland Security Office of Intelligence and Analysis Note – Insider Threat to Utilities

What a Coordinated Attack Looks Like

Depending on the capability and intent of an attacker, it can be very difficult to determine in advance that a coordinated cyber attack is occurring. A sophisticated attack, such as the Stuxnet worm, could have some or all of the following characteristics:

First seen (new type of attack) or very rare

Requires resources & skill to develop (thousands of hours of planning, development, and testing)

Usually highly structured threat actors

Can be specific & directed

Technology (hardware) targeted

Application (software) targeted

Objective-based (e.g. impact BPS reliability)

Can contain counters or responses to neutralize anticipated protective measures

Difficult to attribute

High reliability (usually tested before use)¹⁷

Cyber attack paths and methods (i.e. attack vectors) can also vary significantly based on the capability of the attacker, resource constraints, the intended target, and consequence. Attack vectors include:

Via communication link between data and decision layers (e.g. Historian or real-time database server)

Via connected WAN (e.g. Transmission SCADA Network, Corporate Network, etc.)

Via connected device (e.g. Travel upstream from a data concentrator or application server)

Via telecommunication network (e.g. POTS into dial-up accessible equipment)

Via Wireless network (e.g. Blue tooth, 802.11x, etc.)

Via remote connection (e.g. VPN for maintenance)

Via portable media (e.g. USB stick)

Physical access to the system¹⁸

A coordinated cyber attack may be timed to coincide with routine or abnormal bulk power system wide operational vulnerability periods in the daily or seasonal Demand-Response cycle. Cyber attacks may be combined with physical attacks which might be used to soften the system for a cyber knockout punch or to gain access to key facilities.

¹⁷ Scipio Group, LLC 2011

¹⁸ Ibid

Prerequisites of an Attack

Three conditions must be present in order for an attacker (also known as a *threat agent*) to carry out an attack against a utility's system.

1. The defender must have **vulnerabilities** or weaknesses in their system.
2. The attacker must have sufficient **resources** available to exploit the defender's vulnerabilities. This is known as **capability**.
3. The attacker must believe they will **benefit** by performing the attack. The expectation of benefit drives **motivation**.

Condition one is completely dependent on the utility. Whether condition two is satisfied depends on both the utility and the attacker. The utility has some influence over which vulnerabilities exist and what level of resources will be required to exploit them. Different attackers have different capabilities.¹⁹

Condition three is associated with intent. Does the attacker have intent to disrupt or destroy the target or to exploit the target without disruptions?

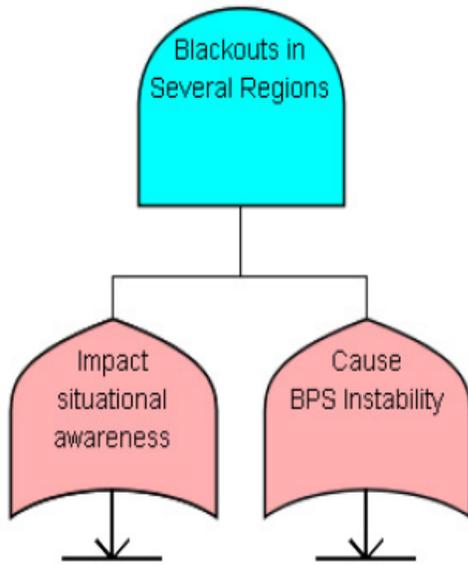
The task force chose to use an attack tree methodology to begin to build a picture of what a coordinated cyber attack could look like based on the attacker's intent to disrupt.

Attack Trees allow you to incorporate the capabilities of the attacker using specific profiles. The task force created attacker profiles that corresponded to low, medium, and high threat levels. In addition, resources (i.e. technical capability, noticeability, cost of attack, and attributability) associated with each leaf on the tree can be pruned or eliminated based on the profile of the attacker. In other words, an attacker with only medium technical ability would not be able to successfully navigate certain attack paths because steps (leaf nodes) required strong technical capabilities.

See Appendix A for an overview of attack trees.

¹⁹ Ibid, page 3

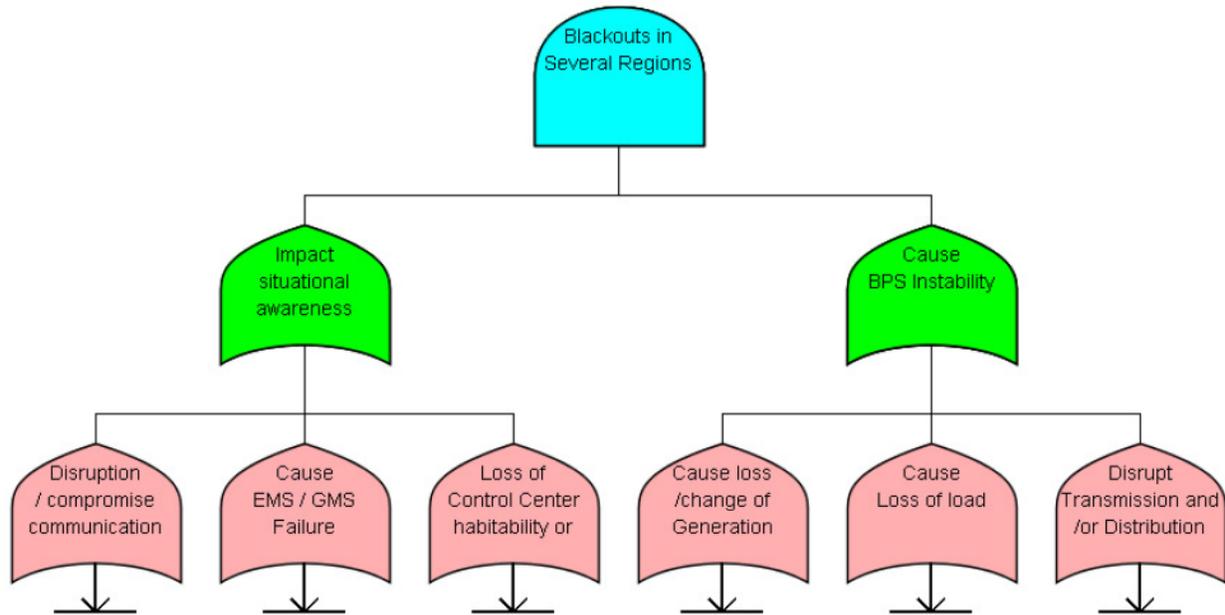
Coordinated Cyber Attack Scenario and Assumptions:



1. **BPS Instability** - Transmission Operators report unexplained and persistent breaker operation that occurs across a wide geographic area (i.e. within state/province and neighboring state(s)/province(s).)
2. **Impact Situational Awareness** - Communications are disrupted, disabling Transmission Operator voice and data with half their neighbors, their Reliability Coordinator, and Balancing Authority.
3. **BPS Instability** - Loss of load and generation causes widespread BPS instability, and system collapse within state/province and neighboring state(s)/province(s). Portions of the grid remain operational.
4. **Attack Result** - Blackouts in several regions disrupt distribution supply to several million people.

The foundation assumption for a successful attack that results in a blackout in several regions is that two events need to occur: 1) situational awareness needs to have been compromised and 2) there must be a bulk power system event or instability.

Operational events regularly occur on the bulk power system without any noticeable impact to consumers. Operators are trained to take actions to mitigate the impact of such events. However, if the operator is unaware of wide area operating conditions, he/she can't implement mitigation actions and the result can be significant.



Expanding each of the two events:

Situational Awareness is impacted IF

- There is a Disruption / Compromise in Communications OR
- There is a failure of the Energy Management System or Generation Management System OR
- The Control Center is inaccessible or uninhabitable

The BPS Instability can occur IF

- There is a Loss/Change in Generation OR
- A Loss of Load OR
- A Disruption to Transmission or Distribution

Beyond the second layer of the Attack Tree are multiple layers that expand into literally millions of steps and paths (nodes) to accomplish the attacker's intent – blackouts in several regions. Work continues in the development of comprehensive attack trees and is the subject of a task force recommendation.

Detection Capabilities

The ability to respond to an attack is contingent on the utility knowing that the attack could occur, is occurring or has occurred. The earlier the alert or warning, the better the chances that the operator, security teams and response tools can implement mitigation measures to minimize the impact of the attack on the bulk power system. However, operators can only go to the fight with the tools, awareness and training they have, so the effectiveness of mitigation depends critically on strategic preparations and investments necessarily taken over a long period of time at significant expense.

Operators must also be cognizant that the attacker may adapt to the implementation of defensive measures. But detection allows system defenders to manage the situation and make decisions to limit consequences or increase the effort required by the attacker throughout the process.

Operators must also be cognizant that the attacker may adapt to the implementation of defensive measures. But detection allows system defenders to manage the situation and make decisions to limit consequences or increase the effort required by the attacker throughout the process.

Coordinated attacks require a significant amount of planning. Consequently, indicators of an attack could be identified far outside the operator's normal field of vision. Indicators could occur at a neighboring utility, within a balancing authority, in another region or interconnect or even in another country. Indicators may arise in areas totally outside the electricity sector, such as in the finance, IT or communications sectors.

Monitoring information sources for indicators of an attack is essential to maintaining situational awareness. Effective sector information sharing is key to obtaining useful indicators and warnings of a cyber attack and bulk power system risk.

An important nexus for collaborative information sharing on threats, vulnerabilities, prevention, and mitigation is the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Operated by NERC, ES-ISAC is a center for sector-wide cybersecurity coordination, trust, and engagement. This vision is achieved through rapid sharing and analysis of information with the sector and its partners, providing sector-wide visibility and situational awareness. ES-ISAC staff are integrated with activities of the National Cybersecurity and Communications Center (NCCIC), a major government fusion cell operated by Department of Homeland Security (DHS).

In the event an attack, disables the ES-ISAC's ability to communicate with the electricity sector, a backup plan for distribution of critical information would need to be established. This is part of NERC's Crisis Plan, which is still under development. This is also true for inter-utility communication.

Global Monitoring of Internet Activity

A number of security firms and IT service providers have sensors on sections of the Internet and for a fee will provide analysis of a company's network traffic offering alerts and indicators of potential attacks or reconnaissance.

In addition, some utilities have established partnerships with IT service providers to share advanced threat information. Some of these service providers also work with Department of Defense information, and can take advantage of other information sharing sources such as the DoD Cyber Crime Center's DIBNet. For example, Lockheed Martin announced a program called Palisade intended to provide utility and energy industry IT analysts with advanced threat detection and forensic tools, actionable intelligence to effectively identify and mitigate cyber security threats.²⁰

Federal Initiatives

Several federal agencies have initiatives in progress that are designed to assist the electricity sector in identifying indicators of a coordinated attack

- Department of Energy's Electricity Sector Network Monitoring (ESNM) program coordinated with Pacific Northwest National Laboratory (PNNL).
- The Department of Defense's program with Defense Industrial Base companies and their Internet Service Providers. DoD is providing attack signatures to help identify potential attackers. This program is expected to expand into the electricity sector.
- Department of Homeland Security - The Einstein system is intended to provide the government with early warnings about cyber attacks against federal networks, near real-time identification of malicious attacks, and automated disruptions of those strikes. The first version of Einstein dates back to 2003 and the second phase rolled out in 2008. It is now deployed at 15 out of 19 departments and agencies and in 2010, Einstein 2 sensors picked up 4.5 million "hits" or alerts based on pre-determined intrusion detection signatures. The Department of Homeland Security is currently working on Einstein 3, "which will provide DHS with the ability to automatically detect and disrupt malicious activity before harm is done to critical networks and systems."

While these types of programs for monitoring and identification of attacks have a solid foundation, there are limitations. Attacks can be crafted and implemented where there are no observable signatures in place.

Peer Groups

NESCO, working with the National Electric Sector Cybersecurity Organization Resource (NESCOR), serves as a focal point bringing together utilities, federal agencies, regulators, researchers, and academics. This group, along with domestic and international experts, developers, and users help to focus cybersecurity research and development priorities, to identify and disseminate effective common practices, organize the collection, analysis and

²⁰ <http://s1.securityweek.com/lockheed-martin-launches-cyber-security-solution-utility-and-energy-industry>

dissemination of infrastructure vulnerabilities, and threats. NESCO works to identify and support efforts to enhance cybersecurity of the electric infrastructure. This project is being partially funded by the Department of Energy.

NESCO has established interest groups associated with intrusion detection, security architecture, threat assessment, and forensics.

The Electric Power Research Institute (EPRI) is coordinating several complimentary initiatives associated with industry and federal agencies. These efforts include 1) assessing combined cyber-physical attacks where the deliverables involve attack scenarios to feed into risk assessment models; 2) creating a scalable Advanced Metering Infrastructure (AMI) Incident response. The intent is a logical architecture for a scalable AMI intrusion detection system, a set of alarms and alerts to be standardized across vendors and guidelines for responding to AMI alarms.

A number of utilities have informal information sharing arrangements so sensitive information can be communicated to trusted sources.

Alerts

There are multiple sources of alert information that the electric industry can reference to better identify early signs of a coordinated cyber attack. NERC's ES-ISAC and DHS's Industrial Control System – Computer Emergency Response Team (ICS-CERT) are import providers of relevant threat and vulnerability information related to Industrial Control Systems.

Many software and hardware manufacturers have e-mail or other alert distribution methods to notify customers of vulnerabilities and associated mitigation measures.

In addition to software and hardware vendors, utilities can look to activity in other countries as a potential precursor to a coordinated attack in North America.

Specialized Industrial Control Systems software along with off-the-shelf software is utilized in other critical infrastructure sectors that have close ties to the electricity sector. For example, PLCs are used in oil and nature gas and water facilities as well as power stations. Monitoring for malicious activity in other sectors can be an early indicator of a coordinated attack in the electricity sector.

See Appendix B for a list of sources and associated links.

Precursors and Local Indicators

Experienced operators and support staff usually develop a 6th sense in regards to their job. Many times it is this "feeling" that something isn't right that heads off larger problems. While using this 6th sense is certainly valuable, establishing a baseline of expected values and then comparing those against real-time data points is an excellent method of comparison to determine if an unexpected situation exists. Following anomaly detection, trained staff can then follow-up with detailed analysis.

Appendix F contains a list that can be used as a starting point for indications of an unusual event. By developing real-time monitoring for these key metrics and comparing them to the base line, potential cyber attacks could be identified. However, these indicators do not take into consideration loss of data integrity where values are still within tolerances established by the entity. The industry eventually needs security state monitoring tools that trigger autonomic (i.e., quick device response) and/or dynamic (i.e., can evolve) corrective actions within the control system, while allowing operators to override them, if necessary²¹. One potential proxy for this type of capability is the North American Synchro Phasor Initiative.

Synchrophasors are precise grid measurements now available from monitors called phasor measurement units (PMUs). PMU measurements are taken at high speed (typically 30 observations per second – compared to one every four seconds using conventional technology). Each measurement is time-stamped according to a common time reference. Time stamping allows synchrophasors from different utilities to be time-aligned (or “synchronized”) and combined together providing a precise and comprehensive view of the entire interconnection. Synchrophasors enable a better indication of grid stress, and can be used to trigger corrective actions to maintain reliability (i.e. improving situational awareness)²².

This type of technology provides indication of electrical network issues and could be used as an early warning indicator on a large scale. However, due to the speed of cascading events whether man-made or natural and their PMU indication, response to this type of detection may need to be automatic using predefined programmatic actions.

²¹ Roadmap to Achieve Energy Delivery Systems Cybersecurity – September 2011, page 29

²² North American Synchro Phasor Initiative - <https://www.naspi.org/>

Deterrence / Defensive Capabilities

In broad terms, we can envision protecting the electricity sector with three separable, but complementary, layers of capability. The first layer is deterrence—capabilities and policies designed to convince an adversary not to launch a cyber attack. This is the job of the U.S., Canadian and Mexican governments. The second layer is defense—capabilities designed to reduce the effectiveness of the adversary’s cyber attack. This layer is primarily the responsibility of the electricity sector asset owners but does include governmental assistance. The third layer is reconstitution and robustness—capabilities designed to enable the bulk power system to continue functioning once it has suffered cyber damage and to enable the electricity sector to restore and rebuild its infrastructure after being damaged. Again, this is primarily the responsibility of the asset owners.

These layers achieve their objectives in different ways. Deterrence influences the adversary’s intentions, convincing an adversary not to attack; defense works against the adversary’s capabilities, defeating attacks that the adversary launches; reconstitution and robustness reduce the implications of successful attacks by the adversary. The layers complement each other by making up for limitations in other layers. If deterrence were known to be perfect, defense and reconstitution would be unnecessary; similarly, if defense were perfect, deterrence and reconstitution would be unnecessary. But, when none of the layers is perfect, each contributes to the sector’s overall ability to protect itself.

Deterrence is frequently divided into two types—deterrence by punishment and deterrence by denial. When relying on a strategy of deterrence by punishment, the U.S., Canadian, and Mexican governments threaten to inflict costs (i.e. punishment) in retaliation for the bulk power system being attacked. The effectiveness of deterrence by punishment depends on both the size of the costs being threatened and the credibility of the threat. Credibility depends on both the ability to retaliate and the will to retaliate.

Deterrence by denial works by a different logic: in this approach, the electricity sector deploys capabilities to convince its adversary that the probability of its attack succeeding are low; this reduces the expected benefits of the attack and can therefore result in successful deterrence.²³

The scope of this document will focus on the electricity sector’s defensive and reconstitution/robustness (i.e. survivability) capabilities.

A defense in depth security architecture has been, and continues to be, the foundation entities rely on to defend against cyber attacks. However, the engineering design of the electrical system also provides redundancy and resiliency that can help in minimizing or slowing down the impact or progress of an attack.

The NERC Critical Infrastructure Protection standards, CIP002 – CIP009 version 3, provide a minimum level of control and protection for what an entity believes are their critical assets and

²³ Deterrence of Cyber Attacks and the U.S. National Security, Charles L. Glaser

associated critical cyber assets. Specific electronic and physical controls and processes are mandated for all critical cyber assets and any cyber assets within the defined electronic and physical security perimeters.

CIP-002 – CIP-009 Version 4, which has not been approved by FERC, and CIP-002 – CIP-011 Version 5, which is still under development seek to clarify the breadth of assets that should be protected to provide adequate resiliency to the BPS in response to cyber and physical attack.

Other well known standards and documents that serve to help entities protect their key assets include;

ANSI/ISA-99 is a complete security life-cycle program, with best practices for developing and deploying policy and technology solutions to address security issues in control systems. One aspect of the standard involves containing communication in control sub-systems to avoid having security issues in one area migrate to another area. ISA-99 introduces the concepts of “zones” and “conduits” as a way to segment and isolate the various sub-systems in a control system. A zone is defined as a grouping of logical or physical assets that share common security requirements based on factors such as criticality and consequence. Equipment in a zone has a security level capability. If that capability level is not equal to or higher than the requirement level, then extra security measures, such as implementing additional technology or policies, must be taken.

- **NIST SP800-53**, “Recommended Security Controls for Federal Information Systems,” was developed primarily for Information Technology systems, but has been updated to address industrial control systems as well. It contains information for securing electronic systems from cyber intrusion. The standard is organized in sections or families of security categories.
- **NIST SP800-82**, “Guide to Industrial Control Systems (ICS) Security,” is a guideline for securing industrial control systems. It is organized much the same as NIST SP800-53, but focuses on industrial control systems.
- **SANS 20 Critical Security Controls** - These Top 20 controls were agreed upon by a powerful consortium brought together by John Gilligan (previously CIO of the US Department of Energy and the U.S. Air Force) under the auspices of the Center for Strategic and International Studies. Members of the Consortium include NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities.

In addition to the CIP standards, NERC alerts (e.g. Aurora, Stuxnet, and other vulnerabilities) provide guidance on additional controls to protect vulnerable or at risk equipment from attack.

Appendix H contains a list of some common defensive capabilities that have been or could be employed by electric utilities as part of their overall defense in-depth security architecture.

Education / Training

As a coordinated attack has not been experienced to date, an operator faced with such an attack would have no real-life experience to draw on when responding to it. Further, little training presently exists to drill responses to these events, though certain organizations have recently begun to incorporate this material into their training programs.²⁴

Training needs to include not only operators but field technicians as well. Focus should be on establishing a baseline to judge if “something looks or acts differently.” Then, the training needs to exercise the entities incident response plan which includes reporting.

Appendix C contains sample cyber attack scenarios that could be used to augment operational training.

More formal attacker/defender exercises such as those offered by Idaho National Laboratory (INL) are extremely beneficial in making entities aware of how attackers can respond.

NERC’s Cyber Risk Preparedness Assessment (CRPA) is complementary to the program offered by INL. Using cyber threat and attack scenarios, this NERC-sponsored project conducts a qualitative, expert-based assessment of the preparedness of BPS entities to detect, respond to, and limit the potential damage caused by plausible cyber incidents.

These assessments focus on BPS entities’ abilities to protect their cyber assets and improve preparedness regarding their cybersecurity posture. This is done by examining an entity’s ability to defend its information systems, deter/deny attacks against those systems, detect attacks against its own or its peer systems, and respond to cyber attacks in a timely and efficient manner. The exercise also assesses the ability of BPS entities to isolate and limit attacks so that a system is able to withstand subsequent equipment losses and quickly be restored.

The objective is to leverage technically grounded cyber threat scenarios as the basis for assessing how BPS entities might detect, respond to, mitigate, and report cyber incidents, and to identify any capability gaps in their cybersecurity postures. In turn, this assessment will be used to identify steps required to improve overall BPS preparedness.²⁵

Incident Response Plans

Many entities have existing emergency plans that can complement or provide a foundation for cyber incident response planning. CIP008 requires the establishment and testing of a cyber incident response plan on an annual basis. Some of these plans address NERC or Regional Transmission Operator (RTO) requirements to ensure operational continuity, so backup or redundant assets could be leveraged to provide on-going capabilities from an incident.

²⁴ High Impact, Low-Frequency Event Risk to the North American Bulk Power System, June 2010

²⁵ NERC Cyber Risk Preparedness Assessment – Tabletop Exercise Report April 2010

For example:

- NERC Reliability Standard EOP-005 requires a restoration plan to recover from a partial or total shutdown of the bulk power system. This plan would identify assets that would be utilized for such a recovery. The incident response plan could be enhanced to include processes for addressing cyber incidents affecting restoration plan assets.
- NERC Reliability Standard EOP-008 establishes requirements to ensure continued reliable operation of the BPS in the event of the loss of a primary control center. A cyber incident response plan could be enhanced to assess this loss from a cyber perspective and provide information to complement the loss of control center plan.

The Severe Impact Resilience: Considerations and Recommendations report created by the Severe Impact Resiliency Task Force contains recommendations to address the loss of both primary and backup control centers.

NERC Reliability Standard COM-001 establishes requirements for adequate and reliable telecommunications and operating information. Entities would establish levels of redundancy or resiliency (or both) and provide an operational plan to recover from a loss.

Incident response plans could define crucial planning materials to allow for smooth response activities. This includes defining accurate and precise roles and responsibilities between IT, operations, and other support teams. Listing potential options for containing an incident, suggested measures for removing a threat such as malware or compromised accounts, suggested forensic methods, escalation methods, third party notification procedures, including vendors and law enforcement.

Defining roles and responsibilities will assist in the escalation and mobilization of response activities. Clear delineations between teams should be defined. Additionally, particular individuals should have clear authority to make decisions surrounding investigation and response activities as well as recovery activities.

At the industry level, NERC is in the process of finalizing their Crisis Response Plan. At the national level is the National Response Framework (NRF). The National Response Framework presents the guiding principles that enable all response partners to prepare for and provide a unified national response to disasters and emergencies – from the smallest incident to the largest catastrophe. This important document establishes a comprehensive, national, all-hazards approach to domestic incident response.

The framework defines the key principles, roles, and structures that organize the way we respond as a nation. It describes how communities, tribes, states, the federal government, private-sector, and nongovernmental partners apply these principles for a coordinated, effective national response. It also identifies special circumstances where the federal government exercises a larger role, including incidents where federal interests are involved and catastrophic incidents where a state would require significant support. The framework enables

first responders, decision-makers, and supporting entities to provide a unified national response.

Complimentary to the NRF is the DHS National Cyber Incident Response Plan (NCIRP). The National Cyber Incident Response Plan (NCIRP) was developed according to the principles outlined in the National Response Framework (NRF) and describes how the nation responds to significant cyber incidents.

ES-ISAC has developed a policy protected communications corridor which delineates special protections and handling for security discussions to encourage participation from the entities and insulate against excessive compliance concerns which might otherwise impede vital security dialogue. Policies like this set the stage for enhanced security by establishing venues for effective information sharing crucial to BPS risk management and response.

Rules of engagement for detecting, containing, and eradicating various incident scenarios will help guide personnel who are familiar with the incident response plan. This may include checklists for containment methods, procedures for forensic capture and evidence handling, and guidelines for disabling compromised accounts or reimaging server equipment.

One of the most important roles of any incident response plan involves communication. Communication could involve coordination:

- Between Reliability Coordinators
- Between Balancing Authorities
- Between Transmission Operators – minimize activities (i.e. maintenance outages) that would constrain an interface
- Between utilities
- With law enforcement
- With National Security Staff
- With regulators
- With ES-ISAC
- Between other sectors (oil and natural gas, nuclear, and dams)
- With and among technology vendor community participants

Creating an incident response plan is only one step towards being prepared for a security incident. It is invaluable to hold multi-team exercises or drills which develop familiarity with the incident response plans and defined roles and responsibilities during such events. Additionally, scenario-based drills which offer a plausible situation are a powerful tool to prepare staff on the potential confusion and hesitation which is inherent in an ongoing security incident. As part of any drill and in the case of an actual coordinated attack, it is imperative to communicate significant operational actions taken including their success or failure in mitigating or stopping the attack. This information is vital to partners so their responses are complimentary and not disruptive.

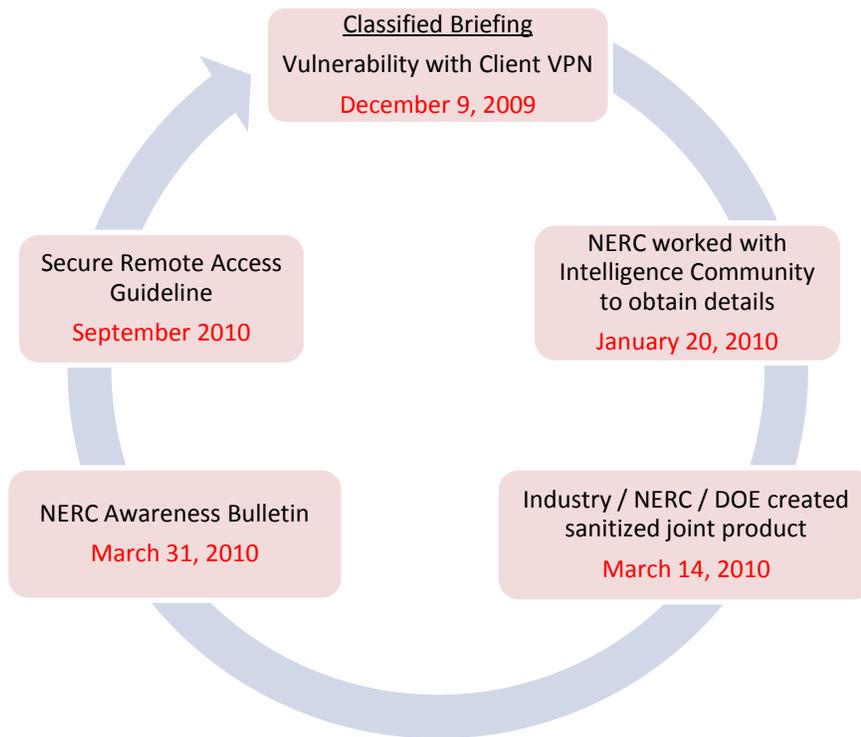
Auxiliary preparedness materials such as customer communication templates, emergency contact lists and preplanned secure/alternative communications methods (e.g. phone conference bridges; Government Emergency Telecommunications System (GETS) & Wireless Priority System (WPS) for priority access to telecommunications; satellite phone communications for the occurrence where landline and cellular facilities are not available) will enable a more rapid response operation. Creating customer communication templates may help customer support line representatives address calls from customers while other prepared documents may act as a template for communications staff to engage the local news media or government officials during or shortly after any impact from a security related incident. Emergency contact lists may list mobile contact information for management escalation and support staff such as operations staff, IT or cyber security team members. Additionally, it may list outside parties such as ES-ISAC, local, state or federal law enforcement, managed security service providers and system vendor technical support lines.

Information Sharing

Information sharing is a critical component of any preparation as well as part of the actual response plan. Besides the formal, regulatory requirements for reporting unusual events outlined in the NERC CIP standards and the Department of Energy's OE-417, there exists an informal communication network between utilities and non-regulatory entities such as the North American Transmission Forum and the North American Generation Forum.

There have been successes between the industry, regulatory agencies and the intelligence community with taking classified intelligence, having industry experts assess sensitive information in a classified setting, remove or translate sensitive data and create an alert that can be distributed to a wider audience in the electricity industry.

A case study of success:



This exercise of having industry experts work with NERC and the Intelligence Community demonstrates the process can work. Future team efforts should strive to reduce the amount of time from briefing to awareness/alert.

Existing formal and informal sources of information include: NERC ES-ISAC, RCIS / CIPIS, North American Transmission Forum, North American Generation Forum; US-CERT, ICS-CERT, RRO and RTO “communities” – mail distribution groups, newsletters, etc. and Vendor “User Communities” such as EMS users’ groups.

Energy Security Public-Private Partnership (ES3P) Joint Working Group has been formed under the Electricity Sub-Sector Coordinating Council (ESCC) and the Energy Sector Government Coordinating Council (ES-GCC). With co-Chairs from Department of Energy and NERC, as well as representation from Departments of Defense and Homeland Security, industry trade groups and interdependent sectors (such as Oil and Natural Gas, Water, Nuclear), ES3P offers a protected venue for sensitive critical infrastructure and mission assurance discussion.

Gaining awareness of a cyber attack before it occurs and stopping its effects is the best case scenario for information sharing. Sharing of information during the attack’s reconnaissance phase or early delivery phase will help achieve this end.

Sharing of concise indicators of compromise (IOC) or attempted compromise will allow for quicker analysis of information and development of mitigations to prevent future incidents. These indicators of compromise may take the form of file MD5 hashes, IP addresses, targeted

phishing email header information, captured network traffic, or other detailed activity. Such IOCs will be detected by the industry and must be shared with its various partners such as the ES-ISAC to 'connect the dots'. The correlation of related indicators of compromise reported from independent industry members will create an industry view of attacks and will lead to informed preventative and detective measures which reduce overall risk to the BPS.

Post-Event Analysis (Lessons Learned)

In order to properly prepare for the next security incident it is critical to capture lessons learned from prior incidents such as Stuxnet, Aurora, Night Dragon, Shady Rat and even events such as major hurricanes or tornados that resulted in disruptions. The lessons learned process should strive to identify how to prevent future attacks, prevent or limit disruption if they do occur, and create early visibility of such attacks through enhanced awareness and security monitoring.

Additionally, analysis of publicly disclosed attacks may provide a level of learning which may be incorporated into incident response plans, protective measures, resilience activity and preparedness. The FBI is working with the Pacific Northwest National Laboratory to evaluate and trend cases related to the electricity sector. The results of this analysis will be an important reference.

The NERC enterprise-wide event analysis program is based on the recognition that bulk power system events that occur, or have the potential to occur, have varying levels of significance. The manner in which registered entities, regional entities, and NERC evaluate and process these events is intended to reflect the significance of the event and/or specific system conditions germane to the reliability of the bulk power system and the circumstances involved.

The key ingredients of an effective post-event analysis program are to:

- Identify what transpired – sequence of events;
- Understand the causes of events;
- Understand the vulnerabilities that were exploited;
- Identify and ensure timely implementation of corrective actions;
- Develop and disseminate recommendations and valuable lessons learned to the industry to enhance operational performance and avoid repeat events;
- Develop the capability for integrating risk analysis into the event analysis process; and
- Feed forward key results to facilitate enhancements in and support of the various NERC programs and initiatives (e.g., performance metrics, standards, compliance monitoring and enforcement, training and education, etc.)²⁶

While the full or partial loss of a single EMS or SCADA system may not result in the blackout depicted in the task force scenario, analysis of the causes of such a loss could be helpful in correcting conditions on the utility's EMS or SCADA system and possibly lead to the identification of useful lessons learned for the industry. However, in the case of a coordinated

²⁶ NERC Event Analysis Program

attack, impacting potentially multiple EMS and SCADA systems, it is imperative to capture the relevant actions and responses across each utility to create an accurate timeline similar to the 2003 Blackout.

Details of intrusions or compromises should also be incorporated into attack trees to continue to build on the catalogue of attack vectors and vulnerabilities.

Procurement Language

A significant amount of work has been done by DOE, DHS, the national labs and electricity industry to create contractual language that entities can use when acquiring systems and equipment from vendors. EMS, SCADA and field devices often have a much longer operational lifetime than traditional IT business systems. By obligating vendors to provide documentation and evidence of security features, entities are better equipped to do adequate acceptance testing as well as properly design defensive measures when built-in security features need to be augmented.

See reference section for a link to the Cyber Security Procurement Language for Control Systems.

Independent Testing of Systems and Equipment

Identifying and alerting the electricity sector of vulnerabilities so mitigation steps can be implemented is an important way to limit the number of successful attack vectors. Establishing partnerships between independent testing groups, hardware and software vendors and ICS-CERT and ES-ISAC encourages vulnerabilities to be identified and industry alerts issued in concert.

Unfortunately, the independent testing community is not always in synch with the hardware and software community when it comes to prioritizing the threats or even agreeing that there is a vulnerability. Recent examples involve the S4 Project Basecamp initiative where six ICS devices were evaluated, vulnerabilities identified, and exploit code made publically available. This partnership needs further development so the time between discovery of the vulnerability, disclosure of exploit code and release of patches or alerts is minimized as much as possible.

Responses to Attack

Background

Since the 2003 Blackout Report, the electricity sector has stressed the importance for system operators to maintain situational awareness of their respective systems. In the case of Reliability Coordinators (RC) there is also the need for these RC's to maintain situational awareness over a wide area (an area that extends beyond the operating zone of the RC). To achieve situational awareness the electricity sector has over the past decades developed increasingly sophisticated network applications, meters, and telemetry to paint the view of the system in ever more accurate terms. Often times these systems refresh for the operators every few minutes and in some case every few seconds.

In spite of these applications having availability rates in the 99% range, these systems do occasionally fail. As such, every operating entity has back-up, call-out, and response plans to rapidly diagnose and address the rare application crashes.

Just as important as the system operations applications is the data and communication paths that feed these applications. These applications typically pull in thousands of data points from transmission sub-stations, lines, and generators every few seconds. In addition, entities are dependent on understanding and reacting to systems conditions with their neighbor's assets as well.

Cyber Security experts often stress the importance of being able to protect the confidentiality and integrity of data and information, and the availability of systems/applications. While the confidentiality of our customers and member's data is very important a breach of this pillar of security does not necessarily jeopardize system reliability.

In contrast the impacts associated with attacks on integrity (are outputs trusted?) and availability (are outputs meaningful and timely?) can have profound impacts on reliability.

The ideal response for these systems when under attack is to gracefully degrade in terms of capability without a material effect on operational reliability. This might mean, for example, that non-essential tools and functionality are shed, but control and communication with generating plants is maintained. If not already in place, this would require clear separation between core system reliability functionalities and business and market systems, external networks, and non-essential inputs. Networks should be designed such that these services can be quickly and easily disconnected from critical reliability functions at a moment's notice

Cyber Security experts often stress the importance of being able to protect the confidentiality and integrity of data and information, and the availability of systems/applications. While the confidentiality of our customers and member's data is very important a breach of this pillar of security does not necessarily jeopardize system reliability.

without affecting operational reliability. This will essentially allow system operators to “fly with fewer controls.”²⁷

Identification of those core systems and functions that are essential to maintaining operational reliability would include:

- EMS (energy management system) – a control system with a suite of applications that provides decision support capability to monitoring and controlling the transmission system.
 - “Model” the heart of the EMS which replicates the portion of the grid the entity is responsible for operating,
 - State Estimation (SE) the way in which the model/EMS can estimate points not physically monitored (i.e. calculate the readings in the middle of a line with data from the readings on both ends of the line) and,
 - Security Analysis (SA) the more advanced applications of the EMS that conduct the “What If” contingency analysis so that operators can always position the system in a conservative/reliable state.
- GMS (generation management system) – the suite of applications that enable an entity to keep generation and other resources in balance with load.
- Ability to maintain communications control centers and field equipment (i.e. RTUs) to provide input to EMS/GMS.
- Core skilled workforce availability.

Isolation and Survivability

Survivability involves focusing on protecting those systems and functions that are essential to maintaining reliable operations. Reliable operations will degrade, over time, resulting in the gradual reduction in services and functions until essential operations are no longer possible. The key is trying to maintain reliable operations in a reduced state for as long as possible. This resilience characteristic is known as graceful degradation of service.

A number of survivability and isolation tactics are outlined in Appendix G.

There are difficulties associated with isolation. Monitoring and situational awareness suffers as automated processes designed to inform operational staff are systemically severed. This includes both internal monitoring as well as connectivity with neighboring utilities. Bulk Power System control centers can pose risks to other BPS control systems via essential communication links. Internal data corruption, man in the middle scenarios, malicious code injections are all possible scenarios that must be considered when evaluating the operational impact that one control system may have on other externally connected control systems. Physically deploying

²⁷ High-Impact Low-Frequency Event Risk to the North American Bulk Power System page 37

staff to locations to determine status and relay information to operators in control centers would be challenging for an extended period of time.

Once integrity has been verified on end devices and communication paths, connectivity can be re-established. However, monitoring should be continued to ensure a re-occurrence of the disruption does not happen nor develop without operator recognition.

Restoration

Restoration from a coordinated cyber attack could introduce conditions that are not normally encountered during restoration from hurricanes or other types of probabilistic events.

During a cyber attack and the following aftermath, responders may be lulled into the false sense of security that there is only one wave of assault. As with a storm, once the storm passes, everyone pitches in to begin the restoration process with a clear and understood recovery plan. If the attack vector(s) and techniques/tools for the attack are not fully understood and mitigated, the attacker could launch subsequent attacks to disrupt recovery efforts or respond to mitigation efforts. These later attack waves may hold devastating impact potential if not understood and expected.

Restoration from a coordinated cyber attack could introduce conditions that are not normally encountered during restoration from hurricanes or other types of probabilistic events

To ensure the attack vector(s) and methods have curtailed and can't be restarted, entities may need to restore application files and operating systems to a safe or trusted release. This can introduce problems or delay recovery due to any entity installed modifications. In addition, certain types of attacks can render hardware or other equipment inoperable. Consequently, new equipment may have to be acquired and installed. Manufacturer assistance may need to be obtained.

Restoration of situational awareness may have to be manually implemented with staff physically stationed at key locations until communication with monitoring equipment and associated telemetry is restored. Restoration may also involve repair or replacement of parts suffering physical damage from a cyber event. Some of these may require long lead times for replacement due to supply chain or skilled installation workforce availability issues.

Safety plays an even more important role during recovery than before. Because systems and equipment may behave unpredictably during restoration, extra caution should be communicated to staff to make them aware of this issue.

Forensics

Determining the actual cause of an attack is difficult at best even with logs and other monitoring and intrusion detection capabilities found on business system networks. On the operational side of the Bulk Power System, equipment and software are not always capable of capturing information necessary to do a proper forensic analysis. Nonstandard protocols,

legacy architectures that can be several decades old, and irregular or extinct proprietary technologies can all combine to make the creation and operation of a cyber forensics program challenging.²⁸

To aid asset owners and operators in this preparation, ICS–CERT has identified key elements for developing incident response capabilities necessary to collect data and perform follow-on actions to restore systems to normal operation.

One of the key elements is preserving forensic data. This includes methods for collecting, analyzing, and reporting these data, all of which are important components of any plan to avoid loss of essential information, provide for rapid operational restoration, and improve both near and long-term mitigation and security strategies. The following activities are recommended for preserving these important data in the event of a suspected incident.

- Keep detailed notes of what is observed, including dates/times, mitigation steps taken/ not taken, strange or unusual operational behavior, device logging enabled/disabled, and machine names for suspected compromised equipment. More information is generally better than less information.
- When possible, capture live system data (i.e., current network connections and open processes) prior to disconnecting a machine suspected of being compromised from the network.
- Capture forensic images of the system memory and hard drive prior to powering down the system.
- Avoid running any antivirus software “after the fact” as the antivirus scan changes critical file dates, which impedes discovery and analysis of suspected malicious files and timelines.
- Avoid making any changes to the operating system or hardware, including updates and patches, because they will overwrite important information about the suspected malware.

²⁹

The ICS-CERT provides onsite incident response, free of charge, to organizations that require immediate investigation and resolve in responding to a cyber attack. Upon notification of a cyber incident, ICS-CERT will perform a preliminary diagnosis to determine the extent of the compromise. At the customer’s request, ICS-CERT can deploy a fly-away team to meet with the affected organization to review network topology, identify infected systems, image drives for analysis, and collect other data as needed to perform thorough follow-on analysis. ICS-CERT is able to provide mitigation strategies and assist asset owners/operators in restoring service and provide recommendations for improving overall network and control systems security.³⁰ ICS-CERT cannot, however, conduct criminal investigations.

²⁸ Recommended Practice: Creating Cyber Forensics Plans for Control Systems

²⁹ ICS-CERT Monthly Monitor July/August 2011

³⁰ DHS – Industrial Control System Computer Emergency Response Team (http://www.us-cert.gov/control_systems/ics-cert/more_information.html)

Entities that utilize outside services to assist with forensics or possible criminal prosecution should make sure the service provider or law enforcement agency is aware of all operational requirements and obligations. This could preclude or inhibit the collection of certain evidence (i.e. hardware and software) as part of the investigation.

See reference section for links to documents related to establishing a forensics program for control systems.

If prevention eventually fails, preparedness to detect the compromise before impact is realized is the next goal. The same data sources that lead to a sound post-incident forensics analysis will also provide the mechanisms to proactively detect and deter successful compromises.

These data sources include standard IT infrastructure logging such as firewall and intrusion detection systems. Secondary data sources that have proven to be invaluable during detection and forensics include Netflow data, Domain Name Resolution (DNS) logging, proxy logging, Email (SMTP) Logging, Remote Access (VPN) logging and full packet captures. It is recommended to extend the retention of these logs as long as feasible to maintain the historical forensics capability.

Once the above data sources are logged, they may be correlated together to give context of the source of the intrusion and the methods the adversary may be using. This correlation of key artifacts may be distilled into what is known as Indicators of Compromise (IOCs) which can allow for detection for follow-on attempts or sharing with the industry through trusted partners such as the ES-ISAC or ICS-CERT.

Recommendations

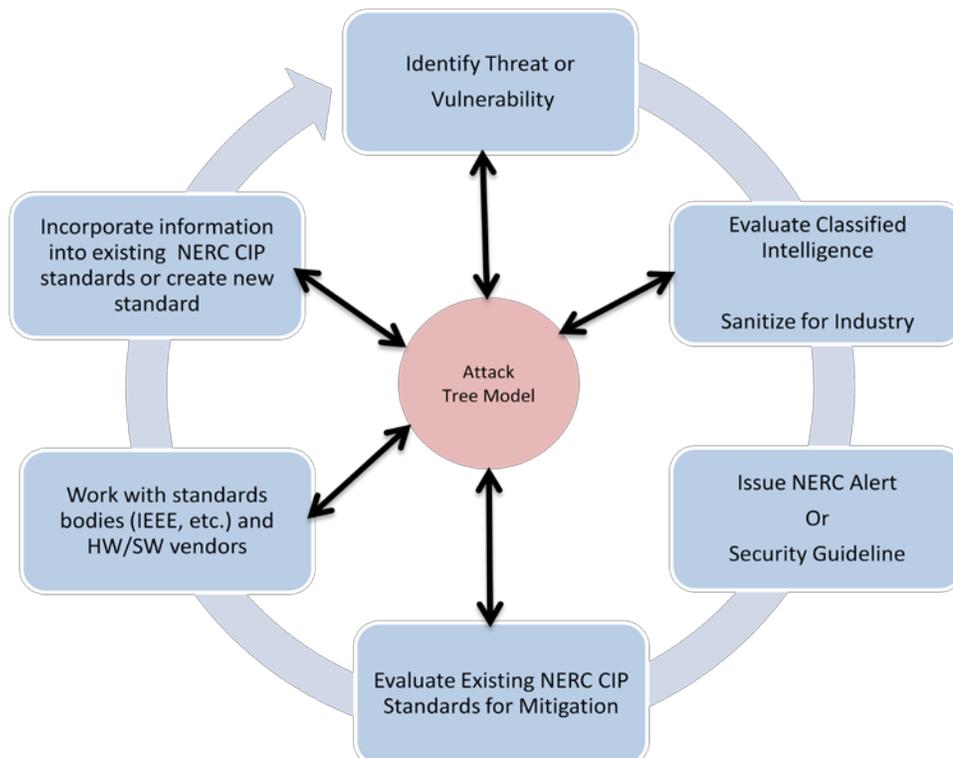
Following are the recommendations from the task force:

- Continue to build on the Attack Trees** - A significant amount of work has gone into creating the attack tree framework, however recommendations from detailed analysis have not been completed. The top level root node of the attack tree is very specific to the task force scope, but lower level branches are applicable to many other scenarios such as attacks on generation, transmission/distribution or disrupting situational awareness.

A separate working group under NERC's Critical Infrastructure Protection Committee (CIPC) should be established to further develop attack trees with the goal of populating the nodes, performing detailed analysis and providing recommendations to industry from this analysis.

While these trees will never be finished, they do provide a solid structure to build on. For example, for each revision to the CIP standards the new requirements could be incorporated into the attack trees and analysis rerun to determine any positive or negative consequences of the propose changes. Prior to release of a NERC Alert, compare mitigation measure actions against the attack trees to determine if the recommendations provide the greatest likelihood of reducing the potential for compromise. At least annually evaluate the attack trees to incorporate new information.

Because of the sensitive information captured and developed, the attack trees should be stored and managed as part of the NERC ES-ISAC documentation library, or in some cases, on classified systems.



- **Continue to develop security and operations staff skills to address increasingly sophisticated cyber threats** - Utilities should seek or develop methods to rapidly build the cybersecurity skills needed to enhance the security and reliability of the nation’s electricity delivery system. Training programs should create development plans based on job roles and identified competencies to ensure that content and delivery addresses both knowledge and skill building. Hands-on development trainers are needed to provide practice opportunities and customize training. Aptitude assessments should be used to help tailor development efforts to meet the needs of individuals and teams and assess development effort effectiveness.

Development efforts should include challenging cyber attack scenarios that are customized to the utility’s technology environments and business operations. Development efforts should recognize gaps in the knowledge, skills, and abilities of cybersecurity personnel in detecting and responding to these threats.

Entities should maintain an understanding of the current cyber threat as it applies to the electric sector; develop the skills to maintain situational awareness of that threat; strengthen the capability to match the external threat environment to the internal environment; and develop staff capability to use threat intelligence to best protect their organizations.

Development programs should identify the skill components most in need by both security and operations job roles, and use assessment tools that will ensure that the programs produce the right skills and knowledge. These efforts should be applied beyond traditional information security environments and include the SCADA emergency management system, automated generation control, plant-level control systems, protection/safety systems, and field equipment.

- **Augment Operator Training with Cyber Attack Scenarios** – Several cyber attack scenario templates are included in Appendix C of this report. Existing Operator Training Simulators (OTS) or Dispatcher Training Simulators (DTS) should be leveraged to include cyber attacks. If these scenarios can be realistically captured and simulated, operators and technical staff could train under realistic conditions to recognize, react, respond, and defend against cyber-attacks before they ever encounter one in a production setting. The training should include collaboration and teamwork with physical and cyber security experts.
- **Conservative Operations** - Conservative Operations is an operational state resulting from the intentional actions taken in response to unknown, insecure, or potentially risky system conditions in order to move to a known, secure, and low-risk operating posture.

A significant amount of work in preparing for conservative operations is documented in the Severe Impact Resilience: Considerations and Recommendations report created by the Severe Impact Resiliency Task Force. Entities should review this document for applicable best practices.

- **Continue to endorse existing NERC initiatives that help entities prepare for and respond to a cyber attack** – NERC has a number of initiatives that can help the industry with cyber attack identification, defense and response. Three examples are:
 - Cyber Readiness Preparedness Assessments (CRPA)
 - NERC Grid Security Exercise
 - ES-ISAC portal and collaboration

The 2010 CRPA report identified eight observations and associated recommendations that came from 10 utility assessments. Each company should review the recommendations outlined in Appendix I for applicability to their program.

Over 70 entities participated in the first NERC Grid Security Exercise. This provided an opportunity to test both internal and industry responses and communication capabilities.

The CIPC should encourage entities to participate in all three efforts to fine tune their response plans. NERC should continue to fund and provide the necessary resources to expand the number entities that can participate in these programs.

- **Conduct exercise with Transmission Planners** – The bulk power system is inherently highly resilient to threats. Probabilistic planning criteria consider a wide range of potential contingencies and consider probabilistic failure (i.e. equipment failure, human error, and weather events) yet do not consider a structured, coordinated, and intelligent attacker. Additionally, the definition of a “single asset” under this criterion is often based on the probabilistic failure of a given system component (i.e. a single bus or circuit breaker or a single unit at a generating plant) and may not cover the loss of every component at multiple given physical locations (i.e. several entire substations or generating plants), as could be effected by a physical attack. Cyber attacks take this one step further by creating the possibility that an asset could be misused to affect assets connected to it. Consider the example of a large substation with multiple generating units connected to it. Though this capability has not been successfully demonstrated to date, an experienced cyber attacker could use relays and breakers within that substation to affect the operation of each of those plants.

In order to accurately evaluate the system’s resilience to structured attacks, the sector should work to incorporate these new perspectives and take a broader view of the system than is generally provided by traditional system planning and operating criteria. Entities within the sector have conducted such analyses with results that indicate the system would retain its integrity in the event of certain targeted attacks, however this practice should be considered more widely as planning methods evolve. Priority should be given to designing for survivability, such that the system could withstand and recover from a structured multi-

node attack. At a minimum, system planners and operators should be able to model the effects of such an attack and drill restoration measures.³¹

Working with Department of Energy national labs and a pilot group of electricity utilities, a transmission planning exercise should be coordinated by NERC to simulate a coordinated cyber attack that creates a cascading event and blackout. The event should attempt to identify the point at which current transmission planning criteria is exceeded and how to deal with dynamic mitigation. The results could provide insight into additional facilities/locations that might need protection beyond what is called for with the CIP and Transmission Planning (TPL) standards.

The exercise scenarios should be selected from a comprehensive hazard analysis method, such as using the attack tree work completed by the CATF or selecting another rigorous approach to identify and bound the attack scenarios.

- **Increase Awareness for Department of Energy Initiatives** - The Energy Sector Control Systems Working Group recently released the latest Roadmap to Achieve Energy Delivery System Cybersecurity. There are numerous initiatives that will help ensure protection of critical systems supporting the Bulk Power System going forward. In addition, the document serves as an excellent reference document that all entities can benefit from reading. Two initiatives that can have an immediate benefit are:
 - **Digital Bond / DOE – Bandolier initiative:** Digital Bond’s Bandolier project helps asset owners and vendors identify and audit optimal security configuration for industrial control system (ICS) servers and workstations. Digital Bond partners with leading ICS vendors to identify the optimal security configuration that still allows the vendor’s product to operate properly. This requires access to the vendor’s security experts, lead engineers and a test lab. Digital Bond then creates Bandolier Security Audit Files that work with the compliance plugin in the Nessus vulnerability scanner. Bandolier Security Audit Files are available for over twenty control system components, with more on the way.
<http://www.digitalbond.com/tools/bandolier/>
 - **Digital Bond / DOE – Portaledge Project:** Portaledge is a Digital Bond research project that **aggregates** security events from a variety of data sources on the control system network and then correlates the security events to identify cyber attacks. Portaledge leverages the aggregation and correlation capability of OSISoft’s PI server, and its large installed base in the energy sector to provide this cyber detection capability in a system many industrial control system (ICS) owner / operators already have deployed.
<http://www.digitalbond.com/tools/portaledge/>

³¹ High-Impact Low Frequency Event Risk to the North American Bulk Power System page 36

- **Continue to Extend Public / Private Partnership** – More and more US and Canadian electricity sector staff have been granted clearances to see classified information. As the US and Canadian Intelligence Communities working with NERC discovers new vulnerabilities and threats, this information should be disseminated to the electricity sector as quickly as possible. The electricity industry must ensure an appropriate mix of operational, security, technical and managerial staff is cleared and available to evaluate, respond and make timely decisions to slow or stop an attack.

Effective information sharing can be enabled in multiple ways including having clearances passed to local FBI offices and Fusion Centers so expedited secure communications can be accomplished with a wider portion of the industry. It is important to ensure the inclusion of the appropriate representation from the law enforcement community, as the traditional separation of tactical field operations and national security operations do not necessarily facilitate the proper sharing of information. In Canada, jurisdiction for Canadian electricity utilities varies from province to province. The provincial law enforcement agencies have a reporting relationship with the Royal Canadian Mounted Police (RCMP).

In addition, NERC and federal agencies should continue to involve sector experts to help translate classified information (e.g. preparing useful tear-line material) into alerts that can be issued to the industry. This re-enforces the life cycle approach to addressing vulnerabilities.

The ES-ISAC offers an increasingly robust portal environment to organize electronic collaboration and this development effort should be strongly supported. ES-ISAC is establishing protective procedures to provide insulation from compliance concerns which might otherwise limit the willingness to share vital security information before, during or after a contingency. In the event standard information sharing protocols are unavailable during an attack (e.g. between utilities, ES-ISAC, etc), alternative methods need to be defined.

In parallel, the electricity sector needs to improve its sharing of information with federal agencies. Historically, there has been and continues to be a reluctance to do this because of the uncertainty about where the information could end up or that the disclosure could result in a perceived compliance violation.

Outreach

Outreach is an important part of asserting deliberate intent of the sector to cause transformative change. If the goal is to fortify sector security against a coordinated cyber attack, outreach activity will raise awareness of the issue and equip sector participants with the motivation and knowledge to enhance capabilities.

SUCCESS ELEMENTS	WHAT IT MEANS...	ACTIONS
Skilled Workforce	Long-term workforce development providing scale and capacity of vital skill sets and qualifications in security related professions and trades.	<ul style="list-style-type: none"> • Work in conjunction with National Board of Information Security Examiners (NBISE) initiatives to enhance workforce development in both IT and OT security • Encourage continued participation in Advanced Industrial Control System Red/Blue Team Training offered by Idaho National Labs.
Leadership Engagement	Leaders driven by passionate focus on security viewed as a strategic competitive advantage at entity, sector, national and international levels.	<ul style="list-style-type: none"> • Provide periodic updates to the NERC CIPC, ESCC on status of Cyber Attack Task Force and any follow-up working group activities.
Vertical Communications	Effective two-way communications between authoritative information sources and entities.	<ul style="list-style-type: none"> • Report events to the ES-ISAC, the FBI and applicable Canadian law enforcement agencies to better identify trends • Engage FBI, DHS and DOE resources to provide input to attack trees • Coordinate with DOE, the national labs and DHS on other cyber attack programs, both at the classified and unclassified level. • Communicate with FERC and Congressional staff (through NERC and Industry Trade Associations) to educate regulators about the work being done by the electricity sector.
Horizontal Communications	Communications between proactively engaged entities sharing issues, opportunities, perceived gaps and best practices.	<ul style="list-style-type: none"> • Encourage entity sharing of information with ES-ISAC related to systems events. • Participate in initiatives such as those offered by NESCO

<p>Communications Content</p>	<p>Comprehensive with holistic integration of threat, vulnerability, planning, operational, mitigation, and process issues. Standard lexicon, formats and redundant, interoperable, classification controlled pathways are employed.</p>	<ul style="list-style-type: none"> • CIPC members and other Subject Matter Experts should continue to work closely with the NERC ES-ISAC on timely and relevant alerts
<p>Advanced Technology Application</p>	<p>Provision and use of cost effective, sustainable technologies and services. Vendors and supply chain participants are energized and innovative --committed to trusted secure supply chains and optimal new product development, informed by sector expertise, emerging threats and real vulnerability gaps.</p>	<ul style="list-style-type: none"> • Work with the Energy Sector Control Systems Working Group on enhancements and updates to the Roadmap to Achieve Energy Delivery Systems Cybersecurity

References

Name	Link
DOE/NERC HILF “ <i>High Impact, Low Frequency Risk to the North American Bulk Power System</i> ” report	http://www.nerc.com/files/HILF.pdf
Critical Infrastructure Strategic Roadmap	http://www.nerc.com/docs/escc/ESCC_Strat_Roadmap_V5_20_Oct2010_clean.pdf
NERC Technical Committees’ Report – <i>Critical Infrastructure Strategic Initiatives Coordinated Action Plan</i>	http://www.nerc.com/docs/ciscap/Critical_Infrastructure_Strategic_Initiatives_Coordinated_Action_Plan_102510.pdf
NERC Scope: Cyber Attack Task Force	http://www.nerc.com/filez/catf.html
Roadmap to Achieve Energy Delivery Systems Cybersecurity – September 2011	http://www.controlsroadmap.net/pdfs/roadmap.pdf
NERC CIP Standards	http://www.nerc.com/page.php?cid=2 20
Insider Threats to Utilities	DHS Office of Intelligence and Analysis – July 19, 2011 Note
US Electricity Sector Faces High Cyber Exploitation Threat, Low Cyber Attack Threat	FBI presentation, http://www.nerc.com/docs/cip/CIPC%20Presentations%20September%202011.zip
NERC Cyber Risk Preparedness Assessment – Tabletop Exercise Report April 2010	http://www.esisac.com/Public%20Library/Reports/CRPA%202010%20Report.pdf
DHS Report – Preventing and Defending Against Cyber Attacks – June 2011	http://www.dhs.gov/xlibrary/assets/preventing-and-defending-against-cyber-attacks.pdf
DHS Recommended Practice: Creating Cyber Forensics Plans for Control Systems	http://www.us-cert.gov/control_systems/pdf/Forensics_RP.pdf
DHS Cyber Threat Source Descriptions	http://www.us-cert.gov/control_systems/csthreats.html
Recommended Practice: Creating Cyber Forensics Plans for Control Systems	http://www.inl.gov/technicalpublications/Documents/4113665.pdf
DHS -	http://www.us-cert.gov/control_systems/pdf/Incident_Handling_Brochure_Nov_2010.pdf

The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems	http://www.tofinosecurity.com/professional/use-attack-trees-assessing-vulnerabilities-scada-system
Developing an Industrial Control Systems Cybersecurity Incident Response Capability, 2009	http://www.usert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf .
NIST SP800-86 Guide to Integrating Forensic Techniques into Incident Response	http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
NIST 800-61, "Computer Security Incident Handling Guide	http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
National Electric Sector Cyber Security Organization	http://www.energysec.org/nesco
Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies	http://www.us-cert.gov/controlsystems/practices/RecommendedPractices.html
ERO Event Analysis Process	http://www.nerc.com/filez/eawg.html
NSA Manageable Network Plan	http://www.nsa.gov/ia_files/vtechrep/ManageableNetworkPlan.pdf
DHS Procurement Language for Control Systems	http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf
National Response Framework	http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf
SANS 20 Critical Security Controls	http://www.sans.org/critical-security-controls/

Appendix A: Introduction to Attack Trees

Threat trees are the first component of an attack tree. Threat (or fault) trees are used to determine whether the conditions necessary for a threat to be realized exist and are unmitigated. A threat tree consists of threat outcomes

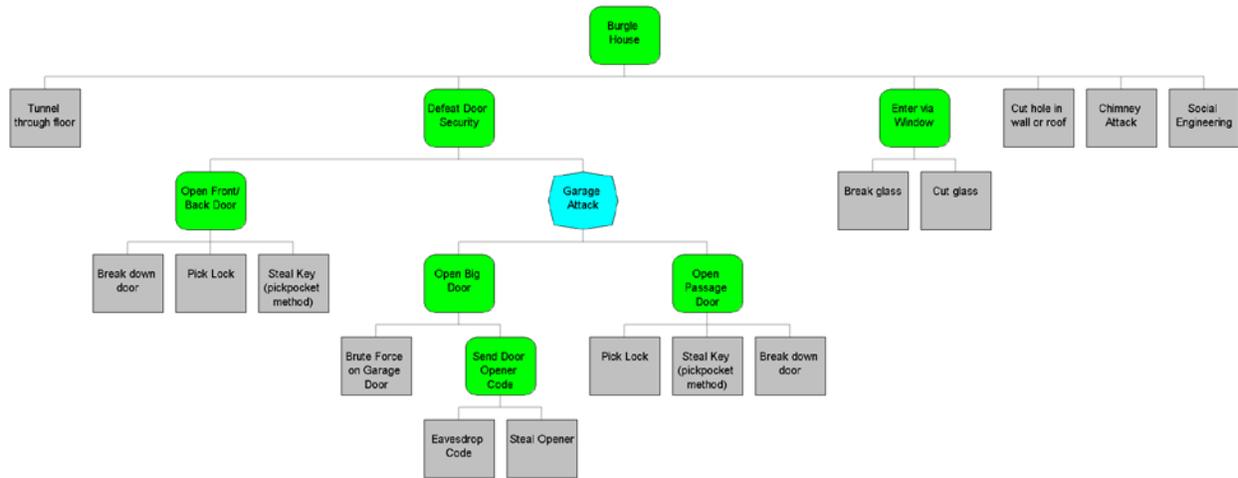
(e.g., long-term service disruption to a large area), in which preexisting conditions that must be true for an adversary to realize the threat (e.g., a circuit breaker is accessible through Internet connectivity). Any condition can, in turn, have one or more preconditions. Two or more conditions at the same level and sharing the same parent node can be combined, resulting in an “and” relationship; otherwise, an implicit “or” condition exists. Determining whether one or more vulnerabilities are associated with a threat is simply a matter of starting at a leaf condition (a node in the threat tree with no child nodes) and following it up to the root threat. If a path is unbroken by a mitigated node or a broken “and” condition exist, a vulnerability exists.

This information combined with intelligence about adversaries can be used to create an attack tree. Certain vulnerabilities are more likely to be exploited based on the attacker’s capabilities (resources, geographic location, and industry experience.), while others will be virtually impossible to exploit.

The impact of a threat can be calculated quickly from the attack tree, which can, in turn, be used to justify or inform expenditures or resource allocation planning on mitigation strategies. Impact can be calculated by adding the financial and operational impact of the root of the tree to any impact created as attackers work their way up the tree. Some of the intermediate nodes in the tree may have an adverse impact, even if the attacker doesn’t have the capabilities to extend further up the tree.

Once an impact is calculated, it is possible to calculate the value of investing in mitigation strategies. Based on the impact and the likelihood of occurrence, it is possible to determine whether countermeasures should be used for that vulnerability – or whether the vulnerability is so difficult to exploit (or has so little impact) that countermeasures are unnecessary.³²

³² American Electric and Power Attack Tree Methodology



Appendix B: Resources

United States

- NERC Electricity Sector – Information Sharing and Analysis Center (ES-ISAC)
<http://www.esisac.net/SitePages/Home.aspx>
- Department of Homeland Security
 - United States Computer Emergency Response Team (US-CERT)
<http://www.uscert.gov/>
 - Industrial Control System – Computer Emergency Response Team (ICS-CERT)
http://www.uscert.gov/control_systems/ics-cert/
 - Control Systems Security Program
http://www.us-cert.gov/control_systems/cstraining.html#workshop
- International Computer Emergency Response Teams
<http://www.internationalcybercenter.org/certicc/certworld>
- National Council of Information Sharing and Analysis Centers (ISACs)
http://www.isaccouncil.org/index.php?option=com_content&view=article&id=87&Itemid=194
- Federal Bureau of Investigation
<http://www.fbi.gov>
<http://www.infragard.net/>
- Domestic Security Alliance Council
<http://www.dsac.gov/Pages/index.aspx>

United Kingdom

- CPNI – Center for the Protection of National Infrastructure
<http://www.cpni.gov.uk/>
- SOCA – Serious Organized Crime Agency
<http://www.soca.gov.uk/>

Canada

- RCMP – Royal Canadian Mounted Police
<http://www.rcmp-grc.gc.ca/index-eng.htm>
- CCIRC – Canadian Cyber Incident Response Center
<http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx>

New Zealand

- CCIP – Center for Critical Infrastructure Protection
<http://www.ncsc.govt.nz/>

Australia

- AFP – Australian Federal Police
<http://www.afp.gov.au/>
- CERT Australia – Computer Emergency Response Team
<http://www.uscert.org.au/>

Vendor Alerts

- ABB – www.abb.com
- Alstom Grid – www.alstom.com/grid/products-and-services/electrical-network-systems/
- Open Systems International – www.osii.com
- Schweitzer Engineering Laboratories – www.selinc.com
- Siemens – www.seimens.com

Appendix C: Cyber Event Scenarios for System Operators

Overview

The following scenarios are presented in order from more plausible to less plausible. Plausibility is based on the perceived ease with which a malicious individual could accomplish the task. The scenarios are centered on operator trainee actions as opposed to support personnel actions.

We identified at least four major categories of events, and chose scenarios from among these:

- Social engineering
- Denial of service
- Spurious device operation
- Realistic data injection

Almost all of the symptoms described in these scenarios could, and in overwhelming likelihood would arise from any number of problems *other* than a cyber attack. These other likelihoods should be considered before a cyber attack is assumed.

Social Engineering – false request or information to operator

Description

In this scenario, a malicious individual contacts an operator and makes a request for action or information, or supplies false information. This individual could be a disgruntled current or former employee. They could represent themselves as field personnel, and RTO employee, or any number of legitimate individuals.

Implementation

During a training exercise a phone call could be made to the trainee, with the individual asking for an action or supplying false information.

Example: “Hello, this is John Doe at Metropolis substation. We’ve got a big problem here and need you to open the 1A breaker ASAP.”

Recognition

Awareness and a questioning attitude are probably the best tools for recognizing this scenario.

- Is this an unusual request?
- Is this a familiar identifiable person?
- Does this person possess particular knowledge about the situation when asked?
- Is this one of many unusual or suspicious requests?

Response

If a suspicious request is received, obviously the trainee would not act on it. They should:

- Try to gain more information from the caller if possible
- Consider the appropriateness of the request
- Attempt to identify the individual
- Verify the request with another entity (cross check)
- If the situation remains suspicious, report the incident to their appropriate supervision and support personnel

Denial of Service – EMS network

Description

EMS computer network becomes fully or partially unavailable, or network performance declines. Scenario proposes that malicious activity has adversely affected EMS network.

Implementation

This is most easily staged in a training simulator environment, or even on a separate training network. Any number of methods could produce the appearance of network loss or overload.

- Disconnect operator workstations from network at a location unseen by the trainees
- Remotely alter workstation or training network settings such that slow network response is observed
- Administratively terminating workstation sessions may give the appearance of network loss

Recognition

- EMS system may seem completely unresponsive
- User interface may spuriously disconnect then reconnect
- May experience timeouts when performing actions
- May experience multiple telemetry failures
- Other evidence of unauthorized system access exists or was suspected

Response

- Consider the extent of symptoms – one or two workstations, entire system, other corporate non-EMS systems
- Contact I.T. support staff
- Consider a move to offsite disaster facility while support staff secures primary EMS facility

Denial of Service – EMS applications halted

Description

Certain applications on the EMS have been maliciously halted. Therefore, the EMS system is not providing proper updates. Could be coupled with control compromise or physical sabotage in the field – the trainee of course would not be aware of it.

Implementation

Most likely requires a training simulator environment. In that environment, key applications such as the alarm system or data scanning applications are quietly halted. This might be accompanied by simulated manipulation of the actual power system while these programs are unavailable.

If the situation should go unnoticed, a simulated call from field personnel asking about a particular situation might call attention to the lack of updates.

Recognition

- EMS system does not appear to be updating
- May be lack of EMS alarms for an extended period
- Phone call from other personnel reporting changes not reflected in EMS
- When EMS system is restored, a large number of changes might be indicated
- Other evidence of unauthorized system access exists or was suspected

Response

- Cross check indicated data with other personnel or systems
- Notify support staff

Spurious Device Operations

Description

Multiple, un-commanded, unexpected device operations indicated in EMS system. Scenario could be based on:

- Indication-only compromise (devices aren't actually changing)
- Control compromise (devices are actually being manipulated)

Implementation

Most likely requires a training simulator environment. In that environment, event scenarios could be devised to:

- Simulate compromised telemetry, such that false indications and alarms are present
- Alter the power system simulation, such that power system devices actually operate (simulate a control compromise)

Recognition

- Unexpected state changes
- Could be multiple changes at unrelated locations
- May be conflicting indications (e.g. breakers open but flow present)
- Other evidence of unauthorized system access exists or was suspected
- State estimator may indicate that data is conflicting

Response

- If possible verify indications (cross-check)
- Verify with field personnel
- Call support staff

Realistic Data Injection

Description

Convincing injection of false data into EMS or associated systems, for the purpose of changing operator behavior. This is much more subtle than strict denial of service and requires much greater knowledge of the system. Examples of changed operator behavior:

- Convince them to shed load
- Convince them to allow equipment overload/damage
- Cause them to ignore changes taking place on the power system

Implementation

Most likely requires a training simulator environment. In that environment, event scenarios could be devised to bias operator indications so that they do not match the true power system simulation. The power system simulation may be trending toward an adverse state, and this would be unknown to the trainee.

Recognition

The fact that this attack is very difficult to accomplish completely can help in recognition. It is possible the offender would make mistakes such that some indications would not look normal.

- Lack of correlation between measurements
- Indications defy known system conditions
- Some indications appear abnormal (offender failed to accomplish convincing injection)
- State estimator may flag anomalies where they didn't previously exist
- Other evidence of unauthorized system access exists or was suspected

Response

- If possible verify indications (cross-check)
- Verify with field personnel
- Call support staff

Appendix D: Acronyms

AGC	Automatic Generator Control
BA	Balancing Authority
CA	Critical Asset
CCA	Critical Cyber Asset
CIPAC	Critical Infrastructure Partnership Advisory Council
CIPIS	Critical Infrastructure Protection Information System
CIPC	Critical Infrastructure Protection Committee
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Services
DOS	Denial of Service
DDOS	Distributed Denial of Service
EGSEC	Energy Grid Security Executive Council
EMS	Energy Management System
ES3P	Electricity Sector Public Private Partnership
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
ESP	Electronic Security Perimeter
ESCC	Electricity Sub-sector Coordinating Council
ICCP	Inter- Control Center Communication Protocol

ICS	Industrial Control System
IDS	Intrusion Detection System
IP	Internet Protocol (see TCP/IP)
IPS	Intrusion Prevention System
MAC	Media Access Control
MD5	Message Digest 5
OS	Operating System
PLC	Programmable Logic Controller
POTS	Plain Old Telephone Service
RC	Reliability Coordinator
RCIS	Reliability Coordinator Information System
RRO	Regional Reliability Organization (SERC, NPCC, WECC, etc.)
RTO	Regional Transmission Operator
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
TCP/IP	Transmission Control Protocol / Internet Protocol
TPL	Transmission Planning
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

Appendix E: Potential Responses to an Attack

Because attacks can come in different forms and attackers have different capabilities and motivations, it is impossible to prepare for them all. Each utility should create and execute a triage plan that will protect the most critical systems associated with real-time operations and situational awareness.

Listed below are a list of actions to consider based on the characteristics of the attack. These actions are broken up into the following categories:

- Voice and Data Communications
- Network Defenses (Internal and External)
- Operations (EMS/SCADA, Transmission, Generation)
- Information Sharing
- Forensics
- Personnel

Response Actions to Consider

- **Voice and Data Communications**
 - Determine impact to landline, VOIP and cellular communications as it relates to the Bulk Power System
 - Determine impact to ICCP, VOIP and other messaging data communications as it relates to Bulk Power System
 - Initiate satellite communication systems
 - Intra-communication to key power plants, etc.
 - Extra-communication to neighboring utilities, RC, RTOs, etc.
- **Network Defenses (Internal and External)**
 - Review password settings on key operational equipment and systems and knowledge of that information, and determine if possible modifications should be considered.
 - Check integrity of facility support systems (HVAC, water supply, physical access controls)
 - Review IDS/IPS and firewall settings to verify allowed access is still valid and required for current operating conditions.
 - Consider disconnecting external connections to business partners (e.g. VPNs or other point to point connections)
 - Remove all non-essential in-bound network access to control systems and related ESPs (remove support staff remote access)

- Remove all dial-up and remote command and control access links
- Implement IDS, IPS systems or FW rules that shun or block access attempts from source (if source info is provided)
- Review external network activity logs (especially for ESPs)
- Validate that only authorized access attempts are indicated in log files
- Tighten down host-based controls
- Temporarily change logging thresholds on key systems to capture more data for analysis
- **Operations (EMS/SCADA, Transmission, Generation)**
 - Review password settings on key operational equipment and systems and knowledge of that information, and determine if possible modifications should be considered.
 - Initiate emergency operations plans dealing w/ loss of communications and loss of control center functionality
 - Change control systems passwords for all systems deemed CCAs. Include non-CCAs as appropriate.
 - Remove contractor access to control systems and require escort access for all non-employees
 - Terminate control systems (EMS/SCADA) communication to the point that compromise is contained or rendered ineffective
 - Ensure EMS and State Estimation functions are operating properly. Validate and much as possible critical assumptions and values in database(s)
 - On a pre-determined schedule - Coordinate with Neighboring TOP/RCs on data validation points. Validation points are points where both entities have either independent monitoring or state estimated points from their own respective models. Both entities should be able to confer that based upon a predetermined set of validation points their respective state estimation and security analysis applications are both arriving at similar (not necessarily equal) values.
 - Disable EMS/SCADA control in a manner that preserves system stability while maximizing situational awareness for operators. (e.g. disable operator-initiated controls, followed by AGC if absolutely needed)
 - If disabling control fails to isolate the conditions, fully disable EMS/SCADA and operate power grid in manual mode by disabling all RTU communications. Disabling EMS/SCADA will hopefully preserve the state of the system forensic analysis.
 - Recover offsite backup tapes or “gold” copies of operating systems, configuration file, or applications for recovery purposes.

- Failover to backup control system(s)
 - Contact your key hardware and application (including EMS/SCADA/Relays) vendors.
 - Establish trigger points of distrust – i.e., if values diverge from one scan to the next by X% - attempt to validate value from other associated readings (i.e. are signals of large generation losses confirmed by changes in tie values). With such triggers, Operators should only take actions that can be validated at multiple ends via telecommunications.
 - Work with vendor to develop/implement a solution (i.e. update firmware/software, replace compromised equipment with updated firmware, passwords, etc.)
 - If attack corrupts primary and backup control center (BUCC) systems run off-line analysis from BUCC EMS packages and/or PSSE study files to validate outputs of control systems.
 - Determine whether EMS Test environments can be leveraged in any way.
 - Validate that only authorized access attempts are indicated in log file
- **Information Sharing**
 - Forward information (logs, backups, etc) to the ES-ISAC and/or ICS-CERT for further review and analysis. This includes any un-authorized access (electronic or physical) attempts.
 - Inform ISO/RTO/RC and neighboring utilities of incident
 - Contact local law enforcement for assistance with physical security
 - Actions could result in activation of NERC Crisis Plan and/or issuance of a NERC Essential Action Alert
 - Forward any evidence of related activity to ES-ISAC and *regional utilities* for further analysis and communication
 - System Operations and ESP Monitoring personnel should have frequent conference calls to correlate monitored ESP activity and system operations abnormal readings.
 - Utilize system “All-Call” and the RCIS to notify related operating entities of this activity and the need to consider validating readings and conducting conference calls to coordinate major system activities (i.e., opening lines, ramping down generation in a morning pick-up)
- **Personnel**
 - If unmanned, have a second shift man backup control centers.
 - If unmanned, deploy personnel to key substations, blackstart facilities and generation facilities

- All non-essential personnel shall be removed critical facilities (e.g. control centers, substations, generation plants)
 - All affected facilities vital to the operation of the BPS should be staffed as needed by security trained and background checked individuals during the notice
 - Co-locate Security Monitoring – or Cyber Incident Response team personnel with System Operations – so that the team can quickly assess suspect data/outputs and correlate it to ESP monitoring.
 - Perform walk-downs of all critical facilities looking for abnormalities or unusual situations (tags on equipment maintenance ports are properly installed)
 - Check seals on physical ports (i.e. maintenance ports) of programmable devices such as smart relays to determine if physical tampering has occurred.
 - If “assigned” or “trackable” seals are used to manage access, validate seal information (i.e. serial number, scan code, etc.) to ensure that the proper seal is intact.
- **Forensics**
 - Preserve evidence to the extent possible (keep the system(s) in question in a state that allows for further forensic analysis).
 - All control system logs shall be maintained for 3 years for facilities that have CCAs (this includes non-impacted sites)

Appendix F: Precursors and Local Indicators of an Unusual Event

Some activities can be a precursor to the start of an actual event. While local indicators can happen routinely, having multiple occur could be a sign of an out the ordinary situation.

Precursors to Anomalies

- Reconnaissance activity on public facing web sites, with a focus on harvesting of email addresses or other contact information
- Correlated targeted malware delivery attempts (such as spear phishing) across the industry
- Correlated malware samples contained within the industry
- Observed anomalies along perimeter, guest, remote access or wireless networks
- Anomalies of outbound or egress traffic from highly controlled environments
- Public threats by activist or hacktivist groups
- Geo-political crisis

Anomalies in EMS/SCADA system application

- Displays not updating or erratic display update times
- Alarm “heart beat” fails
- Flurry of alarms determined by the system operator to be erroneous
- Flurry of alarms by State Estimator indicating a mismatch between field values and SE.
- Generator units not responding to AGC
- Not able to recover from a Control Performance Standard 1 and 2 excursion
- Large number of RTUs not available for scanning
- AGC or electronic dispatches not matching schedules
- ICCP in-operative
- Sporadic malfunctions of equipment or process

Anomalies in EMS/SCADA system hardware behavior

- High disk I/O rate
- Quickly diminishing free disk space
- High CPU utilization
- Undocumented service(s) running
- Slow network response
- Operator consoles losing connection
- Change in network topology
- Unexpected network traffic
- Unexpected server(s) and firewall(s) restarts

- Unexpected loss of network connectivity, both internal and external
- Change in sound or pitch of equipment

Anomalies within Substations

- Alarms associated with relays, communications processors, SCADA
- Indications of physical access to equipment (tamper-proof tape on maintenance ports)
- Changes to relay configurations or settings
- Changes to ports/services on PCs or other equipment in substations (i.e. different from baseline)
- Changes to breaker settings or configurations
- Changes to RTU configurations or settings
- Passwords changed or checked out outside normal change cycle
- Alarms associated with devices unplugged or unauthorized devices connected to secured network (MAC addresses, switch ports normally turned down)
- Loss of RTU / DCS communication to the master EMS
- Change in sound or pitch of equipment

Anomalies in Situational Awareness

- Decrease in expected activity
- Similar activity as in previous hour, 24 hours or day that does not appear to match field readings
- Telemetry readings not matching schedules

Communication from (RTO and/or neighboring utilities, customers)

- Confirmed cyber security event at another entity
- Alarms associated with RTUs at interconnect points (multiple RTUs)
- Unconfirmed cyber security event
- Customer calls describing outages that do not correspond with normal alarms

Personnel

- Multiple personnel absent due to illness
- Erratic or nervous behavior
- Personnel missing or present during unusual times of during the day or shift

Appendix G: Isolation and Survivability Tactics

None of the suggested actions should be taken without first understanding the operational or situational awareness impact

Network Isolation

- Disable non-essential corporate connections to Internet, including e-mail
- Disable backup (dial-up or emergency) connections to Internet
- Disable connections with business partners (point-to-point connections and site-to-site VPNs)
- Disable remote access (dial-up, and client VPN) connectivity connections to internet
- Remove inbound connectivity to critical networks from corporate or business networks
- Remove outbound connectivity from critical networks to corporate or business networks to prevent further propagation

Operational Isolation

- Disable AGC and operate using local generator control
- Disable SCADA and Communications networks from Substations and Generation facilities
- Disable communications from Communications Processors in Substations from Intelligent Electronic Devices (IEDs) such as relays.
- Disconnect relays from breakers
- Islanding
- Under Frequency Load Shedding

Appendix H: Defensive Capabilities

Voice and Data Communications

- Telecom Companies (Cellular, POTS, etc.)– loss of RTUs, percentage thresholds
- Company owned copper – loss of RTUs, percentage thresholds
 - Have multiple path technology in place that could use several connection types / ISP's with the communications path using all that are available automatically.
- Multiple facilities/cell areas
- Cell phones / Smart phones – Social engineering, unsolicited inquiries
- Internet Service Providers detecting and dropping or rerouting malicious network traffic.
- Entity Owned Communication Networks (800 MHz, Microwave, Fiber, etc.)
- ICCP or Inter-Company Communications (Voice and Data)– loss of 2 or more simultaneously
- Satellite Communications
- Internal telecommunications facilities (e.g. ICCP.- microwave - local physical attacks (i.e. antennae structure damage)
- Dedicated facilities such as automatic ring downs (ARD) and Hotlines
- Social media – Twitter feeds, Skype, Facebook

Network perimeter defenses (border) – cyber intrusion into control center premise or critical asset premise

- Firewalls
- Intrusion Detection and Prevention systems
- Router Access Control Lists
- Data Diodes (or other methods of isolation – combination of routable and non-routable protocols)
- Vulnerability scanning and configuration management control (scans for changes in settings or configurations)
- Non-routable communications between servers
- Out of band communication to critical equipment (accessible over LAN/WAN and dial-up)
- Real-time logging of events on network and host devices.
- Alarms setup based on defined thresholds for abnormal events such as login fails, privileged account usage, or device probes that result in “access denied messages”.
- Ability to query the log database for specific items that may not be in the current alarm pattern

- Security Information Event Management (SIEM) systems that consolidate logs and provide correlation of seemingly unrelated events,

Physical Defenses or Deterrence

- Motion detection – motion detector alarms, cameras, floodlights, control house intrusion alarms, loss of oil or over-temp transformer alarms
- Key card access
- Use of biometric controls
- Mantraps or other physical barriers that prevent tailgating
- Use of special locks for gates, equipment
- Increased patrols by law enforcement / contracted security
- Logging of physical access
- Increase access restrictions:
 - Advance notification for visitors
 - Limit access by outsiders to business need
- Increase use of security cameras, video surveillance.
- Staffing levels of key facilities
- Background checks
- Continuous behavioral monitoring
- Random drug testing

Generation Defenses

- Use of “Constant Frequency Operations” – previously defined for the Y2k transition.
- Use of “Conservative Operations” to maintain extra capacity
- Day-Ahead Planning – conservative mode unit commitment to maintain extra capacity and responsiveness
- Operation near unity power factor to maintain reactive capability (VAR reserves)
- Blackstart

Appendix I: CRPA Observations and Recommendations

Observations and Recommendations

Observation 1 - Most of the exercises and mini-programs included aspects of concurrent physical and cyber incidents, a tactic used to bring familiarity to the traditional domain of perimeter compromise to the assessment space. This use of mixed incidents was most prevalent when the participating entity migrated to Internet Protocol-based substation and SCADA operations. The goal was to determine general levels of readiness as they pertained to mapping physical asset break-ins to plausibly impact the cyber infrastructure. All entities had formal process and checklists to manage response to physical break-ins and theft of copper, equipment, and other valuable items. However, none had a process to consider if any technology had been *added* to the environment, such as rogue access points, radios, or other devices that could provide access to the EMS operational domain.

Recommendation 1 - Entities should update standard procedures for facility break-ins to include examination of systems for unauthorized changes to cyber assets. Additionally, entities should conduct system “sweeps” to identify any new equipment that may have been introduced to facilitate unauthorized access to the energy management command and control network.

Observation 2 - Most entities involved in the program had some form of cyber incident response plan in place or in development. In each case, the plans identified and assigned personnel and roles to respond to a cyber incident, but the plans lacked contingency planning in the event key personnel were not available. During the exercises and outreach campaigns, several participants noted that they were unfamiliar with the entire set of incident response activities, such as escalation, points of contact, impact analysis, etc. This observation suggests that, although a first-line of response had been established (and roles assigned), there was no capability to back-fill or cross-pollinate roles during a cyber incident. This issue can increase risk if, during an incident, trained personnel are not available and activities cannot be performed.

Recommendation 2 - The entire response team should be assigned primary and secondary roles, guaranteeing overlap in capabilities should the situation require it. Also, entities should include more group members from each response group in incident response training. This redundancy will provide some depth to the entity’s “bench strength” and offer more resiliency. An entity should select a minimum number of people per department who should have incident response training, and ensure that those people receive the necessary training. Cross-train at least two additional staff members as incident response leaders who can take command of incident response activities.

Observation 3 - Having a corporate capability to interact with local and federal law enforcement during or after a cyber incident is something all entities deemed mandatory. While most organizations had at least one person in place that had some contacts in the law enforcement community, very little of their experience and knowledge had been internalized by the organization in the form of policies and procedures. After action reporting from exercise activity, combined with outreach and entity interviews, suggested that incorporating a law-enforcement communication function in the incident response plan would be useful, and that any experience and relationships entity personnel may have should be leveraged.

Recommendation 3 - Entities should work with local law enforcement to create a pre-populated list of law enforcement activities that could be performed during a cyber event. Establishing a pre-determined communication protocol with law enforcement entities would also be beneficial in helping to understand what law enforcement will do if called to support investigations. Feedback from participating entities suggested including law enforcement in exercise training activities, and proactively working with law enforcement to understand what is required should an actual incident occur. Entities should initiate a cooperative partnership with local Federal Bureau of Investigation or Royal Canadian Mounted Police offices, and include them in the response planning activities. NERC may wish to review any framework development that empowers BPS entities to create a law enforcement communication plan based on known investigative procedures, or suggest the augmentation of NERC CIP language to define the parameters that support law enforcement communications.

Observation 4 - During the exercises, interviews, and after-action discussions, the majority of participants appeared unsure about the necessary involvement of the RC in a cyber incident and are unsure how or when to engage them.

Recommendation 4 - Entities may wish to explore this issue further, as present protocols in place for interaction with RCs may not always include strategies as it pertains to a cyber incident where (a) reliability of BPS operation may be jeopardized, and (b) the communications path to the RC may be an attack vector. Entities are encouraged to work with their RC to establish a set of pre-defined incident response procedures which will determine when to include them in the communication chain during an incident. Moreover, NERC should investigate the protocol regarding entity-RC communications and reporting during cyber duress.

Observation 5 - The CRPA covers many aspects of entity operations and looks specifically at security operations for critical cyber assets; also included in the project activities were Primary Control Centers (PCC)/Main Control Centers and Back Up Control Centers (BUCC). A review of the findings indicates that, in many cases, the entity maintains BPS operations across a flat network and, to support redundancy, mirrors activities to a BUCC on that network. As the BUCC receives updates in real time from the systems in the PCC, a potential attack vector to the BUCC is established. Observations show that this architecture could create a situation where a cyber incident can impact mission critical backup data and critical cyber assets in the BUCC. The recovery protocol deployed suggests that should operators need to close the PCC and move to the BUCC, the operational environment at the BUCC would be useless as it has been compromised by association or archived (recovery) data is corrupted.

Recommendation 5 - Entities should consider expanding cyber protection measures to the communications infrastructure that support primary and backup facility operations. As it is assumed that all critical contingency communication resides behind and within the ESP, entities should consider monitoring the connection between the BCC and PCC for anomalous communications and other potential security-related events.

Observation 6 - The exercises showed that, while the technical teams were often quick to respond to the cyber incident (and begin their incident response activities), there were situations where no clear incident “leader” emerged to manage the incident on behalf of the whole organization. Key elements that were not coordinated included media relations, customer support, law enforcement, regulatory authorities and reporting agencies, and communications.

Recommendation 6 - Entities should continue to create and run incident response training exercises which include, and even focus on, management teams.

Observation 7 - The CRPA exercises, interviews, and after-action reporting demonstrated that the security architecture of vital transmission and distribution assets was constructed with significant security controls. Observers noted that assets are often managed by an internal team with a high level of skill and knowledge pertaining to BPS resiliency and EMS recovery. However, in many cases, the management of an entity’s generation element(s) has been outsourced to third parties, resulting in increased response times, reduced control systems knowledge, and an impaired ability to manage energy assets in accordance with the entity’s response protocols. These issues created extreme difficulty in managing fast-paced cyber incidents that include generation assets.

Recommendation 7 - Although these situations can be rare, the risk associated with insufficient security knowledge and response experience in the generation asset domain could prove to be significant during a cyber incident. Entities should consider moving management of all assets within the main EMS/SCADA and IT Engineering groups, resulting in an improvement to the overall management of generation assets.

Observation 8 - Despite the number of public displays of system compromise in recent years, combined with well-known cyber incidents impacting the energy sector, some individual participants remain skeptical about the possibility of a successful cyber attack on their own critical cyber assets, and as an extension, of the BPS cyber infrastructure itself. Participants did concede, however, that participating in scenario-driven exercises that used non-fictitious elements (cyber attack) to force them to test traditional response activities was very useful.

Recommendation 8 - As the threat and risk landscape can change quickly, entities are encouraged to incorporate specific intelligence about their operations into their planning and training agenda. In addition, as part of the risk assessment process, entities could extend their activities to determine actual and plausible threats against their cyber infrastructure and use that data to populate their exercise and training curricula. Training activities for SCADA/EMS operators should be expanded to include general cybersecurity training to all EMS/SCADA IT, Electric System Operations, Corporate IT, and IRT training regimens.

Appendix J: Case Studies

Breaking Air Gap Myths About Control System Inaccessibility - Stuxnet

Just because there is an “air gap” doesn’t mean a control system is inaccessible to adversaries. Stuxnet is a great example. A USB thumb drive can be transported from an infected host machine and inserted into the target network that is air-gapped. Then stuxnet can propagate on the local target network via multiple exploits. That propagation results in forming a hostile Peer to Peer (P2P) network which operates on the probability of finding resident hosts with indirect or direct internet accessibility. It then utilizes these hosts to establish an indirect Command and Control (C2) bridge for hostile control. In sum, USB served as not only the delivery mechanism but also to establish a network of hostile P2P relationships within the target network.

Another Example, Breaking Air Gap Myths About Control System Inaccessibility – Buckshot Yankee

SIPRNET is Department of Defense’s (DoD) Secret-level network. This network is commonly perceived as completely air-gapped, yet in 2010 Deputy Defense Secretary William Lynn publicly disclosed a 2008 worm infestation on the network. The DoD response to this infestation was called Buckshot Yankee. Also in 2010, well-known former counter terrorism official Richard Clarke released a book entitled “Cyber War.” Clarke gave a more detailed account of Buckshot Yankee. The delivery mechanism was USB insertion, much like stuxnet, but its C2 method was novel. Instead of P2P C2, Buckshot Yankee relied on sneaker-net C2. The infected thumb drive payload carried not only the malware worm but also a data file. This data contained requests and responses which serve as a C2 channel to the next internet connected devices the USB is inserted into. The result: USB creation of an effective hostile sneaker-net C2 channel across the perceived air gap which “secures” the target network. The bottom line: USB established a delivery mechanism within an air-gapped network and then sneaker-net connectivity enabled by repeated usage of USB devices between both air-gapped and non-air-gapped networks.

TAKE AWAY, what these examples say about Cyber Attack awareness...

Techniques such as utilizing USB devices as delivery mechanisms to enable hostile penetration of targeted “secure” control networks is widely known. Approaches of establishing hostile C2 channels across the gap using techniques such as P2P or sneaker-nets are less well known.

Techniques like these mean that defensive measures limited to reliance on air gaps need to be evaluated skeptically. Other advanced and novel means of hostile penetration, and the means to offer effective layered defense against them, must be considered to achieve true control network and device security and true risk management. These observations point towards integrated consideration of policies, procedures, system design, operational approaches, intrusion detection, anomaly, monitoring and awareness technologies which deliver a capability

to understand own network health, vulnerabilities and mitigation options. Take a proactive and more informed view towards the challenges and opportunities to enhance your security by keeping apprised of hostile techniques, tactics and procedures (TTP) like the two illustrative examples above.

Disruption through swarming

Creating an open call for volunteers in an ad-hoc, extemporaneous way to do something is popularly known as crowd sourcing. It's leaderless or structure-less network of people coming together for a common purpose and then disbanding. Adversaries use this tactic. The Anonymous (a loose knit global hacktivist group) hive is the personification of this but there are others.

In 2008, at the onset of war between Russia and Georgia, a distributed denial of service attack (DDoS) began against government websites. As hostilities began, this was extended to Georgian media websites covering the hostilities. These various DDoS attacks lasted for hours and had a peak of over 800Mbps. A few months later an analysis under the moniker of "Project Grey Goose" was released. This report outlined the coordination ground for these DDoS to a website called stopgeorgia.ru. This was a password-protected forum launched within 24 hours of hostilities. These DoS attacks were interspersed with website defacements posting pro-Russian propaganda.

These DoS activities and defacements were seemingly self-organized or crowd sourced on sites such as stopgeorgia.ru. Many believe the Russian government was in the background of these pro-Russian hacktivists. At the very least, the Russian government appeared to condone the activities as evidenced by their clear restraint in not launch any investigation of the attacks.

Anonymous uses surprisingly similar tools to organize (online forums) - and similar tools to launch attack activity (denial of service attacks). Their tool of choice is called Low Orbit Ion Cannon (LOIC). LOIC is an application designed to launch DDoS attacks. LOIC by itself is uninteresting. It's the forums that are interesting. You'll see a long list of independently organized "operations" or "ops". Each of those operations are public and open to the community to comment on. There are dozens of ops at any given time, most of them become background noise. Others take off and develop a life of their own. The HBGary Saga is a good example of a successful op. But for each successful op there are countless that don't see the light of day. Combine this with the LOIC tool: when you give it to the hands of 10,000 who point it at the same target then you have a distributed denial of service. This is what was used in Operation Payback when Anonymous attacked PayPal and others after they refused to provide services to wikileaks.

This is a noteworthy tactic as indications are that it is employed by a wide range of adversaries. Pro Russian groups used it as a propaganda and disruption tool, and Anonymous continues that tradition.

TAKE AWAY is that swarming is a practice that has been observed, Crowd sourcing and social media techniques are easily available to motivated groups that may seek to use them for distributed denial of service disruption.

Off the shelf tools

There exists an ecosystem of tools available to the adversaries. Some of these are dual use for offensive and defensive purposes. Some of these tools are merely used at research levels, others for active attacks. Fuzzing tools and Security debugging tools such as olly or ida pro - which are development environments. These can pinpoint flaws in software and ultimately lead to exploit code that can be weaponized.

LAMP stands for Linux Apache Mysql and PHP. It is a “vanilla” OS, Webserver, SQL server and a web application language and how those four off the shelf technologies can be combined for rapid web development. LAMP is the model being packaged and sold by malicious underground adversaries in order to exploit people. These are known as exploit kits. Exploit kits use LAMP to set up malicious web pages, and use those pages to attack web browser and client components. The exploit kit also keeps track of the overall success rate. The kits create malicious iframes that will attempt to use a series of several exploits all at once in order to execute a malicious payload on the target machine. These iframes are windows cut into the webpage that allow visitors to view another page on the site or off the site without reloading the entire page. The exploit kit will also track victims by IP address, country, browser, OS-level, etc...

These malicious pages are delivered through vectors such as search engine optimization (SEO) and Phishing attacks.

Contagio dump (a web based collection of the latest malware samples, threats, observations and analyses) is tracking 64 versions of 42 unique exploit kits in the wild. Most of these contain between 10-20 exploits and each kit is sold for between \$1000 to \$2000. These 64 unique exploit kits have a total of over 100 unique exploits! Mostly targeting flash, adobe, quicktime, java, or browser vulnerabilities. Tools other than exploit kits also exist. LOIC is another off the shelf tool to be aware of. Additionally, there are Trojans, such as poison ivy, zeus, TDL, and others, which threat actors can purchase or gain use of through underground or criminal communities.

TAKE AWAY is that exploit kits are ubiquitous and inexpensive for criminal groups to obtain and utilize. Software development quality control and layered defense in depth, combined with own systems awareness are key defensive measures.

Lateral Movements

Adversaries with long-term motives will typically focus in on first gaining access to a target network, then finding target hosts on the network which enable network understanding. This tactic is generically referred to as moving laterally in the compromised network. This is where it can be tough to remove an adversary on your network because the adversary is in several places.

The tactic - and both Google Aurora as well as the RSA breaches saw this tactic used - starts with patient zero. Once patient zero is compromised the adversary begins compromising other workstations or servers with back doors. Adversaries will then use those backdoors and stand up their operations. One workstation may host various attacker tools: another workstation will be for data staging if the aggressor plans on finding and exfiltrating data. Yet another box is simply given a back door and not touched in case the aggressor loses access to the other boxes. Aggressors may continue lateral movements as they seek long-term objectives and escalate privileges on the network.

Lateral movement typically occurs through a technique such as Passing the Hash. To illustrate, if an attacker gains access to a target user workstation and the user happens to be a local administrator, the goal becomes to jump from this springboard workstation to a print server and plant a "back door." This is convenient because the attacker already knows the print server hostname since the user has access to it. What might not be known to the attacker is the target user domain password nor whether his account has access to interactive sessions with the print server. Attackers may rely on the fact that Windows has a core OS service running known as Local Security Authority. This service caches the users and associated password hash data after a user has authenticated to the local system. The adversary can then utilize a tool known as Windows Credential Editor (or metasploit...) and dump password hashes. This is not the plain text password. The password is not needed. Windows Credential Editor can utilize this NTLM hash and start processes as the attacked user. The attacker uses Windows Credential Editor and dumps the cached hashes in LSA. The attacker identifies an account called "service Veritas." That shines out to the attacker because Veritas is a backup software solution. If the backup software is using this service, there is a high likelihood that it is domain admin or nearly equivalent. Windows Credential Editor allows the attacker to use this hash and pass it on to the system to run processes as that user. On the local machine, he can then remotely connect to boxes as that service account. That's how backdoors can be planted. Subsequently, one could come back to the print server and list hashes that are cached on the print server. If the domain equivalent user has recently talked to the print server, that hash can be stolen and used as an attacker enabler for easy internal movement within the target network environment.

TAKE AWAY is that a foundational defensive element of strategy for every organization should be development and maintenance of own asset and own system baseline configuration and operational states, as well as own systems operational awareness. Obtaining and keeping good forensic and log data can be very crucial to effective and sustainable defensive posture. Often a few Indicator of Compromise (IOC's) can be developed around a few key, but important, departures or anomalies from normal operating parameters. These can be used to identify and triage attempts at compromise.

Appendix K: Task Force Goals and Objectives

The goals and objectives of the CATF are:

Goals	Objectives
Review current situation and capabilities	<ol style="list-style-type: none"> 1. Consider the ability of entity system operators and cyber security analysts to detect and respond to a coordinated cyber attack. 2. Consider the extent to which entities may not isolate critical cyber systems from other business or Internet-facing systems, and the extent to which this increases the vulnerability of their systems. 3. Consider opportunities to isolate, prevent further propagation, or otherwise protect cyber systems and bulk power system assets. 4. Consider the capabilities of voice and data communications tools and energy management systems, with a focus on which minimum functional needs system operators must retain and the alternative methods to acquire or maintain this capability even in a reduced state. 5. Consider staffing capacity, challenges, and safety. 6. Assess the adequacy of current CIP cyber security practices under a coordinated cyber attack scenario.
Perform needs assessment	<ol style="list-style-type: none"> 7. Identify the functions needed to support reliable power system operations that would be particularly challenged under a coordinated cyber attack scenario.
Develop alternative solutions	<ol style="list-style-type: none"> 8. Assess the options, benefits, and costs associated with isolating critical cyber systems (i.e. control systems, energy management systems, protections systems, and their networks). Consider complete or virtual (e.g. virtual private network) separation. 9. Propose a range of alternative solutions to enhance operating capabilities, including estimated costs and effort to develop and maintain this capability. Identify the residual

	risks that may be associated with each of these solutions.
Coordinate Solutions	10. Assist in outreach efforts to educate regulators, organizations, and other infrastructures in better understanding the electricity sector's preparations to address these threats.
Recommend Solutions	11. Recommend potential practices or programs for use by NERC or individual entities. Create scalable drill templates that registered entities could utilize to train personnel and enhance current restoration and operating protocols.

Electricity Sector Information Sharing and Analysis Center (ES-ISAC) Update: Enhancing Capability

Action

Information

Background

The mission of the ES-ISAC is to improve the security and reliability of the North American bulk power system (BPS) by facilitating the sharing and analysis of security-related information across the electricity industry and with government. The ES-ISAC develops and disseminates authoritative guidance regarding cyber, physical, and all-hazards threats to BPS reliability. The ES-ISAC depends on the information it receives from entity owners and operators, U.S. and Canadian government sources, and other critical infrastructure sector ISACs.

During 2012, the ES-ISAC is enhancing the capability of its two primary functions; information sharing and information analysis.

Information Sharing

In February 2012, the NERC Board of Trustees approved the ES-ISAC policy statement that separates the operation of the ES-ISAC from compliance activities. It is anticipated that this policy will encourage entities to share information to a greater extent with the ES-ISAC regarding security incidents or vulnerabilities. A new ES-ISAC members-only portal, planned to be available by July 2012, will further encourage sharing by providing a confidential and secure mechanism. Approximately 200 NERC members are currently registered for the portal. Certain NERC staff now have access to the classified portal at the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center. The ES-ISAC's information sharing capability is being enhanced through a number of initiatives, such as:

- Subscribing to Critical Intelligence Reporting services to more closely monitor emerging threats and vulnerabilities affecting industrial control systems, including Supervisory Control and Data Acquisition Systems (SCADA) and Energy Management Systems (EMS).
- Providing the secure communications technologies required to collaborate with the U.S. Computer Emergency Readiness Team (US-CERT) in order to analyze threats and disseminate NERC Advisories promptly to entities.

Information Analysis

ES-ISAC staff is increasing their ability to analyze threats and their potential impact on bulk power system reliability through a number of initiatives such as:

- Subscribing to Looking Glass Cyber Intelligence to monitor real-time cyber threats that potentially affect the industrial control systems of asset owners and operators.
- Developing comprehensive Attack Tree models to help analysts assess the real risks to reliability of new and evolving threats.
- Implementing a comprehensive Analyst Workbench with the tools needed to analyze malicious software of particular interest to bulk power system entities.

External Affairs Update

Janet Sena

Vice President and Director, Policy and External Affairs

May 9, 2012

RELIABILITY | ACCOUNTABILITY



- ERO Activity Support
 - Reliability Risk Management
 - Find, Fix, Track and Report (FFT)
 - Reliability Assessment and Performance Analysis
 - EPA Cumulative Regulations Report
 - EPA RE Meetings
 - FERC Whitepaper Response
- *2012 Special Reliability Assessment: Effects of Geomagnetic Disturbances on the Bulk Power System (GMD) Report*
- Administration Activities
 - Electricity Sub-Sector Coordinating Council (ESCC)
 - Department of Homeland Security (DHS) Cybersecurity Briefing

- Cybersecurity Legislation
 - House Cyber Week
 - DHS Bills
 - Mandatory versus Voluntary Standards
- Nominations

- Media Inquiries
 - Solar Storm Coverage
 - GMD Coverage
 - Southwest Outage
 - Cyber
 - EPA
- ERO Support
 - Report Rollouts
 - Regional Communicators Group

Operating Committee Report

Action

None

Background

This report provides a summary of the key activities of the Operating Committee (OC) and its associated subcommittees in support of the NERC or OC mission and corporate goals. All these activities support the NERC or OC mission and NERC corporate goals. The March 2012 OC meeting minutes are posted at ([OC March 2012 Meeting Minutes Link](#)).

Status of Operating Committee's Major Initiatives for 2012

1. Event Analysis Working Group (EAWG) Work and Lessons Learned
 - a. Links to NERC Top Priority Issues 1: Misoperations of relay protection and control systems and 2: Human errors by field personnel.
 - b. The OC is currently forming an Event Analysis Subcommittee (EAS); which should better enable the OC to support the ERO and industry in rapidly identifying reliability gaps and potential mitigations.
 - c. The new subcommittee expects to present its draft scope to the OC in June 2012 for approval.
 - d. The OC has appointed Sam Holman (Duke) and Hassan Hamdar (FRCC) as Chair and Vice Chair respectively.
2. Geomagnetic Disturbance and Severe Impact Resilience Task Forces (SIRTF)
 - a. Links to NERC Top Priority Issue 7: Preparedness for high impact, low frequency events.
 - b. OC to incorporate some SIRTF recommendations into its 2012-2013 work plan.
3. Human Performance and Field Personnel
 - a. Links to Top Priority Issues 1: Misoperations of relay protection and control systems and 2: Human errors by field personnel.
 - b. The OC revised the COM-002-2 Reliability Standard Audit Worksheets (RSAWs) and is developing a Reliability Guideline: System Operator Communication (the latter of which was requested by the Board of Trustees at their February 2012 meeting).
 - c. OC to discuss the possibility of a Human Performance Subcommittee or Working Group based on the interest expressed by a number of people who attended NERC's Human Performance Seminar.

Actions from the March 2012 OC Meeting

Critical Infrastructure Strategic Initiatives: Coordinated Action Plan

The OC endorsed the Cyber Attack Task Force Final Report and approved the SIRTf Report *Severe Impact Resilience: Considerations and Recommendations*.

Event Analysis Process

The Event Analysis Process (EA Process) became effective on February 12, 2012. The EAWG is developing the scope of the new EAS for the OC's consideration at its June 2012 meeting.

OC Strategic Plan

The OC Executive Committee and its subcommittee leadership met to review the committee's 2012 work plan and to align its existing work plan with NERC's 2012 corporate goals and objectives. This is the first of this type of meeting which is designed to ensure each subcommittee is in alignment with the OC's and the ERO's strategic priorities and can more effectively coordinate each other's tactical initiatives.

Manual Time Error Correction Elimination Field Trial

The OC reviewed the results of its requested investigation of the causes of fast time (i.e., Interconnection operating above 60 Hz), evaluation of the reliability risks of conducting time error corrections, and investigation of other issues around reliability, including compliance risks. The OC approved discontinuing further pursuit of the elimination of manual time error corrections.

OC Subgroup Highlights

The OC now has 13 subgroups, five of which jointly report to the Planning Committee (PC) and the OC.

Joint OC/PC subgroups highlights

1. **Performance Analysis Subcommittee (PAS)** – The OC endorsed the Event Driven Index white paper.

Other Subgroup Highlights

1. **Operating Reliability Subcommittee (ORS)** – The ORS continues to work with the North American Energy Standards Board's Business Practices Subcommittee on the Parallel Flow Visualization project and is addressing the notification process for geomagnetic disturbances.
2. **Resources Subcommittee (RS)** – The OC endorsed the ACE Diversity Interchange white paper and tasked the RS to transition the white paper into a reliability guideline. The RS is also working with the Frequency Response Standard Drafting Team to identify frequency events within each of the Interconnections.

Planning Committee Report

Action

None

Background

Along with annually producing reliability assessments, performance analysis reports and special assessments, the NERC Planning Committee (PC) is actively engaged in a number of areas that are important to maintain the reliability of the bulk power system of North America. At its March 6-7, 2012 meeting in Phoenix, AZ, the PC took action on a number of issues, including the following top-priority items:¹

Support for Technical Justification of Bulk Electric System (BES) Definition Thresholds

The PC will provide technical assistance in support of the Phase 2 efforts of the BES Standard Drafting Team (DBES SDT). The PC is researching the following four items and will provide technical justification to the DBES SDT effort for:

1. A bright-line voltage level or other criteria for the core definition of the BES using interconnection-wide solutions if necessary.
2. Real power thresholds for *Inclusion I2* of the BES definition and assess the need for separate values for single units and aggregated values at a plant.
3. Allowing power flow out of a local network in *Exclusion E3* of the BES definition, and if power flow is allowed, establish the value and duration for same.
4. Reactive power thresholds in *Inclusion I4* of the BES definition.

A written report of the results of the group's analysis and technical justifications will be provided to NERC's Planning and Operating Committees for approval in December 2012. Upon approval, the report will be submitted to the DBES SDT for consideration in development of Phase 2 thresholds.

Creation of Protection System Misoperations Task Force

Nearly all major system events, excluding those caused by severe weather, have had relay or automatic control misoperations contributing to their propagation. The Protection System Misoperations Task Force (PSMTF) will provide analysis and expertise to support NERC in addressing its top priority reliability issues. The PSMTF will analyze relay misoperation data, research root causes, and develop industry recommendations to reduce future relay misoperation occurrences. The key findings and recommendations will serve as technical input for industry actions to mitigate the reliability risks that can result from future protection system misoperations. The Protection System Misoperations Task Force will focus on four areas of excellence:

1. Provide a trend analysis of protection system misoperations data and root cause identification;

¹ The draft minutes are posted at <http://www.nerc.com/filez/pcmin.html>.

2. Form conclusions/recommendations from the analysis to reduce future misoperations from occurring;
3. Provide recommendations to NERC staff (e.g., NERC Alerts, etc.) and industry actions; and
4. Develop industry guidance through technical documents and webinars on trends, conclusions, and recommendations.

The task force will develop a report for approval by the PC that summarizes the trends from misoperation of protection systems, identification of root causes, and recommendations for actions. This report is expected to be presented at the December 2012 PC meeting for review and approval.

Continuing Work on the Performance Analysis Annual Report

The ultimate goal of the Performance Analysis Annual Report is twofold:

1. The report assesses the historical, overall bulk power system reliability picture. By using robust data, the reliability of the system can be explained and documented. Currently, there are no measures, datasets, or reports that explicitly and completely state the historical performance of the system.
2. The report will help identify risk clusters, and prioritize and create actionable results for reliability improvement. Once a risk universe has been found, it can be parsed into component clusters. These significant risk clusters can be selected as priority projects to develop coordinated and multifunctional solutions to relevant problems.

The Performance Analysis Annual Report provides an industry reference for historical bulk power system reliability, analytical insights with a view to action, and enables the discovery and prioritization of specific and actionable risk control steps.

Other key items addressed at the March 2012 meeting were approval of the:

- *Event Driven Index Whitepaper*
- *Severe Impact Resilience Task Force (SIRTF) Report*
- *Reliability Assessment Data Working Group (RADWG) Scope*
- *Model Validation Working Group (MVWG) Scope*
- *System Analysis and Modeling Subcommittee (SAMS) Scope*

Future Meeting Schedule

The PC future meetings are scheduled as follows:

- June 19-20, 2012 – Toronto, Canada
- September 18-19, 2012 – St. Louis, MO
- December 11-12, 2012 – Atlanta, GA

Critical Infrastructure Protection Committee Report

2012 Goals and Objectives – TOP 3

Overview

Reorganize and expand the Critical Infrastructure Protection Committee (CIPC) structure to facilitate and accomplish a greater volume of work and deliverables. This will include establishing new subcommittees in areas such as physical security and cyber security. In addition, will provide an oversight for specific task force and working group efforts, as well as creating new task forces and working groups to address the new initiative requests from the NERC CEO and Board of Trustees.

- **Create and assign a BES Security Metrics Working Group** that will collaborate with the CIPC Executive Committee (EC), CIPC members and NERC staff to develop an ongoing “Annual Security Assessment” report. This working group will reach out to the joint Operating and Planning Committees Event Analysis Working Group to ensure a coordinated effort between the groups. A charter has been drafted into final version for CIPC approval. The working group consists of 15 members (11 Subject Matter Experts (SMEs) and 4 NERC Staff). The group will conduct four webinar meetings. Deliverables are scheduled for CIPC’s approval in December.
- **Create and assign a Personnel Security Clearances Task Force** to deliver recommendations to industry and government for private sector security clearances. This will entail coordination with the Department of Homeland Security to increase the number and levels of U.S. Government Security clearances available to members of the CIPC and other industry SMEs. The charter has been drafted for CIPC’s approval and members from industry and government have been added. Meetings are scheduled to begin work.
- **Completion and approval of one report and two guidelines**
“Cyber Attack Task Force Report” was approved by CIPC at the March 7, 2012 meeting.
“Protecting Sensitive Information Guideline” was approved by CIPC and is out for industry comment.
“Security Guideline for the Electric Sector” was approved by CIPC and is out for industry comment.

CIPC Strategic Plan Status

- The strategic plan and associated work plan were approved by CIPC at the March 7 meeting. Submission to the Board of Trustees for their approval at their May meeting.
- Status of work plan activities for 2012
- *Obstacles to any work plan tasks or efforts:* The biggest challenge in 2012 will be to enlist CIP SME's on the various new subcommittees, task forces, and working groups and ensuring that they are all actively engaged and progressing toward their milestones. Even in the early progress of the BES Security Metrics Working Group and the Personnel Security Clearances Task Force, the volunteers that have stepped forward to lead are already very promising.

**Critical Infrastructure Protection Committee
2012 Strategic Plan**

Action

Approve the CIPC 2012 Strategic Plan.

Background

In November 2011, the CIPC Executive Committee, chaired by CIPC Chair Barry Lawson, began to draft the CIPC Strategic Plan and develop goals to align the committee's activities with the NERC electric reliability organization (ERO) enterprise's strategic plan and top priority reliability issues. The CIPC was presented with the 2012–2016 Strategic Plan draft at the March 2012 meeting for comment. The CIPC approved the 2012 Strategic Plan and recommends it for consideration and approval by the Board of Trustees (BOT).

2012 CIPC Strategic Plan

The 2012 CIPC Strategic Plan serves as the foundation for the alignment of CIPC activities, including coordination with other standing committees, the strategic direction of NERC, and BOT. The strategic plan emphasizes conforming activities with the priorities of the NERC ERO enterprise and regulators, and effectively using CIPC's resources. The strategic plan describes CIPC's mission, vision and guiding principles, and outlines the areas of strategic focus and key activities for the upcoming years, while recognizing potential changes that may be required in the future by calling for an annual review of the strategic plan.

Implementation of the CIPC Strategic Plan and Linkage to NERC's Top Priority Issues

The following table reflects specific activities that the CIPC and its subgroups will be addressing in 2012 and beyond.

Activity No.	CIPC Area	CIPC Activity	Why is the activity required?	Deliverable and Schedule
1	Advisory Panel to Board of Trustees	<p>Provide reports of CIPC activities at the BOT meeting.</p> <p>Chair will serve as an active member of the ESCC contributing expertise on CIP matters.</p> <p>Chair will serve on the Standing Committee Coordination Group (SCCG).</p> <p>Chair will serve as a CIPC point of contact for the ES-ISAC requests; for input and assistance.</p> <p>Coordinate across all NERC committees and working groups to assure the highest degree of collaboration possible.</p>	All are required by CIPC Charter Section 2.1	<p>2012 May BOT meeting.</p> <p>Attended ESCC calls and March 15, 2012 meeting.</p> <p>Attended Jan 4th and April 5th meetings.</p> <p>Continuing.</p> <p>Continuing through SCCG.</p>
2	NERC Industry Alerts	CIPC will continue to support the coordinated action of NERC's technical committees (Operating Committee, Planning Committee, and CIPC) for pending NERC Alerts.	NERC President's Top Priorities and Issues: Goal 8, CIPC Charter Sections 2.2 and 2.4	Established listing of CIPC SMEs from voting members & alternates with all contact information.
3	Cyber and Physical Security Guidelines	<p>Assist in the development and implementation of NERC standards.</p> <p>Identify the need for new or revised critical infrastructure protection standards and initiate standards actions by submitting standards authorization requests.</p> <p>Assist the standards process by providing expert resources in support of the development of critical infrastructure protection standards authorization requests and standards.</p> <p>Assist the standards process by providing a forum for education, sharing of views, and informed debate of</p>	NERC President's Top Priorities Issues: Goal 8 and CIPC Charter Section 2.5	<p>CIPC members & alternates are on SDTs.</p> <p>Established Compliance & Enforcement Input WG.</p> <p>CIPC members & alternates as SMEs on SDTs.</p> <p>Initiated CIPC Workshops for Cyber & Physical Security.</p>

		<p>critical infrastructure protection standards.</p> <p>Review draft critical infrastructure protection standards authorization requests, standards, and provide comments.</p> <p>Facilitate the implementation of critical infrastructure protection standards by developing reference documents and performing other activities.</p> <p>Provide requested support to SDTs upon direction by NERC or the Standards Committee.</p> <p>Contribute to standards work with the Operating and Planning Committees.</p>		<p>CIPC members are engaged and informed at all CIPC meetings of current status for CIPC and industry comment periods.</p> <p>CIPC members and alternates are asked and encouraged to provide comments on all documents for CIPC and Industry comments by NERC Staff.</p> <p>Physical, Cyber, Operating & Policy Subcommittees have been established and charters have been developed.</p> <p>CIPC members and alternates were advised of SME needs and have populated SDTs.</p> <p>CIPC members and CIPC were asked and provided comments on all documents from OC and PC.</p>
4	Compliance and Enforcement Input	<p>CIPC will create a Compliance and Enforcement Input working group.</p> <p>Support the Compliance Application Notice (CAN) initiative at NERC by providing timely topical expertise on matters related to cyber security, physical security, and prioritization of CANs under development.</p> <p>Utilize the CIPC face-to-face meetings to allow discourse on CAN topic areas and encourage registered entity involvement in commenting.</p> <p>Provide fact-based feedback to NERC on the effectiveness of the CAN process.</p> <p>CIPC EC will solicit members to serve in a consultative or advisory role to NERC staff.</p>	NERC President's Top Priorities and Issues: Goal 7	<p>Working Group approved by CIPC, March 2012, assigned to Policy Subcommittee.</p> <p>CIPC provided input to CAN Prioritization Listing (1/19/12), PER-005 RSAW (3/26/12), and CIP-005 Compliance Report (3/15/12).</p> <p>Compliance Dept. has been added as a permanent agenda item going forward.</p> <p>CIPC is informed and asked to actively participate in an open and transparent CANs process. On-going.</p>

5	Bulk Electric System Security Metrics	<p>CIPC will create a Bulk Electric System Security Metrics working group to develop benchmark recommendations for Bulk Electric System Security metrics to include cyber and physical controls.</p> <p>Align security performance metrics with the Standards Committee Reliability Principals.</p> <p>Align the development of integrated security performance metrics with the adequate level of reliability definition.</p> <p>Developing the Security Risk Matrix/Curve.</p> <p>CIPC and NERC Staff will contribute to the development of an “Annual Security Assessment” report based upon work done by the Bulk Electric System Security Metrics working group.</p>	NERC President’s Top Priorities Issues Goal 8 and ERO Strategic Goal 3	<p>BES Security Metrics Group was approved by CIPC on March 7th, solicited and obtained CIPC. Industry volunteers & NERC SMEs, completed charter for work to include deliverables and schedule.</p> <p>On-going.</p> <p>On-going.</p> <p>On-going.</p> <p>On-going.</p>
6	Electric Sector Security Clearances	<p>CIPC will create and assign a Personnel Security Clearance TF to include industry and government members.</p> <p>The TF will examine protocols in place for granting private sector clearances as well as the government’s legal and policy requirements of the industry.</p> <p>The TF will research ongoing needs of industry for access to actionable and information.</p> <p>The TF will report and make recommendations to CIPC and the ESCC on security clearances.</p> <p>The TF will develop a model for industry use to determine which for personnel should seek a security clearance from government.</p>	NERC President’s Top Priorities Issues - Goal 7 and CIPC Charter Section 3	<p>CIPC approved, March 7th, assigned to Policy Subcommittee, Chair and Vice Chair selected, solicited CIPC members, industry SMEs and NERC Staff support. Ongoing.</p> <p>On-going.</p> <p>Presentation to CIPC EC in 3rd Qtr, CIPC presentation and approval September CIPC meeting.</p> <p>On-going.</p>
7	Public-Private Partnership for Information Sharing	<p>CIPC will create an Information Sharing task force to study present protocols existing between industry and government.</p> <p>The task force will detail and document information-</p>	NERC President’s Top Priorities Issues Goal 7 and CIPC Section 3a	CIPC approved, March 7 th , assigned to Operation Security Subcommittee, Chair selected, soliciting CIPC members, industry SMEs and NERC Staff support.

		<p>sharing requirements.</p> <p>Identify and research the existing information sharing structures, methods and requirements, and search for efficiencies and alternatives to improve or recommend changes in protocols.</p> <p>Propose solutions that will build on practices and tools already in place.</p> <p>Develop a process for secure information sharing with other entities and government partners.</p> <p>Develop a method to communicate lessons learned to other entities with the minimum amount of security classification.</p>		
8	<p>Support to Energy Sector Control Systems Working Group</p> <p>“Roadmap to achieve energy delivery systems cyber security.”</p>	<p>CIPC will continue support of “The Roadmap to Achieve Energy Delivery Systems Cyber Security” prepared by the Energy Sector Control Systems Working Group (ESCS WG).</p> <p>The Cyber Attack Task Force’s report will highlight areas of greatest value to enhance detection and response capability, and this may help prioritize initiatives coming out of the Roadmap.</p> <p>CIPC will update the ESCC on progress implementing recommendations found in the roadmap.</p> <p>Encourage and solicit CIPC engagement and assist ESCC as appropriate.</p>	<p>NERC President’s Top Priorities</p> <p>Issues Goal 7 and 8</p>	<p>On-going.</p>
9	<p>Emerging Issues</p> <p>HILF</p>	<p>CIPC will create a HILF Implementation task force to develop recommendations for actions identified in the Coordinated Action Plan.</p> <p>The task force will review the various task force reports and address the appropriate CIPC related recommendations and propose suggested responses to CIPC for action and implementation.</p>	<p>NERC President’s Top Priorities</p> <p>Issues Goal 7 and 8</p>	<p>CIPC approved, March 7th, assigned to the Operating Subcommittee, Chair selected, soliciting CIPC members, industry SMEs and NERC Staff support.</p>
10	<p>Focus on Balanced Approach in Cyber and Physical Security</p>	<p>The CIPC EC will review rosters to ensure that working groups and task forces have a balance of expertise.</p> <p>The CIPC EC and Physical Security and Cyber Security</p>	<p>NERC President’s Top Priorities</p> <p>Issues: Goals 7 and 8</p>	<p>On-going.</p>

		<p>Subcommittees will coordinate and consult to ensure expertise of the CIPC Members.</p> <p>CIPC alternates and observers are engaged with task forces and working groups tasked with projects and deliver recommendations to the CIPC.</p>		<p>CIPC approved, March 7th, assigned to the Cyber and Physical Subcommittee, Chair selected, soliciting CIPC members, industry SMEs and NERC Staff support.</p> <p>On-going.</p>
11	Analysis of CIP Related Incidents in Coordination with OC and PC	<p>CIPC will create two working groups:</p> <ul style="list-style-type: none"> Physical Security Analysis Working Group Cyber Security Analysis Working Group <p>These working groups will research and recommend activities to improve the security of Bulk Electric System facilities.</p> <p>Develop Cyber and Physical expertise liaisons to coordinate expertise and assist the Joint Event Analysis Working Group as requested.</p> <p>Develop a mechanism for evaluating malicious events while maintaining confidentiality of the compromised entity.</p>	NERC President’s Top Priorities Issues: Goals 7 and 8	<p>CIPC approved, March 7th, assigned to Cyber and Physical Subcommittees.</p> <p>On-going.</p>
12	CIP Training and Educational Outreach	<p>CIPC will create two working groups. (Physical Security Training Working Group and Cyber Security Training Working Group).</p> <p>The working groups will identify and prioritize current topics related to the scope of CIPC.</p> <p>These working groups will coordinate with each other and request NERC resources, if necessary, to support their activities for the forums and workshops.</p> <p>The working groups will report their recommendations at the CIPC meetings.</p> <p>The CIPC will schedule Bulk Electric System security training and education at CIPC meetings.</p>	<p>NERC President’s Top Priorities Issues Goal 7, CIPC Charter Section 2.7 and</p> <p>ERO Strategic Goal 2</p>	<p>CIPC approved, March 7th, assigned to Cyber and Physical Subcommittee.</p>

13	<p>Support Board of Trustees/ESCC/Standing Committees Coordination Group (SCCG) <i>CIPC Charter Sections 2.1-2.2</i></p>	<p>Strengthening and supporting the CIPC relationship with the Board of Trustees, ESCC and SCCG through the CIPC chair reporting to the Board of Trustees and participation on ESCC through more detailed reporting and increased involvement.</p> <p>Providing technical and other support as needed on CIP matters.</p>	CIPC Charter Sections 2.1-2.2	On-going.
14	CIPC Member and Industry Observer involvement	<p>Encouraging and engaging CIPC voting member active participation.</p> <p>Encouraging and engaging CIPC alternate members as active participants.</p> <p>Encouraging and engaging industry observers as active participants.</p> <p>CIPC EC will identify potential leadership candidates for subgroups.</p> <p>CIPC subcommittees will review task force and working group rosters to identify gaps in expertise.</p> <p>CIPC subcommittees will review task force and working group deliverables.</p> <p>CIPC EC will encourage, recognize, and reward excellence.</p>	CIPC Charter Section 4.2	On-going.

Personnel Certification Governance Committee Report

Action

Discussion

Background

This report highlights the key activities of the Personnel Certification Governance Committee (PCGC). The PCGC meets four times a year in addition to conducting taskforce meetings as needed. The meeting minutes are posted at <http://www.nerc.com/filez/pcgcmmin.html>.

Discussion

Key Highlights of the attached report to note:

- Downward trend in the number of exams taken
- Upward trend in the number of certifications credentials issued
- Demographics of operators biased towards the 46-55 age bracket

If trustees have questions or need additional information, they may contact Pete Knoetgen, director training and accreditation, at peter.knoetgen@nerc.net

Personnel Certification Governance Committee Report

Accomplishments

The Personnel Certification Governance Committee (PCGC) has posted the updated NERC Board of Trustee accepted System Operator Certification Program manual on the NERC/System Operator Program Site.

The Examination Working Group (EWG) has completed the preparation of the second version of the new certification exams for each of the four credentials.

The PCGC submitted the System Operator Certification program budget to NERC with operating and maintenance expenses including capital improvements and fee structure recommendations.

Future Tasks

The committee does not expect to propose changes to the certification program that would require posting for comments.

The PCGC continues to work on documentation of the credential establishment process, performance metric tracking, and evaluating the certification program and demographic data.

The PCGC is working with NERC database administrator and contractors to finalize plans for upgrades to the System Operator Certification and Continuing Education Database (SOCCED).

Status Report

NERC Certification Examination Pass Rate

From 2009 through 2011, a total of 2,793 exams were administered. The overall pass rate has been stable the past two years. In 2012, new exams were published. The below data for 2012 is through March 31, 2012 with 6 weeks of data for the new exams.

Year	# of Exams Taken	Number of Exams Passed	PASS Percent
2009	1005	652	64.8 %
2010	914	638	69.8 %
2011	874	607	69.5 %
2012*	149	99	59.1%

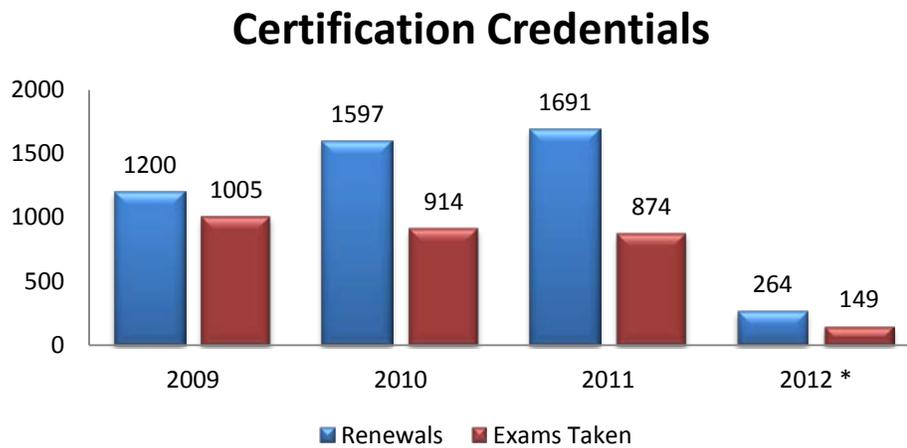
Credential Maintenance

The table below shows the number of credentials maintained using Continuing Education Hours is increasing.

Year	Credentials Renewed
2009	1,200
2010	1,597
2011	1,691
2012*	264

New Certificates versus Credential Maintenance

The graph below shows the number of new certificates issued annually is declining while the number of credentials maintained is increasing.



*Through March 31, 2012

Certified Operator Population

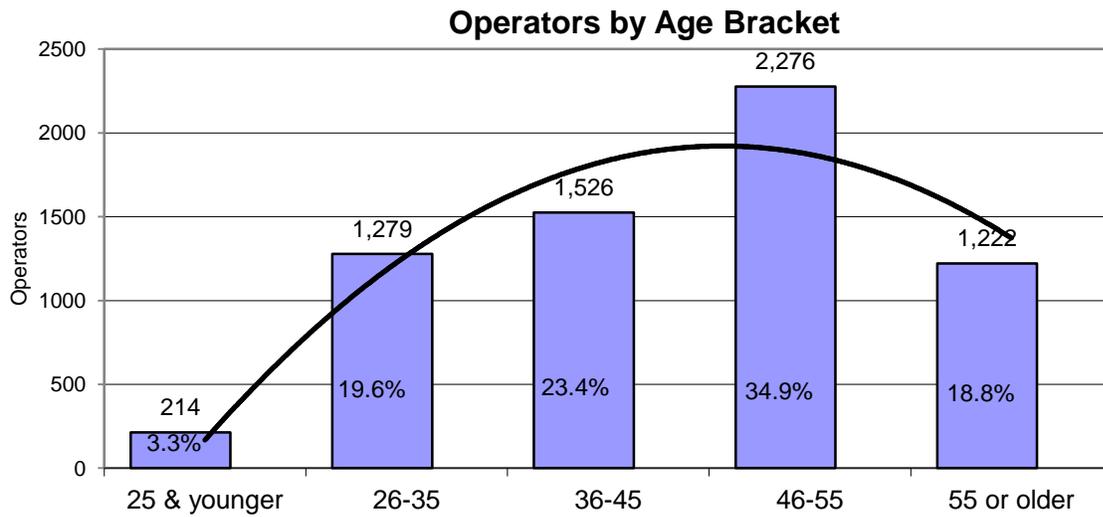
The total number of certified system operators with active credentials is 6,300. The population has appeared to stabilize since the collection of data in 2009.

System Operator Demographics

After three full years of data collection that began in early 2009, all system operators have provided demographic information. This information combines system operators taking their initial exams with those who renewed their credentials through continuing education.

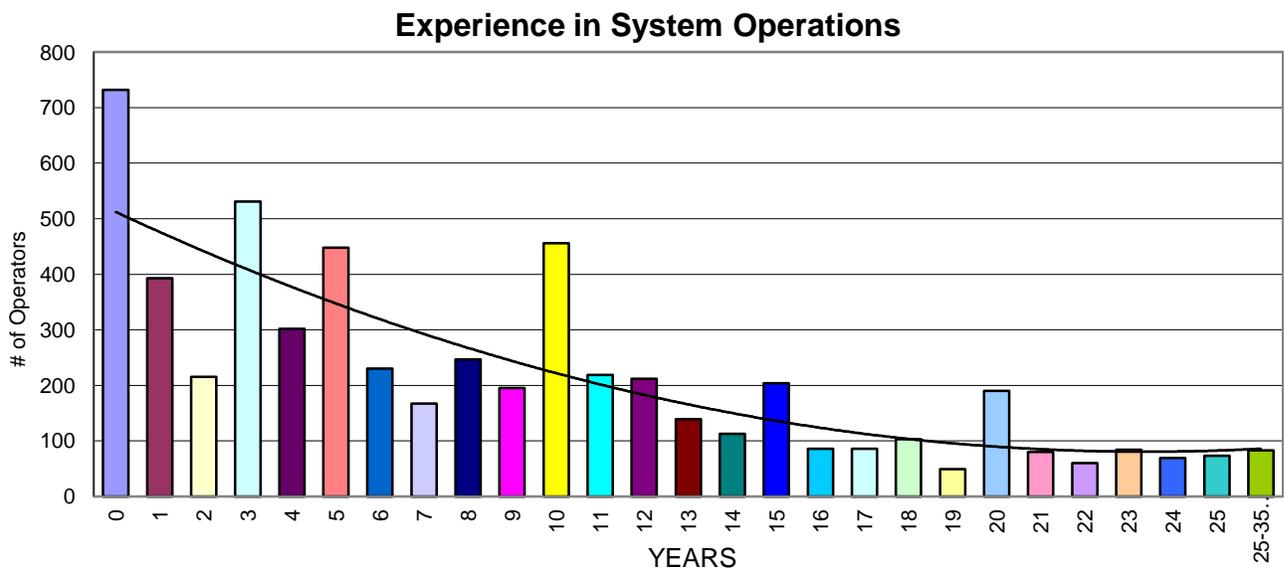
The following figures show current trends that are obtained from the demographics collected, preliminary metrics for average age of system operators and experience in system operations.

Figure 1 - Operator Population Age



The above chart shows 54 percent of system operators are over 45 years old with the largest percentage of system operators in the 46-55 age brackets.

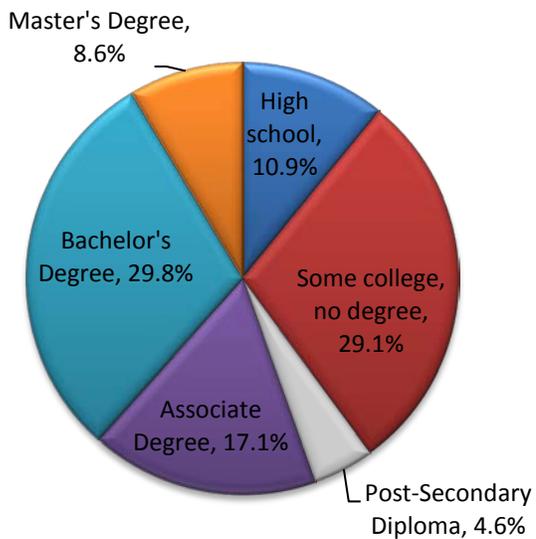
Figure 2 - Experience in System Operations



Approximately 60 percent of the certified system operators have 10 years or less experience in system operations. The average experience remains stable at 11 years.

Additional data indicates 66 percent of the certified system operator population (which includes support personnel) have five years or less experience in their current position with 50 percent of the population having three years or less experience performing their current position.

Figure 3 - Certified System Operators Level of Education



The figure above shows 38 percent of certified system operators have a bachelor degree or higher level of education.

Standards Committee Report

Action

Discussion

Background

This report highlights some of the key activities of the Standards Committee (SC) in support of ERO Enterprise goals. The SC meets monthly and posts its meetings minutes at <http://www.nerc.com/filez/scmin.html>.

Progress in Meeting Major Goals for 2012

The SC identified three major goals for 2012: developing revisions to the standards development process; completing high priority standards associated with topics most critical to bulk power system reliability; and continued refinement of the definition of the term “Bulk Electric System.” The following information highlights progress in accomplishing those goals through the first quarter of 2012.

Goal 1: Revisions to standards process

The SC has initiated action to revise its implementation of the already approved Standard Processes Manual (SPM) and is supporting the efforts of the Standards Process Input Group (SPIG).

- The SC agreed (based on advice from NERC’s legal staff) to adopt the practice, initially on a case-by-case basis, of allowing drafting teams to develop summary responses to comments provided the summary responses address each issue raised by commenters. While stakeholders have become accustomed to more individualized responses, the large volume of comments received by the Cyber Security 706 Drafting Team (approximately 5,000 pages) made individual responses impractical. This practice meets ANSI’s requirements for accreditation, because the drafting team is still obligated to consider every comment.
- The SC sponsored a successful field test of the “Rapid Revision” process in the second half of 2011, demonstrating that making a permanent change to a standard is an efficient alternative to processing an interpretation. During the first quarter of 2012 the SC directed the use of the draft “Rapid Revision” process as an alternative to three additional interpretations.
- The SC has two members (Allen Mosher and John A. Anderson) who are serving on the SPIG, who solicited feedback from other SC members, staff, and various drafting teams aimed at identifying changes to the standard development process that would result in developing a standard in a shorter period of time without adversely impacting either the technical quality of the standards or jeopardizing ANSI’s accreditation of the NERC standards development process.

Goal 2: Complete high priority standards associated with topics most critical to bulk power system reliability

- Protection Systems (PRC-001, PRC-005, PRC-019, PRC-024, PRC-027)
 - PRC-001 – Protection System Coordination – The drafting team completed its second draft of the revised standard (now PRC-001 and PRC-027) and collected informal feedback with a goal of gaining more support for the concepts supporting the new requirements before posting for a formal comment period in the second quarter of 2012.
 - PRC-005 – Protection System Maintenance and Testing – The drafting team posted its next draft of the standard for a parallel successive comment and ballot period through March 28, 2012. If the ballot is successful, and the drafting team makes only minor changes to the standard, the next step will be a recirculation ballot.
 - PRC-019 – Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls – The drafting team working on this standard posted its second draft of the proposed standard for comment/ballot through April 16, 2012.
 - PRC-024 – Generator Performance during Frequency and Voltage Excursions – The drafting team working on this standard posted its third draft of the proposed standard for comment/ballot through March 29, 2012.
- Real-time System Operator Communications (COM-002, COM-003)
 - The drafting team working on COM-002 completed a ballot that achieved an 81 percent approval in February 2012. This version of the standard includes the use of three-part communication when issuing/receiving a Reliability Directive where the term, “Reliability Directive” is defined as: A communication initiated by a Reliability Coordinator, Transmission Operator or Balancing Authority where action by the recipient is necessary to address an Emergency or Adverse Reliability Impact.
 - The drafting team working on COM-003 is working on its next draft of the proposed standard and expects to post its work in the second quarter of 2012. The team is proposing a new term “Operating Communications” defined as: Communication with the intent to change or maintain the state, status, output, or input of an Element or Facility of the Bulk Electric System. This SDT is proposing, among other things, retirement of COM-002 and use of three-part communication for all Operating Communications.
- Cyber Security (CIP-002 through CIP-011, Version 5)
 - The Cyber Security drafting team is working to complete its second draft of the CIP Version 5 standards with plans to post the standards during the second quarter of 2012.

- Frequency Response (BAL-003)
 - The Frequency Response drafting team posted its standard for stakeholder comment and ballot during the last quarter of 2011. The team has identified some significant technical issues associated with the proposed measures. The team is working to redesign its proposed requirements and will not meet the deadline of completing a standard by the May 2012 date.

Goal 3: Continue refinement of the Definition of Bulk Electric System (BES) through Phase 2 as a high priority project

The drafting team working on the definition of BES posted its Standard Authorization Request (SAR) for the proposed scope of work and solicited stakeholder comments during a formal comment period that ended in February 2012. The team narrowed the scope of its work based on stakeholder comments and has submitted a revised SAR for posting during the second quarter of 2012. The BES drafting team has asked the Operating Committee to provide support to this project by conducting studies to determine if there is a technical justification for, among other things, modifying the 100 kV bright line voltage level. The Operating Committee plans to complete these studies by late 2012.

A link to the standards under development web page with links to all of the projects identified above is included here for reference:

http://www.nerc.com/filez/standards/Reliability_Standards_Under_Development.html

If trustees have questions or need additional information, they may contact Allen Mosher, chair of the Standards Committee, at amosher@publicpower.org or Herb Schrayshuen, vice president and director of standards and training, at herb.schrayshuen@nerc.net.

Compliance and Certification Committee Report

Action

Approve Compliance and Certification Committee (CCC) nominations, which were provided as Agenda Item 2b.

Summary

CCC Meeting March 14-15, 2012, Atlanta Georgia

Conducted quarterly CCC meeting (and subcommittee meetings) at NERC headquarters.

Reliability Standards Quality Reviews

Continued assisting the NERC Standards Development staff in performing Reliability Standards quality reviews.

Compliance Application Notices (CANs) Prioritization and Input

Assisted in the prioritization of CANs development activities as well as provided input to the actual language to be included in the CANs.

Risk Management and Internal Controls Subcommittee (RMICS)

Continued working with the RMICS in developing a subcommittee mandate and a 2012 Work Plan. Met with the RMICS members on April 3, 2012 in Washington, D.C.

2011 Stakeholders Perception Survey

Continued reviewing and analyzing the survey results in order to provide the Board of Trustees (BOT) with a list of areas where the CCC believes the BOT should focus on addressing stakeholder concerns. This list is provided by separate memo.

2012 Stakeholders Perception Survey

Continued working with TalentQuest in developing the criteria for the 2012 survey.

Rules of Procedure (ROP)

Continued working with NERC staff with regard to recommended changes in Section 500 and Appendix 5A (Organization Registration and Certification).

Entity Risk Assessment

Continued working with NERC staff in developing a template to be used by NERC, Regional Entities and registered entities in determining a risk identity for each registered entity related to the Compliance Enforcement Program.

Trade Association Update

Participated in the Trades Association update meeting in Washington, D.C. on April 4, 2012.

Standing Committee Chair Group

Participated in the Standing Committee Chair Group meeting in Washington, D.C. on April 5, 2012.

Electricity Sub-sector Coordinating Council Report

Action

None

Background

This report summarizes key activities of the Electricity Sub-sector Coordinating Council (ESCC) in support of NERC's mission and corporate goals related to critical infrastructure. The ESCC is chaired by NERC's CEO and includes a NERC Board of Trustees member, five CEO-level executives appointed by the Member Representatives Committee (MRC), the chair of the NERC Critical Infrastructure Protection Committee (CIPC), and NERC's Director, Critical Infrastructure Protection. The ESCC fosters and facilitates the development of policy-related initiatives to improve the reliability and resilience of the electricity sector, including physical and cyber security. ESCC open meeting minutes are posted at: <http://www.nerc.com/filez/esccl.html>.

ESCC Member Term Renewal

As provided in the ESCC's Charter¹, CEO-level members of the ESCC are approaching the end of their two-year terms and the MRC is currently developing a slate of candidates. Several current CEO members have expressed an interest in continuing to serve on the ESCC to provide continuity.

NERC Board of Trustees member Mr. Paul Barber, recently replaced Ms. Janice Case who had served on the ESCC for several years.

Recent ESCC Activities

Since the previous NERC Board of Trustees report, the ESCC held:

- A closed all-day in-person meeting with senior government officials in Washington, D.C. on March 15, 2012
- An open conference call on March 15, 2012

Involvement in Government Partnership Initiatives

During their March 15, 2012 meeting, the ESCC discussed critical infrastructure initiatives with senior officials at the Assistant Secretary level from the U.S. Department of Energy, Department of Homeland Security, Department of Defense, and National Security staff from The White House.

- The U.S. government has proposed establishing an Energy Sector Public Private Partnership under the Critical Infrastructure Advisory Council's partnership framework to review and address risks associated with energy supplies to critical military facilities.

¹ Ref. ESCC Charter: http://www.nerc.com/docs/esccl/ESCC_Charter_BOT_approved_20100512.pdf

- NERC and the industry are supporting the government's Electricity Sector Cybersecurity Risk Management Maturity initiative to develop a model intended to measure an entity's cybersecurity risk management capabilities. Elements of NERC's Cybersecurity Risk Preparedness Assessment are being adopted as part of this model.
- The DOE/NIST/NERC Cybersecurity Risk Management Process Guideline is expected to be released in May 2012.

Government officials expressed interest in a number of critical infrastructure matters and the ESCC offered to support exploring these in further detail.

- Assess the extent to which electricity reliability may be affected by the loss of global positioning system (GPS) signals used for time synchronization.
- Consider the extent to which supply chains can affect the ability of the industry to respond to catastrophic events.
- Consider conducting a tabletop exercise scenario for a catastrophic emergency event lasting weeks or months to better understand critical interdependencies and the policy-level issues and decisions that would be required.

NERC CIP Updates

The ESCC discussed a number of security-related matters:

- ES-ISAC update, including the new ES-ISAC Policy Statement and web portal enhancement project
- Discussed the Standards Process Input Group
- Endorsed the NERC Critical Infrastructure Protection Committee's Strategic Work Plan
- External affairs update, including pending legislation
- 2011 NERC GridEx Security Exercise Lessons-Learned

Monitoring Progress to Implement the ESCC's Strategic Roadmap

During the past year, the ESCC has monitored the progress and issues associated with the task forces as they implement the *Coordinated Action Plan* to address high-impact, low-frequency risks. The task forces have completed their reports and the Cyber Attack Task Force and Severe Impact Resilience Task Force intend to seek Board of Trustees endorsement for their reports during the May 9, 2012 meeting (ref. table below). All four task force reports highlight recommendations for further study and the ESCC anticipates continuing to provide guidance and support to the Technical Committees.

Task Force or Initiative	Report to be Approved by	Request Comments on Draft	Receive Comments on Draft	ESCC Review	Technical Committees Approve Final	MRC and Board of Trustees Review
Geomagnetic Disturbance	OC and PC	Dec 2, 2011	Jan 6, 2012	Mid-Feb 2012	Feb 1, 2012	Feb 22, 2012
Spare Equipment Database	PC (with OC and CIPC endorsement)	Jun 1, 2011	Jun 29, 2011	Oct 3, 2011	Sep 14, 2011	Nov 3, 2011
Cyber Attack	CIPC (with OC endorsement)	Oct 15, 2011	Feb 8, 2012	Mar 5, 2012	Mar 8, 2012	May 9, 2012
Severe Impact Resilience	OC (with PC endorsement)	Dec 13-15, 2011	Jan 4, 2012	Mar 5, 2012	Mar 7, 2012	May 9, 2012
NERC Crisis Plan	NERC CEO	-	-	Aug 16, 2011	Not Required	Not Required

Shading Indicates Complete

Future ESCC Meetings

Tuesday	July 17, 2012	2:00– 4:00 pm	CLOSED conference call
Thursday	September 27, 2012	8:00 am – 2:00 pm 2:00– 3:00 pm	CLOSED All day in-person meeting, Washington, D.C. OPEN conference call
Tuesday	November 27, 2012	2:00– 4:00 pm	CLOSED conference call



STACY DOCHODA – SPP ED SCHWERDT – NPCC SCOTT HENRY – SERC LANE LANFORD – TRE
DAN SKAAR – MRO TIM GALLAGHER – RFC LINDA CAMPBELL – FRCC MARK MAHER – WECC

Date: April 18, 2012

Memo to: NERC Board of Trustees

From: Tim Gallagher, REMG Chair

Subject: Regional Entity Report for the May Board Meeting

Dear Chairman Anderson:

ERO NERC - Regional Entity Work Groups

All of the Regional Entities take seriously our need to be as consistent as possible in discharging our delegated responsibilities. A key activity toward meeting this objective is our constant collaboration and interaction with each other and NERC. Below are summaries of recent activities of some of the key multi-Regional groups.

Subgroup: ERO-Compliance and Enforcement Management Group (ECEMG)

The ECEMG's purpose is to provide operational and day-to-day policy guidance in the execution of the Regional Entity delegation agreements and the NERC Rules of Procedure, specifically as it pertains to executing the Compliance Monitoring and Enforcement Program (CMEP). The primary initiative of ECEMG is to obtain consistency and uniformity where appropriate, across the ERO enterprise (NERC and the Regional Entities), while ensuring efficient and effective use of resources in executing the statutory responsibilities of the ERO.

Status of current high priority work items:

1. Annual Work Plan: The ERO Compliance and Enforcement Management Group developed a work plan based on the ERO Enterprise Strategic Plan that was approved in Feb 2012. The plan focuses on the cross cutting issues and synchronizes the sub workgroup efforts.
2. Compliance Enforcement Authority (CEA) Staff Training: Consistent, standardized, effective training for compliance staff continues to be a priority effort. NERC and the Regions are improving training for CEA staff. The first of two CEA staff training workshops was conducted in February and the second will be conducted in September. Additionally the ERO will conduct the first ever industry workshop for registered entities on auditor training to facilitate better preparation and understanding of the audit process in February after the CEA staff training. Another session of training for the industry will accompany the September CEA staff training.
3. Risk Based Reliability Monitoring: The ECEMG spent a significant amount of time discussing and identifying the various aspects of this initiative. Several regions are already conducting entity risk assessments and working with entities as part of pilot programs.

The NERC Compliance and Certification Committee (CCC) established a workgroup to gather industry input and perspective on a risk based assessment process and significant progress has been made. ERO focus groups by registered function began in mid-April to gather the various attributes of a sound risk assessment approach to monitoring with a focus on reliability metrics. Industry participation was exceptional and the candid conversation and suggestions will be utilized. These two efforts will be combined; the CCC work group and the industry focus groups will be melded together to develop a draft entity assessment template that will be posted for industry comment by midsummer.

4. FFT Future Phase Development: The group has been working with NERC legal on the FFT compliance filing and report and further refining the various aspects of the next phase of the FFT process and how auditors will be involved in this effort. There are many facets of this effort involving various working group participation, along with NERC staff.

Subgroup: ERO-Reliability Assessments and Performance Analysis Group (ERO-RAPA)

1. SPS/RAS definition update – ERO RAPA initiated an effort to align how the regions evaluate special protection systems (SPS's) and remedial action schemes (RAS's). Surveys of the regions indicated major differences in existing procedures. ERO-RAPA solicited assistance from the NERC Planning Committee (PC) via the system protection and control subcommittee (SPCS) and the system analysis and modeling subcommittee (SAMS) to develop guidelines for addressing SPS/RAS consistently across NERC. A white paper is due to the NERC PC for review in June 2012. This will be leveraged and used in phase 2 of the new PRC-004 standard, addressing SPS's.
2. Protection System Misoperations Update – Nearly a year of misoperations data has been collected under the NERC wide misoperations template. While data and analysis processes are still being refined, the data appears to be consistent and of high quality and is available on the NERC website for review. Some focus areas include improving training on specification and setting of digital relays. A follow-up webinar was well attended by the industry. The ERO-RAPA has requested (via the NERC PC) that the SPCS provide ongoing technical support to the misoperations template, incorporating industry feedback. ERO-RAPA is also providing interfacing between the SPCS and the SDT to minimize differences between the current template and the new PRC-004 standard. A misoperations task force was proposed and approved by the NERC PC. This TF will focus on the data collected to-date and make recommendations to the industry to reduce misoperations.

With this first year misoperations dataset, cross-mapping analyses have indicated that out of 133 three-or-more transmission AC circuit outage events reported, 50% of were initiated by protection system misoperations between 2008 and 2011,¹ validating that misoperations continue to be an important reliability issue.

An effort is also underway to automate the data collection process. A web-based tool is expected to be available in June 2012. This will improve accuracy of data reconciliation between misoperations and transmission/generation outages, and significantly reduce ERO-RAPA staff's time spent on manual reconciliation.

3. UVLS Survey – ERO RAPA has collected information from the regions to investigate similarities/differences in undervoltage load shedding (UVLS) procedures. A report will be

¹ http://www.nerc.com/docs/pc/rmwg/pas/2012_sor_draft/TADS%20Analysis%20Section.docx

presented at the April ERO-RAPA meeting. The initial survey of UVLS data suggests that there are some differences in what is being submitted to the Regions by Registered Entities and also which schemes are considered applicable to the NERC Standards associated with UVLS. RAPA will strive to improve consistency across the Regions in this area as well.

4. 2012 State of Reliability report – This year ERO-RAPA was able to complete the 2011 annual quality review of the Transmission Availability Data System (TADS) one week ahead of schedule. This outstanding effort significantly contributes to ERO’s ability to deliver the 2012 *State of Reliability* report in the second quarter of 2012.
5. Generating Availability Data System (GADS) – ERO-RAPA is leading the first ERO mandatory data collection of conventional generator performance data starting the first quarter of 2012. A web-based tool will be launched on April 24, 2012 for Generator Owners (GOs) to enter generator outages each quarter.
6. Spare Equipment Database (SED) – As a part of ESCC’s critical infrastructure strategic plan, a web-based Spare Equipment Database (SED) tool is expected to be released for GOs and TOs to use on May 22, 2012.
7. Risk Clusters – ERO-RAPA is working with NERC technical committees and their subgroups to continue identifying top initiating events that impact reliability, and aims to build a probabilistic model that statistically links reliability causes and effects. The results can be used as technical bases to prioritize and improve standards development and compliance monitoring.
8. Next Challenges – Based on 2011 post summer assessment, one of major challenges is integration of wind generation during peak hours. ERO-RAPA will be working with stakeholders to develop options, including how demand response could be deployed to improve flexibility and reliability.

Subgroup: ERO - CIP Compliance Working Group (CCWG)

1. The CCWG supported the drafting of the soon to be published Compliance Analysis Report (CAR) on CIP Standard CIP-005-3 and has worked with NERC to develop a revised CAN-0024 (Use of Data Diodes) to address misunderstandings related to compliance requirements.
2. The CCWG also extensively discussed and reached concurrence regarding certain issues associated with CIP-002-4.

Subgroup: ERO - Enforcement Sanction Mitigation Working Group (ESMWG)

1. Currently, the ESMWG is focusing on reliability risk assessments, FFT processing, TFEs, dismissals, and CIP NOP processing. The ESMWG, as always, continues to focus on inter-regional collaboration pertaining to Enforcement and Mitigation topics.

Subgroup: ERO - Compliance Monitoring Process Working Group (CMPWG)

The Compliance Monitoring Process Working Group (CMPWG) has been working to improve the consistency of regional monitoring programs by working on the projects identified below and continual sharing of experiences in the performance of monitoring of the Registered Entities. The following are recent activities in which the CMPWG is involved:

Project	Progress
Review of Sampling Methodology and Samples developed for requirements	Regions have met to discuss their approach. Regional approaches are being gathered for comparison and further discussion, on schedule.
Development of Audit Approaches of 693 Standards	RSAW WG has met with Craig Struck and received direction on how and what to proceed on going forward. Regions are developing audit approaches for review. Work Progressing
Sharing of Audit Process Tools among the Regions	Ongoing, this is being discussed during each call and meeting. Latest tools introduced are MK Insight software package for managing audit and spot checks.
Development of Auditors Workbook	On hold pending changes to RSAWs and other training documents.
Update and development of QRSAWs for 2012	Completed in 2011, RSAW WG will prepare for 2013 AML and work to have them completed for 2013 audits.
Supporting ERO Auditor Workshops	Completed support of NERC Spring Workshop, will work to support Fall Workshop as agenda is developed
Meet with other working groups	Met with CCWG in January and have scheduled another meeting in September. Plans are underway to meet with CRWG in January, 2013.
Provide 10 significant WG activities, tools, or methods that are believed to either align consistent practices for greater implementation across all Regions	Task ready to be presented on May 7 th deadline.
Develop 693 Auditor Team Composition and Training Document	Document has been developed and commented upon by the regions. Document is being finalized for submittal.
Provide review and comments to proposed enhancements of existing NERC Audit tools (Audit Report Template)	Draft Version 2 revision to Compliance Process Directive 2010-CAG-001 Regional Entity Compliance Audit Report Processing.

Subgroup: ERO - Compliance Information Management Group (CIMG)

1. The Compliance Information Management Group (CIMG) and Certification and Registration Working Group (CRWG) have identified the need to accommodate the transfer of open enforcement actions from one entity (deregistered entity) to another entity within the Regional systems. Both working groups are working to revise the NERC Bulletin #2011-005 on Transfer of Assets. Once approved, the Regional Systems will be updated to allow for any newly identified business rules. The CIMG and CRWG are also working to document the expectations for Regions to collect and submit registration change information to NERC for analysis.
2. The CIMG is working with NERC to improve the two-way data transfer between NERC and the Regions, including real-time status of violations, Standards data, and eliminating the manual submittal of data. The CIMG is starting to document additional data fields the Regions would like to receive from NERC, additional fields NERC requires from the Regions, and next steps to securely transfer files from the Regions to NERC. New business rules have also been identified and implemented to improve the data integrity at NERC, including the ability for Regions to update the Standard version and requirement for a violation and successfully transmit the change to NERC. A proposal for NERC to update its Standards database to add an indicator for requirements or sub-requirements that will not have a VRF assigned, because it is explanatory text only, has been drafted and is currently under review.

Subgroup: ERO - Training and Education Group (TEG)

1. In 2012, the ERO Training and Education Group (TEG) is focused on coordination of training projects and priorities for the ERO and stakeholders, and consistent with the charter, is providing a forum for communication and information exchange among NERC staff and the Regional Entity training representatives. Recent discussions included the 2013 budget planning assumptions and opportunities for coordinating training materials and expenses among NERC and Regional Entities.
2. The TEG is focused on two primary training needs for 2012, those being auditor training and development of training on reliability standards for both the ERO staff and industry entities. Auditor training focus includes updating existing auditor and audit team leader training content and delivery, including training for the implementation of the Compliance Enforcement Initiative Phases I and II. In addition, the TEG is providing recommendations for the ERO auditor workshop agendas conducted twice each year. The second priority is developing the methods and training materials for selected reliability standards application guidance for ERO staff and auditors. This guidance and training material would also be shared with the industry in an efficient manner. The TEG will continue to collaborate and provide regional entity input for the training development process.

Subgroup: ERO - Legal Group (EROLG)

The EROLG's purpose is to provide a forum for discussing legal issues involving NERC and Regional Entity activities, especially focusing on the internal and corporate issues germane to the functioning of the ERO. The group meets monthly via telephone and quarterly via face-to-face meetings. The following are recent activities in which the EROLG is involved:

- Development of a standard Conflict of Interest policy and Confidentiality Agreement for use at NERC and the Regional Entities;
- Ongoing development and retention of a pool of potential Hearing Officer candidates;
- Update and development of Regional Entity training programs;
- Development of a pro forma confidentiality agreement for NERC and all Regions;

- Development of an internal review standard and process to create better structure and organization for future proposed revisions to the Rules of Procedure or its Appendices; and
- Ongoing review of implications of relevant Commission Orders.

Subgroup: ERO - Certification and Registration Working Group (CRWG)

1. CRWG is in the process of revision and approval of the Certification Process Documents - 29 Templates created; 30 Finalized; 9 are in process of being reviewed- estimated completion April 26th, 2012. After final approval, these documents will be posted on NERC website for all regional entities and registered entities to view and use for their upcoming functional certification process.
2. CRWG has finalized and approved the new formatted registration letters, which will be sent by NERC to new, revised, and deactivated registered entities. CRWG is working on a single registration form for all regions (20% complete); estimated completion June 30, 2012. CRWG is also working on the development of a training program on Registration and Certification processes for all CRWG members and other working groups as needed.

Subgroup: ERO - Regional Standards Group (RSG)

RSG Meetings

1. The Regional Standards Group (RSG) meets on a monthly basis and has held 3 meetings this year in-person or by phone. The regions have worked to perform quality reviews, post regional standards to the NERC website, and file regional standards and variances with FERC. In addition, they have worked on a whitepaper that helps define the differences between regional standards and regional variances. They also worked together to provide input to the standards section of the Business Plan and Budget Common Assumptions for 2013.

Status of Regional UFLS standards

2. On November 4, 2010, the NERC Board of Trustees adopted PRC-006-1 Automatic Underfrequency Load Shedding and directed NERC staff to file the standard with FERC. Included in PRC-006-1 are Interconnection-wide variances for Quebec and WECC. Concurrent with the development of PRC-006-1, several regions were developing regional underfrequency load shedding standards based on historical documents and practices. Two of those regions, SERC and NPCC, subsequently submitted those regional standards for adoption by the NERC

Board of Trustees. SPP has developed its regional standard with stakeholder consensus and is expecting to present the standard at an upcoming Regional Entity Trustees meeting for action. MRO and TRE have evaluated the continent-wide standard and have determined that it provides sufficient reliability coverage in their respective regions. FRCC is currently performing a comparison between the NERC Board approved continent-wide standard and the FRCC Underfrequency Program to determine if there are any reliability gaps that would require further action in the form of a Regional Reliability Standard or a regional variance to the continent-wide standard. Finally, RFC has suspended the current RFC UFLS standard drafting efforts indefinitely until such time the associated NERC standard (PRC-006-1) is enforced and effective. A report is being prepared for the May BOT meeting.

Status of Efforts to Address Version 0 (Fill-In-The-Blank) Standards

3. The RSG issued a report in October of 2006 establishing a systematic methodology for resolving the potential issues surrounding the existing NERC Reliability Standards that contain "fill-in-the-blank" characteristics. The Report identified 31 continent-wide standards that needed to be addressed and established a work plan to meet the needs identified. Of the 31 fill-in-the-blank standards identified in that 2006 report, revisions to ten standards have been completed; seven are scheduled to be completed in 2012, two in 2014, one in 2015, nine in 2016, and the last two in 2017. A draft report was circulated to the EMG members.

Status of Regional Standards Programs

4. Anthony Jablonski (RFC) is working with the regions to develop the content of a report on the status of regional standards programs in each of the eight regions. The report will be presented at the May BOT meeting.

Subgroup – ERO – Information Technology Steering Group (ITSG)

1. CRATS –webCDMS+ is under development by OATI to primarily develop discrepancy reports for the 5 CDMS regions (MRO, RFC, SPP, TRE and WECC) and a simple export of targeted data for Board reports. All activities are on time and targeted for production in early May. Parallel work is being done with all 8 regions to identify discrepancies and reconcile issues and on revisiting and drafting new business rules. Near term discussions will be held on document synchronization.
2. Events Analysis – ERO Project team identified. First task will be to jointly develop project scope.
3. ERO Project Prioritization – Each region was requested to rank each project within the ERO project list to determine project priorities beyond the existing projects (CRATS, EA, BES Exception and Reliability Assessments). The Project Management Office (PMO) would then take the average of the rankings to recommend priorities beyond what is already defined. The responses were due by April 18.



Mission

The Forum's mission is to **promote excellence** in the reliable operation of the electric transmission system.

Vision

The Forum envisions **continuously improving** the **reliability** of the electric transmission system.

Approach

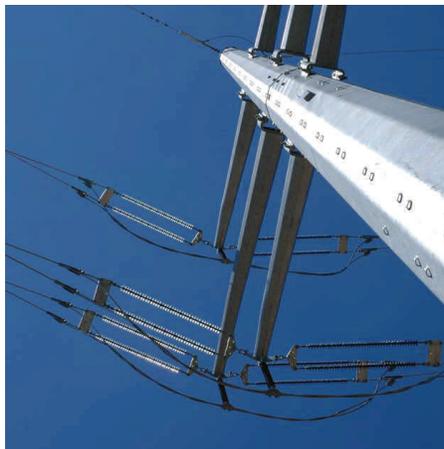
The Forum members advance industry performance by developing and sharing best practices; providing candid, constructive feedback; holding each other accountable, and ensuring the focus and commitment of our members' senior leadership.

The Forum leverages technology for speed and efficiency, and teams of subject matter experts (SMEs) can be assembled quickly to respond to member needs and issues.

SMEs interact through a private Web portal, Internet meetings, online surveys and conference calls. Periodic face-to-face meetings build working relationships and allow knowledge transfer on key reliability issues. Onsite peer reviews, conducted by teams of up to 25 reliability professionals, offer direct, confidential feedback and constructive opinions.

Programs

Our interdependent program areas—practices, information sharing, metrics and peer reviews—are focused on improving reliability among our many diverse members.



Organizations (72)

- Investor-owned: 43
- State/Municipal: 8
- Cooperative: 10
- Federal/Provincial: 6
- ISO/RTO: 5

Percent of total demand. Represents over 90% of the net peak demand in the U.S. and Canada

Transmission. Approximately 370,000 miles of transmission (about 80% of the transmission circuit miles at 100 kV and above in the U.S. and Canada)

Membership Eligibility

Any organization that owns, operates, or controls at least 50 circuit miles of integrated (network) transmission facilities at 100 kV or above, operates a "24/7" transmission control center with NERC-certified transmission or reliability operators, or has an open access transmission tariff or equivalent on file with a regulatory authority, may join the Forum.

Experts (2200+)

Our community of subject matter experts provides broad experience in a range of topics:

- System protection
- Operations
- Maintenance
- Training
- Physical and cyber security
- Vegetation management
- Public relations
- Human performance
- Metrics

Practices

The Forum's groups of subject matter experts hold Web meetings each month and write Forum practices.

- Compliance
- Facility Ratings
- Human Performance
- Line and Substation Maintenance
- Modeling
- Operator Tools
- Operator Training
- Security
- System Protection
- Vegetation Management

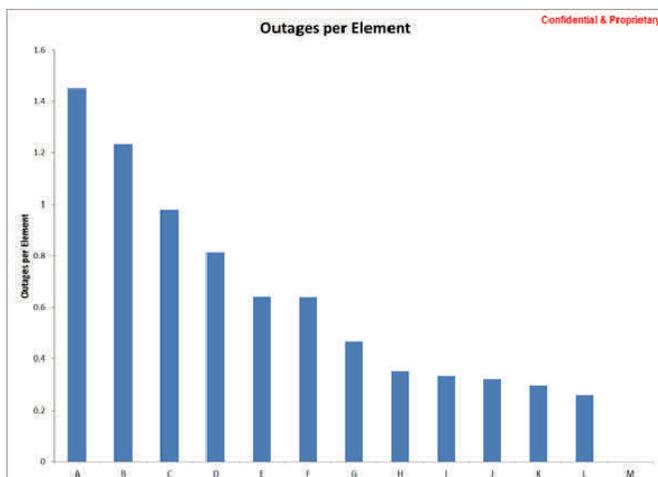
Current topics

- Physical and cyber security
- Personnel training and implementation of PER-005
- Vegetation management community education
- Modeling
- Compliance management
- System protection misoperations

Metrics

The Forum collects transmission equipment performance information, such as TADS data. Improving equipment performance directly contributes to improving reliability. The metrics program:

- Allows Forum members to confidentially view other's data
- Provides tools to facilitate peer benchmarking
- Will expand breadth and depth of data collection in 2012

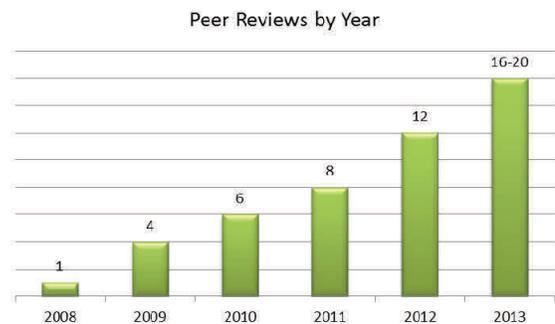


Peer Reviews

Forum peer reviews help our members "raise the bar" for their own operations from good to great.

Review teams that comprise subject matter experts in each practice area spend one week at the "host" peer site. The teams' final reports include noteworthy practices that are shared with the other Forum members, and recommendations for the host to implement.

The program will ramp up through 2014 to a schedule in which members will be reviewed approximately every four years.



Information Sharing

Forum members readily share information for "lessons learned" and assistance:

- System event analysis
- Equipment event reports and alerts
- Vegetation contacts
- Surveys on topical subjects
- Case studies
- Members' practices and procedures
- Audit experiences and lessons
- Compliance violations (feedback to Forum practices)

Recent surveys

- Switching practices
- Operating limits
- SCADA systems
- Logging procedures
- Security
- Facility ratings

Overarching Themes *(Make a positive reliability impact, continuously improve)*

- Measure progress; aggressively pursue continuous improvement, prioritized on a reliability-risk basis
- Promote candid, constructive peer feedback and accountability as membership-wide norms
- Share information effectively and efficiently – get the right information to the right people for optimum results
- Formalize and strengthen processes in all program areas; ensure effective integration
- Continuously add value

Practices *(Clarify reliability linkage, identify and export superior practices)*

- Focus practices on the highest priority reliability topics
- Formalize reliability excellence principles
- Define and disseminate superior practices

Peer Reviews *(Increase formality, focus, and frequency)*

- Conduct rigorous advanced planning, including team selection and associated training
- Systematically communicate key themes to members; increase accountability regarding follow-up
- Incorporate host-member advance self-evaluation as peer review input
- Hone focus, customize scope as warranted to add value

Metrics and Information Sharing *(Measure what matters, set high expectations, share key information efficiently)*

- Define relevant reliability metrics with specific improvement goals
- Foster timely dissemination of lessons learned; facilitate effective member response
- Identify and proactively address adverse trends and precursors to more consequential events
- Refine member benchmarking efforts to increase effectiveness and reduce redundancy

External Interfaces *(Leverage collective wisdom towards reliability improvement)*

- Proactively and routinely interface with FERC, NERC, and others on key reliability issues
- Clarify roles and strengthen working relationships with other industry reliability organizations
- Benchmark relevant organizations from other industries; incorporate findings

New Program Areas and Activities *(Innovate while adhering to the mission and vision)*

- Member assistance - provide targeted assistance upon member request to improve in important areas: human performance (error reduction), internal compliance programs, etc.
- Reliability Initiatives - assume leadership to address selected key reliability challenges
- Enhance event analyses and sharing of lessons learned
 - * Develop cause-determination templates and training to promote quality and consistency
 - * Assume leadership for cause analysis and lessons learned generation for selected events
- Provide for consolidated member training on key reliability topics

MEMORANDUM

To: NERC Board of Trustees

From: Mark Bennett
Chair, North American Generator Forum

Date: May 3, 2012

Subject: North American Generator Forum Report
(May 9, 2012 Board Meeting)

The North American Generator Forum (NAGF or Forum) appreciates the opportunity to provide this activity update to the NERC Board of Trustees (Board). In recent months, much of the Forum's Steering Committee's attention has been focused on developing a dues proposal for member approval and the related effort to obtain Not-for-Profit status. We also are beginning the planning effort for the NAGF's second annual meeting, which we expect to conduct this coming October. We have invited FERC Commissioner John Norris to be our keynote speaker.

As noted below, the NAGF continues to build upon its positive working relationships with the Regional Entities, and our members engage in ongoing dialogue on key reliability and compliance related issues through our Yahoo e:mail platform. A list of these and other specific developments and activities is provided below.

- Expect to finalize and circulate a formal dues proposal for NAGF member review next week. We intend to conduct a webinar to follow up on initial positive discussion during our first annual meeting last October, than conduct an electronic vote on the proposal. If approved (the concept has receive substantial support thus far) a law firm we've already contacted will perform legal work necessary for the NAGF to obtain Not-for-Profit status.
- Will conduct NAGF member vote to obtain approval to expand the Steering Committee from ten to fourteen in order to accommodate six companies that have expressed an interest in joining the Committee (PSEG, PPL, North American Energy Services Company, Duke Energy, EON and MEAGPOWER). These new Committee members will be welcome additions and provide much needed support for the Forum's continued growth and development.
- Conducted a webinar on March 27 to discuss NERC's Find, Fix, Track and Report program and FERC's March 15th Order approving it. Rebecca Michael provided an overview of the Order, and Bob Wargo, Stanley Kopman, Ken Keels and Taud Olsen shared the Regional experiences and perspectives. Over 100 NAGF members participated.

- We are planning future webinars to address: CIP Version 4 and Version 5; the ERCOT experience and related winter preparedness and weatherization issues; status of the generator/TOP issue; and cyber security cost recovery for generators.
- On March 29, at their invitation, NAGF Chair Mark Bennett met with the Generation Council of the Canadian Electricity Association in Ottawa to discuss the progress being made by the NAGF and our work with NERC and the Regions.
- As we have in the past, on May 8 the Forum will conduct a members meeting in conjunction with the NPCC Spring Compliance Workshop being held in Cooperstown, N.Y. from May 8 to June 1. We have invited Stanley Kopman and other NPCC staff to participate, and are also assembling a panel of leading consultants to discuss current issues and provide technical insights.
- The Steering Committee is about to begin planning for the NAGF's second annual meeting, which we expect to conduct this coming October. FERC Commissioner John Norris has been invited to be our keynote speaker. As we did last year, we hope to have NERC staff and the Regions participate.