Northeast Utilities System

107 Selden Street, Berlin, CT 06037

Northeast Utilities Service Company
P.O. Box 270
Hartford, CT 06141-0270
(860) 665-2036

John R. Morissette
Manager – Transmission Siting and Permitting

February 13, 2009

Judge Daniel Caruso
Chairman, Connecticut Siting Council
Ten Franklin Square
New Britain, CT 06051

Re: DOCKET NO. 346 Implementation of Section 8 and Section 54 of Public Act No. 07-242 An Act Concerning Electricity and Energy Efficiency

Dear Judge Caruso:

The Connecticut Light and Power Company (CL&P) is providing the enclosed materials in order to assist the Connecticut Siting Council in its efforts to craft a "White Paper" as described in the staff's Scoping Memo of January 21, 2009. *D346; SA Memo (Scoping), January 21, 2009* The Scoping Memo, on page 3, notes that the staff in its draft BMPs relied on the North American Electric Reliability Council's (NERC) and other standard setting agencies documents for background material in crafting its guidelines. As noted: "Staff concurs with CL&P/UI and CMEEC that the framework for the investigation and evaluation should model the Federal Energy Regulatory Commission's (FERC) Critical Energy Infrastructure Protection (CIP) standards." *D346; SA Memo (Scoping), January 21, 2009, p3.* To assist the Council in developing a complete record, CL&P is filing copies of those regulations and guides that may apply to siting concerns and a complete list of all current electric security standards and regulations. Link to NERC standards web page: http://www.nerc.com/page.php?cid=2|20 and link to NPCC documents web page: http://www.npcc.org/documents/regStandards/Criteria.aspx

To this end, CL&P has enclosed an original and 20 copy of two attachments. Attachment A includes a comprehensive list of all electric security regulations that CL&P must comply with and the web sites where those regulations may be viewed. Regarding Attachment B, because the Scoping Memo notes that the

Council's evaluation of security measures should be limited to the "siting" of facilities; CL&P has attempted to provide copies of those regulations that may possibly apply to siting concerns. Included in Attachment B are copies of regulations that relate to cyber security which do not implicate siting concerns and should not be a component of the "White Paper" but may be of ancillary interest to the Council.

If there are any questions or additional assistance that CL&P can provide please contact 860-665-2036.

Very truly yours,

John R. Morissette

Enclosures

Copies to Service List

SERVICE LIST

Party
John R. Morissette
Manager – Transmission Siting & Permitting
Northeast Utilities Service Company
P.O. Box 270
Hartford, CT 06141-0270
(860) 665-6774

Duncan MacKay, Esq.
Assistant General Counsel
Northeast Utilities Service Company
P.O. Box 270
Hartford, CT 06141-0270
(860) 665-3495
(860) 665-5504 fax
mackadr@nu.com

Robert S. Golden, Jr., Esq.
Carmody & Torrance LLP
P.O. Box 1110
50 Leavenworth Street
Waterbury, CT 06721-1110
(203) 573-1200
(203) 575-2600
rgolden@carmodylaw.com

Party
The United Illuminating Company
Linda L. Randell
Senior Vice President, General Counsel and Secretary
The United Illuminating Company
157 Church Street
New Haven, CT 06506-1904
(203) 499-2575
(203) 499-3664 fax
Linda.randell@uinet.com
uiregulatory@uinet.com

Bruce L. McDermott
Daniel P. Venora
Wiggin and Dana LLP
One Century Tower
New Haven, CT 06508-1832
(203) 498-4400
(203) 782-2889
bmcdermott@wiggin.com
dvenora@wiggin.com

Connecticut Municipal Electric
Energy Cooperative (CMEEC)
Maurice Scully
Executive Director
Connecticut Municipal Electric Energy Cooperative
30 Stott Avenue
Norwich, CT 06360
(860) 889-4088
(860) 889-8158 fax
mscully@cmeec.org

Philip Sussler, Esq.
General Counsel
Connecticut Municipal Electric Energy Cooperative
30 Stott Avenue
Norwich, CT 06360
(860) 889-4088
(860) 889-8158 fax
psussler@cmeec.org

John Buckingham
Department of Public Utility Control
10 Franklin Square
New Britain, CT 06051
860-827-2891
John.buckingham@po.state.ct.us

Intervenor
Connecticut Energy Advisory Board
(CEAB)
c/o Gretchen Deans
805 Brook Street. Bldg. 4
Rocky Hill, CT 06067
(860) 571-7147
(860) 571-7150 fax
gdeans@cerc.com

John Mengacci
Office of Policy and Management
450 Capitol Avenue #55ENR
Hartford, CT 06106
(860) 418-6374
John.mengacci@ct.gov

Julie Cammarata
Office of Policy and Management
450 Capitol Avenue #55ENR
Hartford, CT 06106
(860) 418-6296
Julie.cammarata@ct.gov

Dan Peaco
La Capra Associates
20 Winthrop Square
Boston, MA 02110
(617) 367-6500
dpeaco@lacapra.com

Heather Hunt
Law Office of Heather Hunt
242 Whippoorwill Lane
Stratford, CT 06614
(203) 380-1477
HeatherHuntLawOffice@gmail.com

Joel Gordes
Environmental Energy Solutions
38 Bookmoor Rd.
West Hartford, CT 06107
(860) 561-0566
jgordes@earthlink.net

Department of Emergency
Management and Homeland Security
James M. Thomas, Commissioner
State of Connecticut
DEMHS
25 Sigourney Street, 6th Floor
Hartford, CT 06106

Attachment A

NERC Standard	Title
BAL-001-0.1a	Real Power Balancing Control Performance
BAL-002-0	Disturbance Control Performance
BAL-003-0.1b	Frequency Response and Bias
BAL-004-1	Time Error Correction
BAL-005-0.1b	Automatic Generation Control
BAL-006-1.1	Inadvertent Interchange
CIP-001-1	Sabotage Reporting
CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1a	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets
COM-001-1.1	Telecommunications
COM-002-2	Communications and Coordination
EOP-001-1	Emergency Operations Planning
EOP-002-2.1	Capacity and Energy Emergencies
EOP-003-1	Load Shedding Plans
EOP-004-1	Disturbance Reporting
EOP-005-1	System Restoration Plans
EOP-006-1	Reliability Coordination - System Restoration
EOP-007-0	Establish, Maintain, and Document a Regional Blackstart Capability Plan
EOP-008-0	Plans for Loss of Control Center Functionality
EOP-009-0	Documentation of Blackstart Generating Unit Test Results
FAC-001-0	Facility Connection Requirements
FAC-002-0	Coordination of Plans for New Facilities
FAC-003-1	Vegetation Management Program
FAC-008-1	Facility Ratings Methodology
FAC-009-1	Establish and Communicate Facility Ratings
FAC-010-2	System Operating Limits Methodology for the Planning Horizon
FAC-011-2	System Operating Limits Methodology for the Operations Horizon
FAC-012-1	Transfer Capability Methodology
FAC-013-1	Establish and Communicate Transfer Capabilities
FAC-014-2	Establish and Communicate System Operating Limits
INT-001-3	Interchange Information
INT-003-2	Interchange Transaction Implementation
INT-004-2	Dynamic Interchange Transaction Modifications
INT-005-3	Interchange Authority Distributes Arranged Interchange
INT-006-3	Response to Interchange Authority
INT-007-1	Interchange Confirmation
INT-008-3	Interchange Authority Distributes Status
INT-009-1	Implementation of Interchange
INT-010-1	Interchange Coordination Exemptions
IRO-001-1.1	Reliability Coordination - Responsibilities and Authorities
IRO-002-2	Reliability Coordination - Facilities
IRO-003-2	Reliability Coordination - Wide-Area View
IRO-004-2	Reliability Coordination - Operations Planning
IRO-005-3	Reliability Coordination - Current Day Operations
IRO-006-4	Reliability Coordination - Transmission Loading Relief
IRO-008-1	Reliability Coordinator Operational Analyses and Real-time Assessments
IRO-009-1	Reliability Coordinator Actions to Operate Within IROLs
IRO-010-1	Reliability Coordinator Data Specification and Collection
IRO-014-1	Procedures, Processes, or Plans to Support Coordination Between Reliability Coordinators
IRO-015-1	Notifications and Information Exchange Between Reliability Coordinators
IRO-016-1	Coordination of Real-time Activities Between Reliability Coordinators
MOD-001-1	Available Transmission System Capability
MOD-002-0	Review of TTC and ATC Calculations and Results
MOD-003-0	Procedure for Input on TTC and ATC Methodologies and Values
MOD-004-1	Capacity Benefit Margin
MOD-005-0	Procedure for Verifying CBM Values
MOD-006-0.1	Procedures for the Use of Capacity Benefit Margin Values
MOD-007-0	Documentation of the Use of CBM
MOD-008-1	Transmission Reliability Margin Calculation Methodology
MOD-009-0	Procedure for Verifying TRM Values
MOD-010-0	Steady-State Data for Transmission System Modeling and Simulation
MOD-011-0	Regional Steady-State Data Requirements and Reporting Procedures
MOD-012-0	Dynamics Data for Transmission System Modeling and Simulation
MOD-013-1	Maintenance and Distribution of Dynamics Data Requirements and Reporting Procedures
MOD-014-0	Development of Interconnection-Specific Steady State System Models
MOD-015-0.1	Development of Dynamics System Models
MOD-016-1.1	Documentation of Data Reporting Requirements for Actual and Forecast Demands, Net Energy for Load, and Controllable DSM

Attachment A

NERC Standard	Title
MOD-017-0.1	Aggregated Actual and Forecast Demands and Net Energy for Load
MOD-018-0	Reports of Actual and Forecast Demand Data
MOD-019-0.1	Reporting of Interruptible Demands and Direct Control Load Management
MOD-020-0	Providing Interruptible Demands and DCLM Data
MOD-021-0	Accounting Methodology for Effects of Controllable DSM in Forecasts
MOD-024-1	Verification of Generator Gross and Net Real Power Capability
MOD-025-1	Verification of Generator Gross and Net Reactive Power Capability
MOD-028-1	Area Interchange Methodology
MOD-029-1	Rated System Path Methodology
MOD-030-1	Flowgate Methodology
NUC-001-1	Nuclear Plant Interface Coordination
PER-001-0	Operating Personnel Responsibility and Authority
PER-002-0	Operating Personnel Training
PER-003-0	Operating Personnel Credentials
PER-004-1	Reliability Coordination - Staffing
PRC-001-1	System Protection Coordination
PRC-002-1	Define Regional Disturbance Monitoring and Reporting Requirements
PRC-003-1	Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems
PRC-004-1	Analysis and Mitigation of Transmission and Generation Protection System Misoperations
PRC-005-1	Transmission and Generation Protection System Maintenance and Testing
PRC-006-0	Development and Documentation of Regional UFLS Programs
PRC-007-0	Assuring Consistency with Regional UFLS Program Requirements
PRC-008-0	Underfrequency Load Shedding Equipment Maintenance Programs
PRC-009-0	UFLS Performance Following an Underfrequency Event
PRC-010-0	Assessment of the Design and Effectiveness of UVLS Program
PRC-011-0	UVLS System Maintenance and Testing
PRC-012-0	Special Protection System Review Procedure
PRC-013-0	Special Protection System Database
PRC-014-0	Special Protection System Assessment
PRC-015-0	Special Protection System Data and Documentation
PRC-016-0.1	Special Protection System Misoperations
PRC-017-0	Special Protection System Maintenance and Testing
PRC-018-1	Disturbance Monitoring Equipment Installation and Data Reporting
PRC-020-1	Under-Voltage Load Shedding Program Database
PRC-021-1	Under-Voltage Load Shedding Program Data
PRC-022-1	Under-Voltage Load Shedding Program Performance
PRC-023-1	Transmission Relay Loadability
TOP-001-1	Reliability Responsibilities and Authorities
TOP-002-2	Normal Operations Planning
TOP-003-1	Planned Outage Coordination
TOP-004-2	Transmission Operations
TOP-005-2	Operational Reliability Information
TOP-006-2	Monitoring System Conditions
TOP-007-0	Reporting SOL and IROL Violations
TOP-008-1	Response to Transmission Limit Violations
TPL-001-0.1	System Performance Under Normal (No Contingency) Conditions (Category A)
TPL-002-0a	System Performance Following Loss of a Single Bulk Electric System Element (Category B)
TPL-003-0a	System Performance Following Loss of Two or More Bulk Electric System Elements (Category C)
TPL-004-0	System Performance Following Extreme BES Events
VAR-001-1a	Voltage and Reactive Control
VAR-002-1.1a	Generator Operation for Maintaining Network Voltage Schedules

Attachment B

NERC Standards

Standard CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

Standard CIP–003–1 — Cyber Security — Security Management Controls
Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.

Standard CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.

Standard CIP-006-1 — Cyber Security — Physical Security
Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

Standard CIP–007–1 — Cyber Security — Systems Security Management
Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s).

Standard CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.

Standard CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets
Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

Standard FAC-001-0 — Facility Connection Requirements
To avoid adverse impacts on reliability, Transmission Owners must establish facility connection and performance requirements.

Standard FAC-002-0 — Coordination of Plans for New Facilities
To avoid adverse impacts on reliability, Generator Owners and Transmission Owners and electricity end-users must meet facility connection and performance requirements.

Standard FAC-003-1 — Transmission Vegetation Management Program
To improve the reliability of the electric transmission systems by preventing outages from vegetation located on transmission rights-of-way (ROW) and minimizing outages from vegetation located adjacent to ROW.

Standard NUC-001-1 — Nuclear Plant Interface Coordination[1]
This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown.

Standard PRC-001-1 — System Protection Coordination
To ensure system protection is coordinated among operating entities.

Standard TPL-001-0 — System Performance Under Normal Conditions
Standard TPL-002-0 — System Performance Following Loss of a Single BES Element
Standard TPL-003-0 — System Performance Following Loss of Two or More BES Elements
The above set of 3 transmission planning standards requires periodic simulations and associated assessments to ensure that reliable systems are developed that meet specified performance requirements.

Link to NERC Standards web page:
http://www.nerc.com/page.php?cid=2|20

NPCC Criteria

NPCC Document A-2 Basic Criteria for Design and Operation Of Interconnected Power Systems
Criteria described in this document are to be used in the design and operation of the bulk power system.

NPCC Document A-5 Bulk Power System Protection Criteria
This document establishes the protection criteria, for protection of the NPCC bulk power system.

NPCC Document A-10 Classification of Bulk Power System Elements
This *Classification of Bulk Power System Elements* (Document A-10) provides the methodology for the identification of those elements of the interconnected NPCC Region to which NPCC bulk power system criteria are applicable.

Link to NPCC documents web page:
http://www.npcc.org/documents/regStandards/Criteria.aspx

[1] Becomes effective April 1, 2010

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-1

3. **Purpose:** Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. **Applicability:**

   4.1. Within the text of Standard CIP-003, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Reliability Organizations.

   4.2. The following are exempt from Standard CIP-003:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

   4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. **Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-003:

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.

R2.1. The senior manager shall be identified by name, title, business phone, business address, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-003:

M1. Documentation of the Responsible Entity's cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. Documentation of the assignment of, and changes to, the Responsible Entity's leadership as specified in Requirement R2.

M3. Documentation of the Responsible Entity's exceptions, as specified in Requirement R3.

M4. Documentation of the Responsible Entity's information protection program as specified in Requirement R4.

M5. The access control documentation as specified in Requirement R5.

M6. The Responsible Entity's change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Changes to the designation of senior manager were not documented in accordance with Requirement R2.2; or,

2.1.2 Exceptions from the cyber security policy have not been documented within thirty calendar days of the approval of the exception; or,

2.1.3 An information protection program to identify and classify information and the processes to protect information associated with Critical Cyber Assets has not been assessed in the previous full calendar year.

2.2. Level 2:

2.2.1 A cyber security policy exists, but has not been reviewed within the previous full calendar year; or,

2.2.2 Exceptions to policy are not documented or authorized by the senior manager or delegate(s); or,

2.2.3 Access privileges to the information related to Critical Cyber Assets have not been reviewed within the previous full calendar year; or,

2.2.4 The list of designated personnel responsible to authorize access to the information related to Critical Cyber Assets has not been reviewed within the previous full calendar year.

2.3. Level 3:

2.3.1 A senior manager has not been identified in accordance with Requirement R2.1; or,

2.3.2 The list of designated personnel responsible to authorize logical or physical access to protected information associated with Critical Cyber Assets does not exist; or,

2.3.3 No changes to hardware and software components of Critical Cyber Assets have been documented in accordance with Requirement R6.

2.4. Level 4:

2.4.1 No cyber security policy exists; or,

2.4.2 No identification and classification program for protecting information associated with Critical Cyber Assets exists; or,

2.4.3 No documented change control and configuration management process exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. **Title:** Cyber Security — Critical Cyber Asset Identification

2. **Number:** CIP-002-1

3. **Purpose:** NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

   These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

   Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

   Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. **Applicability:**

   4.1. Within the text of Standard CIP-002, "Responsible Entity" shall mean:

   - **4.1.1** Reliability Coordinator.
   - **4.1.2** Balancing Authority.
   - **4.1.3** Interchange Authority.
   - **4.1.4** Transmission Service Provider.
   - **4.1.5** Transmission Owner.
   - **4.1.6** Transmission Operator.
   - **4.1.7** Generator Owner.
   - **4.1.8** Generator Operator.
   - **4.1.9** Load Serving Entity.
   - **4.1.10** NERC.
   - **4.1.11** Regional Reliability Organizations.

   4.2. The following are exempt from Standard CIP-002:

   - **4.2.1** Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
   - **4.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. **Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-002:

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. 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. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-002:

M1. The risk-based assessment methodology documentation as specified in Requirement R1.

M2. The list of Critical Assets as specified in Requirement R2.

M3. The list of Critical Cyber Assets as specified in Requirement R3.

M4. The records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002 from the previous full calendar year

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

2. Levels of Non-Compliance

2.1 Level 1: The risk assessment has not been performed annually.

2.2 Level 2: The list of Critical Assets or Critical Cyber Assets exist, but has not been approved or reviewed in the last calendar year.

2.3 Level 3: The list of Critical Assets or Critical Cyber Assets does not exist.

2.4 Level 4: The lists of Critical Assets and Critical Cyber Assets do not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change "Control Center" to "control center"	03/24/06

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-1

3. **Purpose:** Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. **Applicability**

   4.1. Within the text of Standard CIP-005, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Reliability Organizations.

   4.2. The following are exempt from Standard CIP-005:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

   4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. **Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-005:

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings; and,

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-005. Responsible entities may document controls either individually or by specified applicable grouping.

M1. Documents about the Electronic Security Perimeter as specified in Requirement R1.

M2. Documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. Documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. Documentation of the Responsible Entity's annual vulnerability assessment as specified in Requirement R4.

M5. Access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless longer retention is required pursuant to Standard CIP-008, Requirement R2.

1.3.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005 from the previous full calendar year.

1.3.3 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 All document(s) identified in CIP-005 exist, but have not been updated within ninety calendar days of any changes as required; or,

2.1.2 Access to less than 15% of electronic security perimeters is not controlled, monitored; and logged;

2.1.3 Document(s) exist confirming that only necessary network ports and services have been enabled, but no record documenting annual reviews exists; or,

2.1.4 At least one, but not all, of the Electronic Security Perimeter vulnerability assessment items has been performed in the last full calendar year.

2.2. Level 2:

2.2.1 All document(s) identified in CIP-005 but have not been updated or reviewed in the previous full calendar year as required; or,

2.2.2 Access to between 15% and 25% of electronic security perimeters is not controlled, monitored; and logged; or,

2.2.3 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed in the previous full calendar year.

2.3. Level 3:

2.3.1 A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Cyber Assets not within the defined Electronic Security Perimeter(s); or,

2.3.2 One or more identified non-critical Cyber Assets is within the Electronic Security Perimeter(s) but not documented; or,

2.3.3 Electronic access controls document(s) exist, but one or more access points have not been identified; or

2.3.4 Electronic access controls document(s) do not identify or describe access controls for one or more access points; or,

2.3.5 Electronic Access Monitoring:

2.3.5.1 Access to between 26% and 50% of Electronic Security Perimeters is not controlled, monitored; and logged; or,

2.3.5.2 Access logs exist, but have not been reviewed within the past ninety calendar days; or,

2.3.6 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than two full calendar years.

2.4. Level 4:

2.4.1 No documented Electronic Security Perimeter exists; or,

2.4.2 No records of access exist; or,

2.4.3 51% or more Electronic Security Perimeters are not controlled, monitored, and logged; or,

2.4.4 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than three full calendar years; or,

2.4.5 No documented vulnerability assessment of the Electronic Security Perimeter(s) process exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change "Critical Assets," to "Critical Cyber Assets" as intended.	03/24/06

A. Introduction

1. **Title:** Cyber Security — Physical Security of Critical Cyber Assets

2. **Number:** CIP-006-1

3. **Purpose:** Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. **Applicability:**

   4.1. Within the text of Standard CIP-006, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Reliability Organizations.

   4.2. The following are exempt from Standard CIP-006:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

   4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. **Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-006:

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.

R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.

R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

R2. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

R2.1. Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

R2.2. Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

R2.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

R2.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R3. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:

R3.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

R3.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms

for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

R5. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

R6. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:

R6.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R6.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.

R6.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-006:

M1. The physical security plan as specified in Requirement R1 and documentation of the review and updating of the plan.

M2. Documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R2.

M3. Documentation identifying the methods for monitoring physical access as specified in Requirement R3.

M4. Documentation identifying the methods for logging physical access as specified in Requirement R4.

M5. Access logs as specified in Requirement R5.

M6. Documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documents other than those specified in Requirements R5 and R6.2 from the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to Standard CIP-003 Requirement R3.

1.4.3 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 The physical security plan exists, but has not been updated within ninety calendar days of a modification to the plan or any of its components; or,

2.1.2 Access to less than 15% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.1.3 Required documentation exists but has not been updated within ninety calendar days of a modification.; or,

2.1.4 Physical access logs are retained for a period shorter than ninety days; or,

2.1.5 A maintenance and testing program for the required physical security systems exists, but not all have been tested within the required cycle; or,

2.1.6 One required document does not exist.

2.2. Level 2:

2.2.1 The physical security plan exists, but has not been updated within six calendar months of a modification to the plan or any of its components; or,

2.2.2 Access to between 15% and 25% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.2.3 Required documentation exists but has not been updated within six calendar months of a modification; or

2.2.4 More than one required document does not exist.

2.3. Level 3:

2.3.1 The physical security plan exists, but has not been updated or reviewed in the last twelve calendar months of a modification to the physical security plan; or,

2.3.2 Access to between 26% and 50% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.3.3 No logs of monitored physical access are retained.

2.4. Level 4:

2.4.1 No physical security plan exists; or,

2.4.2 Access to more than 51% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.4.3 No maintenance or testing program exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. **Title:** Cyber Security — Systems Security Management

2. **Number:** CIP-007-1

3. **Purpose:** Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. **Applicability:**

   4.1. Within the text of Standard CIP-007, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Reliability Organizations.

   4.2. The following are exempt from Standard CIP-007:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

   4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. **Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-007:

M1. Documentation of the Responsible Entity's security test procedures as specified in Requirement R1.

M2. Documentation as specified in Requirement R2.

M3. Documentation and records of the Responsible Entity's security patch management program, as specified in Requirement R3.

M4. Documentation and records of the Responsible Entity's malicious software prevention program as specified in Requirement R4.

M5. Documentation and records of the Responsible Entity's account management program as specified in Requirement R5.

M6. Documentation and records of the Responsible Entity's security status monitoring program as specified in Requirement R6.

M7. Documentation and records of the Responsible Entity's program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. Documentation and records of the Responsible Entity's annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. Documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year.

1.3.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008 Requirement R2.

1.3.3 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information.

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 System security controls are in place, but fail to document one of the measures (M1-M9) of Standard CIP-007; or

2.1.2 One of the documents required in Standard CIP-007 has not been reviewed in the previous full calendar year as specified by Requirement R9; or,

2.1.3 One of the documented system security controls has not been updated within ninety calendar days of a change as specified by Requirement R9; or,

2.1.4 Any one of:

- Authorization rights and access privileges have not been reviewed during the previous full calendar year; or,
- A gap exists in any one log of system events related to cyber security of greater than seven calendar days; or,
- Security patches and upgrades have not been assessed for applicability within thirty calendar days of availability.

2.2. Level 2:

2.2.1 System security controls are in place, but fail to document up to two of the measures (M1-M9) of Standard CIP-007; or,

2.2.2 Two occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.3. Level 3:

2.3.1 System security controls are in place, but fail to document up to three of the measures (M1-M9) of Standard CIP-007; or,

2.3.2 Three occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.4. Level 4:

2.4.1 System security controls are in place, but fail to document four or more of the measures (M1-M9) of Standard CIP-007; or,

2.4.2 Four occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.4.3 No logs exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-1

3. **Purpose:** Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. **Applicability**

   4.1. Within the text of Standard CIP-008, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Reliability Organizations.

   4.2. The following are exempt from Standard CIP-008:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

   4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. **Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-008:

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all

reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of CIP-008:

M1. The Cyber Security Incident response plan as indicated in R1 and documentation of the review, updating, and testing of the plan

M2. All documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008 for the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

1.4.3 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.4.4 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. **Levels of Noncompliance**

2.1. Level 1: A Cyber Security Incident response plan exists, but has not been updated within ninety calendar days of changes.

2.2. Level 2:

2.2.1 A Cyber Security Incident response plan exists, but has not been reviewed in the previous full calendar year; or,

2.2.2 A Cyber Security Incident response plan has not been tested in the previous full calendar year; or,

2.2.3 Records related to reportable Cyber Security Incidents were not retained for three calendar years.

2.3. Level 3:

2.3.1 A Cyber Security Incident response plan exists, but does not include required elements Requirements R1.1, R1.2, and R1.3 of Standard CIP-008; or,

2.3.2 A reportable Cyber Security Incident has occurred but was not reported to the ES ISAC.

2.4. Level 4: A Cyber Security Incident response plan does not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for Critical Cyber Assets

2. **Number:** CIP-009-1

3. **Purpose:** Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. **Applicability:**

   4.1. Within the text of Standard CIP-009, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator

   4.1.2 Balancing Authority

   4.1.3 Interchange Authority

   4.1.4 Transmission Service Provider

   4.1.5 Transmission Owner

   4.1.6 Transmission Operator

   4.1.7 Generator Owner

   4.1.8 Generator Operator

   4.1.9 Load Serving Entity

   4.1.10 NERC

   4.1.11 Regional Reliability Organizations

   4.2. The following are exempt from Standard CIP-009:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

   4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. **Effective Date:** June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-009:

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-009:

M1. Recovery plan(s) as specified in Requirement R1.

M2. Records documenting required exercises as specified in Requirement R2.

M3. Documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. Documentation regarding backup and storage of information as specified in Requirement R4.

M5. Documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-009 from the previous full calendar year.

1.3.2 The Compliance Monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

2. **Levels of Noncompliance**

2.1. Level 1:

2.1.1 Recovery plan(s) exist and are exercised, but do not contain all elements as specified in Requirement R1; or,

2.1.2 Recovery plan(s) are not updated and personnel are not notified within ninety calendar days of the change.

2.2. Level 2:

2.2.1 Recovery plan(s) exist, but have not been reviewed during the previous full calendar year; or,

2.2.2 Documented processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets do not exist.

2.3. Level 3:

2.3.1 Testing of information stored on backup media to ensure that the information is available has not been performed at least annually; or,

2.3.2 Recovery plan(s) exist, but have not been exercised during the previous full calendar year.

2.4. Level 4:

2.4.1 No recovery plan(s) exist; or,

2.4.2 Backup of information required to successfully restore Critical Cyber Assets does not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. **Title:** **Nuclear Plant Interface Coordination**

2. **Number:** NUC-001-1

3. **Purpose:** This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown.

4. **Applicability:**

   4.1. Nuclear Plant Generator Operator.

   4.2. Transmission Entities shall mean all entities that are responsible for providing services related to Nuclear Plant Interface Requirements (NPIRs). Such entities may include one or more of the following:

   4.2.1 Transmission Operators.

   4.2.2 Transmission Owners.

   4.2.3 Transmission Planners.

   4.2.4 Transmission Service Providers.

   4.2.5 Balancing Authorities.

   4.2.6 Reliability Coordinators.

   4.2.7 Planning Authorities.

   4.2.8 Distribution Providers.

   4.2.9 Load-serving Entities.

   4.2.10 Generator Owners.

   4.2.11 Generator Operators.

5. **Effective Date:** First day of first quarter 15 months after applicable regulatory approvals.

B. Requirements

R1. The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt [*Risk Factor: Lower*]

R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements[1] that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs. [*Risk Factor: Lower*]

R3. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the

1. Agreements may include mutually agreed upon procedures or protocols.

electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator. [*Risk Factor: Medium*]

R4. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall: [*Risk Factor: Medium*]

R4.1. Incorporate the NPIRs into their operating analyses of the electric system.

R4.2. Operate the electric system to meet the NPIRs.

R4.3. Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.

R5. The Nuclear Plant Generator Operator shall operate per the Agreements developed in accordance with this standard. [*Risk Factor: Medium*]

R6. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs. [*Risk Factor: Medium*]

R7. Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: Medium*]

R8. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: Medium*]

R9. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2: [*Risk Factor: Lower*]

R9.1. Administrative elements:

R9.1.1. Definitions of key terms used in the agreement.

R9.1.2. Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.

R9.1.3. A requirement to review the agreement(s) at least every three years.

R9.1.4. A dispute resolution mechanism.

R9.2. Technical requirements and analysis:

R9.2.1. Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the agreement.

R9.2.2. Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.

R9.2.3. Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.

R9.3. Operations and maintenance coordination:

R9.3.1. Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.

R9.3.2. Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.

R9.3.3. Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.

R9.3.4. Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.

R9.3.5. Provision to consider nuclear plant coping times required by the NPLRs and their relation to the coordination of grid and nuclear plant restoration following a nuclear plant loss of Off-site Power.

R9.3.6. Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.

R9.3.7. Coordination of the NPIRs with transmission system Special Protection Systems and underfrequency and undervoltage load shedding programs.

R9.4. Communications and training:

R9.4.1. Provisions for communications between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of terms.

R9.4.2. Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.

R9.4.3. Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.

R9.4.4. Provisions for supplying information necessary to report to government agencies, as related to NPIRs.

R9.4.5. Provisions for personnel training, as related to NPIRs.

C. Measures

M1. The Nuclear Plant Generator Operator shall, upon request of the Compliance Monitor, provide a copy of the transmittal and receipt of transmittal of the proposed NPIRs to the responsible Transmission Entities. (Requirement 1)

M2. The Nuclear Plant Generator Operator and each Transmission Entity shall each have a copy of the Agreement(s) addressing the elements in Requirement 9 available for inspection upon request of the Compliance Monitor. (Requirement 2 and 9)

M3. Each Transmission Entity responsible for planning analyses in accordance with the Agreement shall, upon request of the Compliance Monitor, provide a copy of the planning analyses results transmitted to the Nuclear Plant Generator Operator, showing incorporation of the NPIRs. The Compliance Monitor shall refer to the Agreements developed in accordance with this standard for specific requirements. (Requirement 3)

M4. Each Transmission Entity responsible for operating the electric system in accordance with the Agreement shall demonstrate or provide evidence of the following, upon request of the Compliance Monitor:

M4.1 The NPIRs have been incorporated into the current operating analysis of the electric system. (Requirement 4.1)

M4.2 The electric system was operated to meet the NPIRs. (Requirement 4.2)

M4.3 The Transmission Entity informed the Nuclear Plant Generator Operator when it became aware it lost the capability to assess the operation of the electric system affecting the NPIRs. (Requirement 4.3)

M5. The Nuclear Plant Generator Operator shall, upon request of the Compliance Monitor, demonstrate or provide evidence that the Nuclear Power Plant is being operated consistent with the Agreements developed in accordance with this standard. (Requirement 5)

M6. The Transmission Entities and Nuclear Plant Generator Operator shall, upon request of the Compliance Monitor, provide evidence of the coordination between the Transmission Entities and the Nuclear Plant Generator Operator regarding outages and maintenance activities which affect the NPIRs. (Requirement 6)

M7. The Nuclear Plant Generator Operator shall provide evidence that it informed the applicable Transmission Entities of changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Transmission Entities to meet the NPIRs. (Requirement 7)

M8. The Transmission Entities shall each provide evidence that it informed the Nuclear Plant Generator Operator of changes to electric system design, configuration, operations, limits, protection systems, or capabilities that would impact the ability of the Nuclear Plant Generator Operator to meet the NPIRs. (Requirement 8)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.3. Data Retention

For Measure 1, the Nuclear Plant Generator Operator shall keep its latest transmittals and receipts.

For Measure 2, the Nuclear Plant Generator Operator and each Transmission Entity shall have its current, in-force agreement.

For Measure 3, the Transmission Entity shall have the latest planning analysis results.

For Measures 4.3, 6 and 8, the Transmission Entity shall keep evidence for two years plus current.

For Measures 5, 6 and 7, the Nuclear Plant Generator Operator shall keep evidence for two years plus current.

If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor.

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

The Nuclear Plant Generator Operator and Transmission Entities shall each demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

2. Violation Severity Levels

2.1. Lower: Agreement(s) exist per this standard and NPIRs were identified and implemented, but documentation described in M1-M8 was not provided.

2.2. Moderate: Agreement(s) exist per R2 and NPIRs were identified and implemented, but one or more elements of the Agreement in R9 were not met.

2.3. High: One or more requirements of R3 through R8 were not met.

2.4. Severe: No proposed NPIRs were submitted per R1, no Agreement exists per this standard, or the Agreements were not implemented.

E. Regional Differences

The design basis for Canadian (CANDU) NPPs does not result in the same licensing requirements as U.S. NPPs. NRC design criteria specifies that in addition to emergency on-site electrical power, electrical power from the electric network also be provided to permit safe shutdown. This requirement is specified in such NRC Regulations as 10 CFR 50 Appendix A — General Design Criterion 17 and 10 CFR 50.63 Loss of all alternating current power. There are no equivalent Canadian Regulatory requirements for Station Blackout (SBO) or coping times as they do not form part of the licensing basis for CANDU NPPs. Therefore the definition of NPLR for Canadian CANDU units will be as follows:

Nuclear Plant Licensing Requirements (NPLR) are requirements included in the design basis of the nuclear plant and are statutorily mandated for the operation of the plant; when used in this standard, NPLR shall mean nuclear power plant licensing requirements for avoiding preventable challenges to nuclear safety as a result of an electric system disturbance, transient, or condition.

F. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	May 2, 2007	Approved by Board of Trustees	New

A. Introduction

1. **Title:** **Transmission Vegetation Management Program**

2. **Number:** FAC-003-1

3. **Purpose:** To improve the reliability of the electric transmission systems by preventing outages from vegetation located on transmission rights-of-way (ROW) and minimizing outages from vegetation located adjacent to ROW, maintaining clearances between transmission lines and vegetation on and along transmission ROW, and reporting vegetation-related outages of the transmission systems to the respective Regional Reliability Organizations (RRO) and the North American Electric Reliability Council (NERC).

4. **Applicability:**

   4.1. Transmission Owner.

   4.2. Regional Reliability Organization.

   4.3. This standard shall apply to all transmission lines operated at 200 kV and above and to any lower voltage lines designated by the RRO as critical to the reliability of the electric system in the region.

5. **Effective Dates:**

   5.1. One calendar year from the date of adoption by the NERC Board of Trustees for Requirements 1 and 2.

   5.2. Sixty calendar days from the date of adoption by the NERC Board of Trustees for Requirements 3 and 4.

B. Requirements

R1. The Transmission Owner shall prepare, and keep current, a formal transmission vegetation management program (TVMP). The TVMP shall include the Transmission Owner's objectives, practices, approved procedures, and work specifications[1].

R1.1. The TVMP shall define a schedule for and the type (aerial, ground) of ROW vegetation inspections. This schedule should be flexible enough to adjust for changing conditions. The inspection schedule shall be based on the anticipated growth of vegetation and any other environmental or operational factors that could impact the relationship of vegetation to the Transmission Owner's transmission lines.

R1.2. The Transmission Owner, in the TVMP, shall identify and document clearances between vegetation and any overhead, ungrounded supply conductors, taking into consideration transmission line voltage, the effects of ambient temperature on conductor sag under maximum design loading, and the effects of wind velocities on conductor sway. Specifically, the Transmission Owner shall establish clearances to be achieved at the time of vegetation management work identified herein as Clearance 1, and shall also establish and maintain a set of clearances identified herein as Clearance 2 to prevent flashover between vegetation and overhead ungrounded supply conductors.

R1.2.1. Clearance 1 — The Transmission Owner shall determine and document appropriate clearance distances to be achieved at the time of transmission vegetation management work based upon local conditions and the expected time frame in which the Transmission Owner plans to return for future

[1] ANSI A300, Tree Care Operations – Tree, Shrub, and Other Woody Plant Maintenance – Standard Practices, while not a requirement of this standard, is considered to be an industry best practice.

vegetation management work. Local conditions may include, but are not limited to: operating voltage, appropriate vegetation management techniques, fire risk, reasonably anticipated tree and conductor movement, species types and growth rates, species failure characteristics, local climate and rainfall patterns, line terrain and elevation, location of the vegetation within the span, and worker approach distance requirements. Clearance 1 distances shall be greater than those defined by Clearance 2 below.

R1.2.2. Clearance 2 — The Transmission Owner shall determine and document specific radial clearances to be maintained between vegetation and conductors under all rated electrical operating conditions. These minimum clearance distances are necessary to prevent flashover between vegetation and conductors and will vary due to such factors as altitude and operating voltage. These Transmission Owner-specific minimum clearance distances shall be no less than those set forth in the Institute of Electrical and Electronics Engineers (IEEE) Standard 516-2003 (*Guide for Maintenance Methods on Energized Power Lines*) and as specified in its Section 4.2.2.3, Minimum Air Insulation Distances without Tools in the Air Gap.

R1.2.2.1 Where transmission system transient overvoltage factors are not known, clearances shall be derived from Table 5, IEEE 516-2003, phase-to-ground distances, with appropriate altitude correction factors applied.

R1.2.2.2 Where transmission system transient overvoltage factors are known, clearances shall be derived from Table 7, IEEE 516-2003, phase-to-phase voltages, with appropriate altitude correction factors applied.

R1.3. All personnel directly involved in the design and implementation of the TVMP shall hold appropriate qualifications and training, as defined by the Transmission Owner, to perform their duties.

R1.4. Each Transmission Owner shall develop mitigation measures to achieve sufficient clearances for the protection of the transmission facilities when it identifies locations on the ROW where the Transmission Owner is restricted from attaining the clearances specified in Requirement 1.2.1.

R1.5. Each Transmission Owner shall establish and document a process for the immediate communication of vegetation conditions that present an imminent threat of a transmission line outage. This is so that action (temporary reduction in line rating, switching line out of service, etc.) may be taken until the threat is relieved.

R2. The Transmission Owner shall create and implement an annual plan for vegetation management work to ensure the reliability of the system. The plan shall describe the methods used, such as manual clearing, mechanical clearing, herbicide treatment, or other actions. The plan should be flexible enough to adjust to changing conditions, taking into consideration anticipated growth of vegetation and all other environmental factors that may have an impact on the reliability of the transmission systems. Adjustments to the plan shall be documented as they occur. The plan should take into consideration the time required to obtain permissions or permits from landowners or regulatory authorities. Each Transmission Owner shall have systems and procedures for documenting and tracking the planned vegetation management work and ensuring that the vegetation management work was completed according to work specifications.

R3. The Transmission Owner shall report quarterly to its RRO, or the RRO's designee, sustained transmission line outages determined by the Transmission Owner to have been caused by vegetation.

R3.1. Multiple sustained outages on an individual line, if caused by the same vegetation, shall be reported as one outage regardless of the actual number of outages within a 24-hour period.

R3.2. The Transmission Owner is not required to report to the RRO, or the RRO's designee, certain sustained transmission line outages caused by vegetation: (1) Vegetation-related outages that result from vegetation falling into lines from outside the ROW that result from natural disasters shall not be considered reportable (examples of disasters that could create non-reportable outages include, but are not limited to, earthquakes, fires, tornados, hurricanes, landslides, wind shear, major storms as defined either by the Transmission Owner or an applicable regulatory body, ice storms, and floods), and (2) Vegetation-related outages due to human or animal activity shall not be considered reportable (examples of human or animal activity that could cause a non-reportable outage include, but are not limited to, logging, animal severing tree, vehicle contact with tree, arboricultural activities or horticultural or agricultural activities, or removal or digging of vegetation).

R3.3. The outage information provided by the Transmission Owner to the RRO, or the RRO's designee, shall include at a minimum: the name of the circuit(s) outaged, the date, time and duration of the outage; a description of the cause of the outage; other pertinent comments; and any countermeasures taken by the Transmission Owner.

R3.4. An outage shall be categorized as one of the following:

R3.4.1. Category 1 — Grow-ins: Outages caused by vegetation growing into lines from vegetation inside and/or outside of the ROW;

R3.4.2. Category 2 — Fall-ins: Outages caused by vegetation falling into lines from inside the ROW;

R3.4.3. Category 3 — Fall-ins: Outages caused by vegetation falling into lines from outside the ROW.

R4. The RRO shall report the outage information provided to it by Transmission Owner's, as required by Requirement 3, quarterly to NERC, as well as any actions taken by the RRO as a result of any of the reported outages.

C. Measures

M1. The Transmission Owner has a documented TVMP, as identified in Requirement 1.

M1.1. The Transmission Owner has documentation that the Transmission Owner performed the vegetation inspections as identified in Requirement 1.1.

M1.2. The Transmission Owner has documentation that describes the clearances identified in Requirement 1.2.

M1.3. The Transmission Owner has documentation that the personnel directly involved in the design and implementation of the Transmission Owner's TVMP hold the qualifications identified by the Transmission Owner as required in Requirement 1.3.

M1.4. The Transmission Owner has documentation that it has identified any areas not meeting the Transmission Owner's standard for vegetation management and any mitigating measures the Transmission Owner has taken to address these deficiencies as identified in Requirement 1.4.

M1.5. The Transmission Owner has a documented process for the immediate communication of imminent threats by vegetation as identified in Requirement 1.5.

M2. The Transmission Owner has documentation that the Transmission Owner implemented the work plan identified in Requirement 2.

M3. The Transmission Owner has documentation that it has supplied quarterly outage reports to the RRO, or the RRO's designee, as identified in Requirement 3.

M4. The RRO has documentation that it provided quarterly outage reports to NERC as identified in Requirement 4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

RRO

NERC

1.2. Compliance Monitoring Period and Reset

One calendar Year

1.3. Data Retention

Five Years

1.4. Additional Compliance Information

The Transmission Owner shall demonstrate compliance through self-certification submitted to the compliance monitor (RRO) annually that it meets the requirements of NERC Reliability Standard FAC-003-1. The compliance monitor shall conduct an on-site audit every five years or more frequently as deemed appropriate by the compliance monitor to review documentation related to Reliability Standard FAC-003-1. Field audits of ROW vegetation conditions may be conducted if determined to be necessary by the compliance monitor.

2. Levels of Non-Compliance

2.1. Level 1:

2.1.1. The TVMP was incomplete in one of the requirements specified in any subpart of Requirement 1, or;

2.1.2. Documentation of the annual work plan, as specified in Requirement 2, was incomplete when presented to the Compliance Monitor during an on-site audit, or;

2.1.3. The RRO provided an outage report to NERC that was incomplete and did not contain the information required in Requirement 4.

2.2. Level 2:

2.2.1. The TVMP was incomplete in two of the requirements specified in any subpart of Requirement 1, or;

2.2.2. The Transmission Owner was unable to certify during its annual self-certification that it fully implemented its annual work plan, or documented deviations from, as specified in Requirement 2.

2.2.3. The Transmission Owner reported one Category 2 transmission vegetation-related outage in a calendar year.

2.3. Level 3:

2.3.1. The Transmission Owner reported one Category 1 or multiple Category 2 transmission vegetation-related outages in a calendar year, or;

2.3.2. The Transmission Owner did not maintain a set of clearances (Clearance 2), as defined in Requirement 1.2.2, to prevent flashover between vegetation and overhead ungrounded supply conductors, or;

2.3.3. The TVMP was incomplete in three of the requirements specified in any subpart of Requirement 1.

2.4. Level 4:

2.4.1. The Transmission Owner reported more than one Category 1 transmission vegetation-related outage in a calendar year, or;

2.4.2. The TVMP was incomplete in four or more of the requirements specified in any subpart of Requirement 1.

E. Regional Differences

None Identified.

Version History

Version	Date	Action	Change Tracking
Version 1	TBA	1. Added "Standard Development Roadmap." 2. Changed "60" to "Sixty" in section A, 5.2. 3. Added "Proposed Effective Date: April 7, 2006" to footer. 4. Added "Draft 3: November 17, 2005" to footer.	01/20/06

A. Introduction

1. **Title:** **Coordination of Plans For New Generation, Transmission, and End-User Facilities**
2. **Number:** FAC-002-0
3. **Purpose:** To avoid adverse impacts on reliability, Generator Owners and Transmission Owners and electricity end-users must meet facility connection and performance requirements.
4. **Applicability:**
   - **4.1.** Generator Owner
   - **4.2.** Transmission Owner
   - **4.3.** Distribution Provider
   - **4.4.** Load-Serving Entity
   - **4.5.** Transmission Planner
   - **4.6.** Planning Authority
5. **Effective Date:** April 1, 2005

B. Requirements

R1. The Generator Owner, Transmission Owner, Distribution Provider, and Load-Serving Entity seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities shall each coordinate and cooperate on its assessments with its Transmission Planner and Planning Authority. The assessment shall include:

- **R1.1.** Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.
- **R1.2.** Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.
- **R1.3.** Evidence that the parties involved in the assessment have coordinated and cooperated on the assessment of the reliability impacts of new facilities on the interconnected transmission systems. While these studies may be performed independently, the results shall be jointly evaluated and coordinated by the entities involved.
- **R1.4.** Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance in accordance with Reliability Standard TPL-001-0.
- **R1.5.** Documentation that the assessment included study assumptions, system performance, alternatives considered, and jointly coordinated recommendations.

R2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) and NERC on request (within 30 calendar days).

C. Measures

M1. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider's documentation of its assessment of the reliability impacts of new facilities shall address all items in Reliability Standard FAC-002-0_R1.

M2. The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each have evidence of its assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems is retained and provided to other entities in accordance with Reliability Standard FAC-002-0_R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Compliance Monitor: RRO.

1.2. Compliance Monitoring Period and Reset Timeframe

On request (within 30 calendar days).

1.3. Data Retention

Evidence of the assessment of the reliability impacts of new facilities and their connections on the interconnected transmission systems: Three years.

1.4. Additional Compliance Information

None

2. Levels of Non-Compliance

2.1. Level 1: Assessments of the impacts of new facilities were provided, but were incomplete in one or more requirements of Reliability Standard FAC-002_R1.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: Assessments of the impacts of new facilities were not provided.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	January 13, 2006	Removed duplication of "Regional Reliability Organizations(s).	Errata

Standard FAC-001-0 — Facility Connection Requirements

A. Introduction

1. **Title:** **Facility Connection Requirements**
2. **Number:** FAC-001-0
3. **Purpose:** To avoid adverse impacts on reliability, Transmission Owners must establish facility connection and performance requirements.
4. **Applicability:**
   - **4.1.** Transmission Owner
5. **Effective Date:** April 1, 2005

B. Requirements

R1. The Transmission Owner shall document, maintain, and publish facility connection requirements to ensure compliance with NERC Reliability Standards and applicable Regional Reliability Organization, subregional, Power Pool, and individual Transmission Owner planning criteria and facility connection requirements. The Transmission Owner's facility connection requirements shall address connection requirements for:

- **R1.1.** Generation facilities,
- **R1.2.** Transmission facilities, and
- **R1.3.** End-user facilities

R2. The Transmission Owner's facility connection requirements shall address, but are not limited to, the following items:

- **R2.1.** Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:
  - **R2.1.1.** Procedures for coordinated joint studies of new facilities and their impacts on the interconnected transmission systems.
  - **R2.1.2.** Procedures for notification of new or modified facilities to others (those responsible for the reliability of the interconnected transmission systems) as soon as feasible.
  - **R2.1.3.** Voltage level and MW and MVAR capacity or demand at point of connection.
  - **R2.1.4.** Breaker duty and surge protection.
  - **R2.1.5.** System protection and coordination.
  - **R2.1.6.** Metering and telecommunications.
  - **R2.1.7.** Grounding and safety issues.
  - **R2.1.8.** Insulation and insulation coordination.
  - **R2.1.9.** Voltage, Reactive Power, and power factor control.
  - **R2.1.10.** Power quality impacts.
  - **R2.1.11.** Equipment Ratings.
  - **R2.1.12.** Synchronizing of facilities.

R2.1.13. Maintenance coordination.

R2.1.14. Operational issues (abnormal frequency and voltages).

R2.1.15. Inspection requirements for existing or new facilities.

R2.1.16. Communications and procedures during normal and emergency operating conditions.

R3. The Transmission Owner shall maintain and update its facility connection requirements as required. The Transmission Owner shall make documentation of these requirements available to the users of the transmission system, the Regional Reliability Organization, and NERC on request (five business days).

C. Measures

M1. The Transmission Owner shall make available (to its Compliance Monitor) for inspection evidence that it met all the requirements stated in Reliability Standard FAC-001-0_R1.

M2. The Transmission Owner shall make available (to its Compliance Monitor) for inspection evidence that it met all requirements stated in Reliability Standard FAC-001-0_R2.

M3. The Transmission Owner shall make available (to its Compliance Monitor) for inspection evidence that it met all the requirements stated in Reliability Standard FAC-001-0_R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Compliance Monitor: Regional Reliability Organization.

1.2. Compliance Monitoring Period and Reset Timeframe

On request (five business days).

1.3. Data Retention

None specified.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance

2.1. Level 1: Facility connection requirements were provided for generation, transmission, and end-user facilities, per Reliability Standard FAC-001-0_R1, but the document(s) do not address all of the requirements of Reliability Standard FAC-001-0_R2.

2.2. Level 2: Facility connection requirements were not provided for all three categories (generation, transmission, or end-user) of facilities, per Reliability Standard FAC-001-0_R1, but the document(s) provided address all of the requirements of Reliability Standard FAC-001-0_R2.

2.3. Level 3: Facility connection requirements were not provided for all three categories (generation, transmission, or end-user) of facilities, per Reliability Standard FAC-001-0_R1, and the document(s) provided do not address all of the requirements of Reliability Standard FAC-001-0_R2.

2.4. **Level 4:** No document on facility connection requirements was provided per Reliability Standard FAC-001-0_R3.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New

A. Introduction

1. **Title:** **System Protection Coordination**
2. **Number:** PRC-001-1
3. **Purpose:**

   To ensure system protection is coordinated among operating entities.

4. **Applicability**

   4.1. Balancing Authorities

   4.2. Transmission Operators

   4.3. Generator Operators

5. **Effective Date:** January 1, 2007

B. Requirements

R1. Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of protection system schemes applied in its area.

R2. Each Generator Operator and Transmission Operator shall notify reliability entities of relay or equipment failures as follows:

R2.1. If a protective relay or equipment failure reduces system reliability, the Generator Operator shall notify its Transmission Operator and Host Balancing Authority. The Generator Operator shall take corrective action as soon as possible.

R2.2. If a protective relay or equipment failure reduces system reliability, the Transmission Operator shall notify its Reliability Coordinator and affected Transmission Operators and Balancing Authorities. The Transmission Operator shall take corrective action as soon as possible.

R3. A Generator Operator or Transmission Operator shall coordinate new protective systems and changes as follows.

R3.1. Each Generator Operator shall coordinate all new protective systems and all protective system changes with its Transmission Operator and Host Balancing Authority.

R3.2. Each Transmission Operator shall coordinate all new protective systems and all protective system changes with neighboring Transmission Operators and Balancing Authorities.

R4. Each Transmission Operator shall coordinate protection systems on major transmission lines and interconnections with neighboring Generator Operators, Transmission Operators, and Balancing Authorities.

R5. A Generator Operator or Transmission Operator shall coordinate changes in generation, transmission, load or operating conditions that could require changes in the protection systems of others:

R5.1. Each Generator Operator shall notify its Transmission Operator in advance of changes in generation or operating conditions that could require changes in the Transmission Operator's protection systems.

R5.2. Each Transmission Operator shall notify neighboring Transmission Operators in advance of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' protection systems.

R6. Each Transmission Operator and Balancing Authority shall monitor the status of each Special Protection System in their area, and shall notify affected Transmission Operators and Balancing Authorities of each change in status.

C. Measures

M1. Each Generator Operator and Transmission Operator shall have and provide upon request evidence that could include but is not limited to, revised fault analysis study, letters of agreement on settings, notifications of changes, or other equivalent evidence that will be used to confirm that there was coordination of new protective systems or changes as noted in Requirements 3, 3.1, and 3.2.

M2. Each Transmission Operator and Balancing Authority shall have and provide upon request evidence that could include but is not limited to, documentation, electronic logs, computer printouts, or computer demonstration or other equivalent evidence that will be used to confirm that it monitors the Special Protection Systems in its area. (Requirement 6 Part 1)

M3. Each Transmission Operator and Balancing Authority shall have and provide upon request evidence that could include but is not limited to, operator logs, phone records, electronic-notifications or other equivalent evidence that will be used to confirm that it notified affected Transmission Operator and Balancing Authorities of changes in status of one of its Special Protection Systems. (Requirement 6 Part 2)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organizations shall be responsible for compliance monitoring.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to assess compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will

have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Generator Operator and Transmission Operator shall have current, in-force documents available as evidence of compliance for Measure 1.

Each Transmission Operator and Balancing Authority shall keep 90 days of historical data (evidence) for Measures 2 and 3.

If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance for Generator Operators:

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: Failed to provide evidence of coordination when installing new protective systems and all protective system changes with its Transmission Operator and Host Balancing Authority as specified in R3.1.

3. Levels of Non-Compliance for Transmission Operators:

3.1. Level 1: Not applicable.

3.2. Level 2: Not applicable.

3.3. Level 3: Not applicable.

3.4. Level 4: There shall be a separate Level 4 non-compliance, for every one of the following requirements that is in violation:

3.4.1 Failed to provide evidence of coordination when installing new protective systems and all protective system changes with neighboring Transmission Operators and Balancing Authorities as specified in R3.2.

3.4.2 Did not monitor the status of each Special Protection System, or did not notify affected Transmission Operators, Balancing Authorities of changes in special protection status as specified in R6.

4. **Levels of Non-Compliance for Balancing Authorities:**

4.1. Level 1: Not applicable.

4.2. Level 2: Not applicable.

4.3. Level 3: Not applicable.

4.4. Level 4: Did not monitor the status of each Special Protection System, or did not notify affected Transmission Operators, Balancing Authorities of changes in special protection status as specified in R6.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0	August 25, 2005	Fixed Standard number in Introduction from PRC-001-1 to PRC-001-0	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised

A. Introduction

1. **Title:** **System Performance Under Normal (No Contingency) Conditions (Category A)**
2. **Number:** TPL-001-0
3. **Purpose:** System simulations and associated assessments are needed periodically to ensure that reliable systems are developed that meet specified performance requirements with sufficient lead time, and continue to be modified or upgraded as necessary to meet present and future system needs.
4. **Applicability:**
   - **4.1.** Planning Authority
   - **4.2.** Transmission Planner
5. **Effective Date:** April 1, 2005

B. Requirements

R1. The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that, with all transmission facilities in service and with normal (pre-contingency) operating procedures in effect, the Network can be operated to supply projected customer demands and projected Firm (non- recallable reserved) Transmission Services at all Demand levels over the range of forecast system demands, under the conditions defined in Category A of Table I. To be considered valid, the Planning Authority and Transmission Planner assessments shall:

- **R1.1.** Be made annually.
- **R1.2.** Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.
- **R1.3.** Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category A of Table 1 (no contingencies). The specific elements selected (from each of the following categories) shall be acceptable to the associated Regional Reliability Organization(s).
  - **R1.3.1.** Cover critical system conditions and study years as deemed appropriate by the entity performing the study.
  - **R1.3.2.** Be conducted annually unless changes to system conditions do not warrant such analyses.
  - **R1.3.3.** Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.
  - **R1.3.4.** Have established normal (pre-contingency) operating procedures in place.
  - **R1.3.5.** Have all projected firm transfers modeled.
  - **R1.3.6.** Be performed for selected demand levels over the range of forecast system demands.
  - **R1.3.7.** Demonstrate that system performance meets Table 1 for Category A (no contingencies).
  - **R1.3.8.** Include existing and planned facilities.

R1.3.9. Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.

R1.4. Address any planned upgrades needed to meet the performance requirements of Category A.

R2. When system simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-001-0_R1, the Planning Authority and Transmission Planner shall each:

R2.1. Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon.

R2.1.1. Including a schedule for implementation.

R2.1.2. Including a discussion of expected required in-service dates of facilities.

R2.1.3. Consider lead times necessary to implement plans.

R2.2. Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed implementation plans are not needed.

R3. The Planning Authority and Transmission Planner shall each document the results of these reliability assessments and corrective plans and shall annually provide these to its respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.

C. Measures

M1. The Planning Authority and Transmission Planner shall have a valid assessment and corrective plans as specified in Reliability Standard TPL-001-0_R2.1 and TPL-001-0_R2.2.

M2. The Planning Authority and Transmission Planner shall have evidence it reported documentation of results of its Reliability Assessments and corrective plans per Reliability Standard TPL-001-0_R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility
Compliance Monitor: Regional Reliability Organization.
Each Compliance Monitor shall report compliance and violations to NERC via the NERC Compliance Reporting Process.

1.2. Compliance Monitoring Period and Reset Timeframe
Annually

1.3. Data Retention
None specified.

1.4. Additional Compliance Information

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: A valid assessment and corrective plan for the longer-term planning horizon is not available.

2.3. Level 3: Not applicable.

2.4. Level 4: A valid assessment and corrective plan for the near-term planning horizon is not available.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	June 03, 2005	Fixed reference in M1 to read TPL-001-0 R2.1 and TPL-001-0 R2.2	Errata

Table I. Transmission System Standards – Normal and Emergency Conditions

Category	Contingencies	System Limits or Impacts		
	Initiating Event(s) and Contingency Element(s)	System Stable and both Thermal and Voltage Limits within Applicable Rating[a]	Loss of Demand or Curtailed Firm Transfers	Cascading Outages
A No Contingencies	All Facilities in Service	Yes	No	No
B Event resulting in the loss of a single element.	Single Line Ground (SLG) or 3-Phase (3Ø) Fault, with Normal Clearing: 1. Generator 2. Transmission Circuit 3. Transformer Loss of an Element without a Fault	Yes Yes Yes Yes	No[b] No[b] No[b] No[b]	No No No No
	Single Pole Block, Normal Clearing[e]: 4. Single Pole (dc) Line	Yes	No[b]	No
C Event(s) resulting in the loss of two or more (multiple) elements.	SLG Fault, with Normal Clearing[e]: 1. Bus Section 2. Breaker (failure or internal Fault)	Yes Yes	Planned/ Controlled[c] Planned/ Controlled[c]	No No
	SLG or 3Ø Fault, with Normal Clearing[e], Manual System Adjustments, followed by another SLG or 3Ø Fault, with Normal Clearing[e]: 3. Category B (B1, B2, B3, or B4) contingency, manual system adjustments, followed by another Category B (B1, B2, B3, or B4) contingency	Yes	Planned/ Controlled[c]	No
	Bipolar Block, with Normal Clearing[e]: 4. Bipolar (dc) Line Fault (non 3Ø), with Normal Clearing[e]: 5. Any two circuits of a multiple circuit towerline[f]	Yes Yes	Planned/ Controlled[c] Planned/ Controlled[c]	No No
	SLG Fault, with Delayed Clearing[e] (stuck breaker or protection system failure): 6. Generator 7. Transformer 8. Transmission Circuit 9. Bus Section	Yes Yes Yes Yes	Planned/ Controlled[c] Planned/ Controlled[c] Planned/ Controlled[c] Planned/ Controlled[c]	No No No No

D [d] Extreme event resulting in two or more (multiple) elements removed or Cascading out of service.	3Ø Fault, with Delayed Clearing [e] (stuck breaker or protection system failure): 1. Generator 2. Transmission Circuit 3. Transformer 4. Bus Section 3Ø Fault, with Normal Clearing[e]: 5. Breaker (failure or internal Fault) 6. Loss of towerline with three or more circuits 7. All transmission lines on a common right-of way 8. Loss of a substation (one voltage level plus transformers) 9. Loss of a switching station (one voltage level plus transformers) 10. Loss of all generating units at a station 11. Loss of a large Load or major Load center 12. Failure of a fully redundant Special Protection System (or remedial action scheme) to operate when required 13. Operation, partial operation, or misoperation of a fully redundant Special Protection System (or Remedial Action Scheme) in response to an event or abnormal system condition for which it was not intended to operate 14. Impact of severe power swings or oscillations from Disturbances in another Regional Reliability Organization.	Evaluate for risks and consequences. ▪ May involve substantial loss of customer Demand and generation in a widespread area or areas. ▪ Portions or all of the interconnected systems may or may not achieve a new, stable operating point. ▪ Evaluation of these events may require joint studies with neighboring systems.

a) Applicable rating refers to the applicable Normal and Emergency facility thermal Rating or system voltage limit as determined and consistently applied by the system or facility owner. Applicable Ratings may include Emergency Ratings applicable for short durations as required to permit operating steps necessary to maintain system control. All Ratings must be established consistent with applicable NERC Reliability Standards addressing Facility Ratings.

b) Planned or controlled interruption of electric supply to radial customers or some local Network customers, connected to or supplied by the Faulted element or by the affected area, may occur in certain areas without impacting the overall reliability of the interconnected transmission systems. To prepare for the next contingency, system adjustments are permitted, including curtailments of contracted Firm (non-recallable reserved) electric power Transfers.

c) Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted Firm (non-recallable reserved) electric power Transfers may be necessary to maintain the overall reliability of the interconnected transmission systems.

d) A number of extreme contingencies that are listed under Category D and judged to be critical by the transmission planning entity(ies) will be selected for evaluation. It is not expected that all possible facility outages under each listed contingency of Category D will be evaluated.

e) Normal clearing is when the protection system operates as designed and the Fault is cleared in the time normally expected with proper functioning of the installed protection systems. Delayed clearing of a Fault is due to failure of any protection system component such as a relay, circuit breaker, or current transformer, and not because of an intentional design delay.

f) System assessments may exclude these events where multiple circuit towers are used over short distances (e.g., station entrance, river crossings) in accordance with Regional exemption criteria.

A. Introduction

1. **Title:** **System Performance Following Loss of a Single Bulk Electric System Element (Category B)**

2. **Number:** TPL-002-0

3. **Purpose:** System simulations and associated assessments are needed periodically to ensure that reliable systems are developed that meet specified performance requirements with sufficient lead time, and continue to be modified or upgraded as necessary to meet present and future system needs.

4. **Applicability:**

   4.1. Planning Authority

   4.2. Transmission Planner

5. **Effective Date:** April 1, 2005

B. Requirements

R1. The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that the Network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand levels over the range of forecast system demands, under the contingency conditions as defined in Category B of Table I. To be valid, the Planning Authority and Transmission Planner assessments shall:

R1.1. Be made annually.

R1.2. Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.

R1.3. Be supported by a current or past study and/or system simulation testing that addresses each of the following categories,, showing system performance following Category B of Table 1 (single contingencies). The specific elements selected (from each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).

R1.3.1. Be performed and evaluated only for those Category B contingencies that would produce the more severe System results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.

R1.3.2. Cover critical system conditions and study years as deemed appropriate by the responsible entity.

R1.3.3. Be conducted annually unless changes to system conditions do not warrant such analyses.

R1.3.4. Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.

R1.3.5. Have all projected firm transfers modeled.

R1.3.6. Be performed and evaluated for selected demand levels over the range of forecast system Demands.

R1.3.7. Demonstrate that system performance meets Category B contingencies.

R1.3.8. Include existing and planned facilities.

R1.3.9. Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.

R1.3.10. Include the effects of existing and planned protection systems, including any backup or redundant systems.

R1.3.11. Include the effects of existing and planned control devices.

R1.3.12. Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those demand levels for which planned (including maintenance) outages are performed.

R1.4. Address any planned upgrades needed to meet the performance requirements of Category B of Table I.

R1.5. Consider all contingencies applicable to Category B.

R2. When System simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-002-0_R1, the Planning Authority and Transmission Planner shall each:

R2.1. Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:

R2.1.1. Including a schedule for implementation.

R2.1.2. Including a discussion of expected required in-service dates of facilities.

R2.1.3. Consider lead times necessary to implement plans.

R2.2. Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed implementation plans are not needed.

R3. The Planning Authority and Transmission Planner shall each document the results of its Reliability Assessments and corrective plans and shall annually provide the results to its respective Regional Reliability Organization(s), as required by the Regional Reliability Organization.

C. Measures

M1. The Planning Authority and Transmission Planner shall have a valid assessment and corrective plans as specified in Reliability Standard TPL-002-0_R1 and TPL-002-0_R2.

M2. The Planning Authority and Transmission Planner shall have evidence it reported documentation of results of its reliability assessments and corrective plans per Reliability Standard TPL-002-0_R3.

D. Compliance

1. **Compliance Monitoring Process**

   1.1. **Compliance Monitoring Responsibility**

   Compliance Monitor: Regional Reliability Organizations.
   Each Compliance Monitor shall report compliance and violations to NERC via the NERC Compliance Reporting Process.

   1.2. **Compliance Monitoring Period and Reset Timeframe**

   Annually.

   1.3. **Data Retention**

   None specified.

   1.4. **Additional Compliance Information**

   None.

2. **Levels of Non-Compliance**

   2.1. **Level 1:** Not applicable.

   2.2. **Level 2:** A valid assessment and corrective plan for the longer-term planning horizon is not available.

   2.3. **Level 3:** Not applicable.

   2.4. **Level 4:** A valid assessment and corrective plan for the near-term planning horizon is not available.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New

Table I. Transmission System Standards — Normal and Emergency Conditions

Category	Contingencies	System Limits or Impacts		
	Initiating Event(s) and Contingency Element(s)	System Stable and both Thermal and Voltage Limits within Applicable Rating [a]	Loss of Demand or Curtailed Firm Transfers	Cascading Outages
A No Contingencies	All Facilities in Service	Yes	No	No
B Event resulting in the loss of a single element.	Single Line Ground (SLG) or 3-Phase (3Ø) Fault, with Normal Clearing: 1. Generator 2. Transmission Circuit 3. Transformer Loss of an Element without a Fault.	Yes Yes Yes Yes	No [b] No [b] No [b] No [b]	No No No No
	Single Pole Block, Normal Clearing[e]: 4. Single Pole (dc) Line	Yes	No[b]	No
C Event(s) resulting in the loss of two or more (multiple) elements.	SLG Fault, with Normal Clearing[e]: 1. Bus Section	Yes	Planned/ Controlled[c]	No
	2. Breaker (failure or internal Fault)	Yes	Planned/ Controlled[c]	No
	SLG or 3Ø Fault, with Normal Clearing[e], Manual System Adjustments, followed by another SLG or 3Ø Fault, with Normal Clearing[e]: 3. Category B (B1, B2, B3, or B4) contingency, manual system adjustments, followed by another Category B (B1, B2, B3, or B4) contingency	Yes	Planned/ Controlled[c]	No
	Bipolar Block, with Normal Clearing[e]: 4. Bipolar (dc) Line Fault (non 3Ø), with Normal Clearing[e]:	Yes	Planned/ Controlled[c]	No
	5. Any two circuits of a multiple circuit towerline[f]	Yes	Planned/ Controlled[c]	No
	SLG Fault, with Delayed Clearing[e] (stuck breaker or protection system failure): 6. Generator	Yes	Planned/ Controlled[c]	No
	7. Transformer	Yes	Planned/ Controlled[c]	No
	8. Transmission Circuit	Yes	Planned/ Controlled[c]	No
	9. Bus Section	Yes	Planned/ Controlled[c]	No

D [d] Extreme event resulting in two or more (multiple) elements removed or Cascading out of service	3Ø Fault, with Delayed Clearing[e] (stuck breaker or protection system failure): 1. Generator 2. Transmission Circuit 3. Transformer 4. Bus Section 3Ø Fault, with Normal Clearing[e]: 5. Breaker (failure or internal Fault) 6. Loss of towerline with three or more circuits 7. All transmission lines on a common right-of way 8. Loss of a substation (one voltage level plus transformers) 9. Loss of a switching station (one voltage level plus transformers) 10. Loss of all generating units at a station 11. Loss of a large Load or major Load center 12. Failure of a fully redundant Special Protection System (or remedial action scheme) to operate when required 13. Operation, partial operation, or misoperation of a fully redundant Special Protection System (or Remedial Action Scheme) in response to an event or abnormal system condition for which it was not intended to operate 14. Impact of severe power swings or oscillations from Disturbances in another Regional Reliability Organization.	Evaluate for risks and consequences. ▪ May involve substantial loss of customer Demand and generation in a widespread area or areas. ▪ Portions or all of the interconnected systems may or may not achieve a new, stable operating point. ▪ Evaluation of these events may require joint studies with neighboring systems.

a) Applicable rating refers to the applicable Normal and Emergency facility thermal Rating or system voltage limit as determined and consistently applied by the system or facility owner. Applicable Ratings may include Emergency Ratings applicable for short durations as required to permit operating steps necessary to maintain system control. All Ratings must be established consistent with applicable NERC Reliability Standards addressing Facility Ratings.

b) Planned or controlled interruption of electric supply to radial customers or some local Network customers, connected to or supplied by the Faulted element or by the affected area, may occur in certain areas without impacting the overall reliability of the interconnected transmission systems. To prepare for the next contingency, system adjustments are permitted, including curtailments of contracted Firm (non-recallable reserved) electric power Transfers.

c) Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted Firm (non-recallable reserved) electric power Transfers may be necessary to maintain the overall reliability of the interconnected transmission systems.

d) A number of extreme contingencies that are listed under Category D and judged to be critical by the transmission planning entity(ies) will be selected for evaluation. It is not expected that all possible facility outages under each listed contingency of Category D will be evaluated.

e) Normal clearing is when the protection system operates as designed and the Fault is cleared in the time normally expected with proper functioning of the installed protection systems. Delayed clearing of a Fault is due to failure of any protection system component such as a relay, circuit breaker, or current transformer, and not because of an intentional design delay.

f) System assessments may exclude these events where multiple circuit towers are used over short distances (e.g., station entrance, river crossings) in accordance with Regional exemption criteria.

A. Introduction

1. **Title:** **System Performance Following Loss of Two or More Bulk Electric System Elements (Category C)**

2. **Number:** TPL-003-0

3. **Purpose:** System simulations and associated assessments are needed periodically to ensure that reliable systems are developed that meet specified performance requirements, with sufficient lead time and continue to be modified or upgraded as necessary to meet present and future System needs.

4. **Applicability:**

   4.1. Planning Authority

   4.2. Transmission Planner

5. **Effective Date:** April 1, 2005

B. Requirements

R1. The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission systems is planned such that the network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand Levels over the range of forecast system demands, under the contingency conditions as defined in Category C of Table I (attached). The controlled interruption of customer Demand, the planned removal of generators, or the Curtailment of firm (non-recallable reserved) power transfers may be necessary to meet this standard. To be valid, the Planning Authority and Transmission Planner assessments shall:

R1.1. Be made annually.

R1.2. Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.

R1.3. Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category C of Table 1 (multiple contingencies). The specific elements selected (from each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).

R1.3.1. Be performed and evaluated only for those Category C contingencies that would produce the more severe system results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.

R1.3.2. Cover critical system conditions and study years as deemed appropriate by the responsible entity.

R1.3.3. Be conducted annually unless changes to system conditions do not warrant such analyses.

R1.3.4. Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.

R1.3.5. Have all projected firm transfers modeled.

R1.3.6. Be performed and evaluated for selected demand levels over the range of forecast system demands.

R1.3.7. Demonstrate that System performance meets Table 1 for Category C contingencies.

R1.3.8. Include existing and planned facilities.

R1.3.9. Include Reactive Power resources to ensure that adequate reactive resources are available to meet System performance.

R1.3.10. Include the effects of existing and planned protection systems, including any backup or redundant systems.

R1.3.11. Include the effects of existing and planned control devices.

R1.3.12. Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those Demand levels for which planned (including maintenance) outages are performed.

R1.4. Address any planned upgrades needed to meet the performance requirements of Category C.

R1.5. Consider all contingencies applicable to Category C.

R2. When system simulations indicate an inability of the systems to respond as prescribed in Reliability Standard TPL-003-0_R1, the Planning Authority and Transmission Planner shall each:

R2.1. Provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon:

R2.1.1. Including a schedule for implementation.

R2.1.2. Including a discussion of expected required in-service dates of facilities.

R2.1.3. Consider lead times necessary to implement plans.

R2.2. Review, in subsequent annual assessments, (where sufficient lead time exists), the continuing need for identified system facilities. Detailed implementation plans are not needed.

R3. The Planning Authority and Transmission Planner shall each document the results of these Reliability Assessments and corrective plans and shall annually provide these to its respective NERC Regional Reliability Organization(s), as required by the Regional Reliability Organization.

C. Measures

M1. The Planning Authority and Transmission Planner shall have a valid assessment and corrective plans as specified in Reliability Standard TPL-003-0_R1 and TPL-003-0_R2.

M2. The Planning Authority and Transmission Planner shall have evidence it reported documentation of results of its reliability assessments and corrective plans per Reliability Standard TPL-003-0_R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Compliance Monitor: Regional Reliability Organizations.

1.2. Compliance Monitoring Period and Reset Timeframe

Annually.

1.3. Data Retention

None specified.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance

2.1. Level 1: Not applicable.

2.2. Level 2: A valid assessment and corrective plan for the longer-term planning horizon is not available.

2.3. Level 3: Not applicable.

2.4. Level 4: A valid assessment and corrective plan for the near-term planning horizon is not available.

E. Regional Differences

1. None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	April 1, 2005	Add parenthesis to item "e" on page 8.	Errata

Table I. Transmission System Standards – Normal and Emergency Conditions

Category	Contingencies	System Limits or Impacts		
	Initiating Event(s) and Contingency Element(s)	System Stable and both Thermal and Voltage Limits within Applicable Rating [a]	Loss of Demand or Curtailed Firm Transfers	Cascading [c] Outages
A No Contingencies	All Facilities in Service	Yes	No	No
B Event resulting in the loss of a single element.	Single Line Ground (SLG) or 3-Phase (3Ø) Fault, with Normal Clearing: 1. Generator 2. Transmission Circuit 3. Transformer Loss of an Element without a Fault.	Yes Yes Yes Yes	No [b] No [b] No [b] No [b]	No No No No
	Single Pole Block, Normal Clearing [e]: 4. Single Pole (dc) Line	Yes	No [b]	No
C Event(s) resulting in the loss of two or more (multiple) elements.	SLG Fault, with Normal Clearing [e]: 1. Bus Section 2. Breaker (failure or internal Fault)	Yes Yes	Planned/ Controlled [c] Planned/ Controlled [c]	No No
	SLG or 3Ø Fault, with Normal Clearing [e], Manual System Adjustments, followed by another SLG or 3Ø Fault, with Normal Clearing [e]: 3. Category B (B1, B2, B3, or B4) contingency, manual system adjustments, followed by another Category B (B1, B2, B3, or B4) contingency	Yes	Planned/ Controlled [c]	No
	Bipolar Block, with Normal Clearing [e]: 4. Bipolar (dc) Line Fault (non 3Ø), with Normal Clearing [e]: 5. Any two circuits of a multiple circuit towerline [f]	Yes Yes	Planned/ Controlled [c] Planned/ Controlled [c]	No No
	SLG Fault, with Delayed Clearing [e] (stuck breaker or protection system failure): 6. Generator 7. Transformer 8. Transmission Circuit 9. Bus Section	Yes Yes Yes Yes	Planned/ Controlled [c] Planned/ Controlled [c] Planned/ Controlled [c] Planned/ Controlled [c]	No No No No

D [d] Extreme event resulting in two or more (multiple) elements removed or Cascading out of service	3Ø Fault, with Delayed Clearing [e] (stuck breaker or protection system failure): 1. Generator 2. Transmission Circuit 3. Transformer 4. Bus Section 3Ø Fault, with Normal Clearing [e]: 5. Breaker (failure or internal Fault) 6. Loss of towerline with three or more circuits 7. All transmission lines on a common right-of way 8. Loss of a substation (one voltage level plus transformers) 9. Loss of a switching station (one voltage level plus transformers) 10. Loss of all generating units at a station 11. Loss of a large Load or major Load center 12. Failure of a fully redundant Special Protection System (or remedial action scheme) to operate when required 13. Operation, partial operation, or misoperation of a fully redundant Special Protection System (or Remedial Action Scheme) in response to an event or abnormal system condition for which it was not intended to operate 14. Impact of severe power swings or oscillations from Disturbances in another Regional Reliability Organization.	Evaluate for risks and consequences. ▪ May involve substantial loss of customer Demand and generation in a widespread area or areas. ▪ Portions or all of the interconnected systems may or may not achieve a new, stable operating point. ▪ Evaluation of these events may require joint studies with neighboring systems.

a) Applicable rating refers to the applicable Normal and Emergency facility thermal Rating or system voltage limit as determined and consistently applied by the system or facility owner. Applicable Ratings may include Emergency Ratings applicable for short durations as required to permit operating steps necessary to maintain system control. All Ratings must be established consistent with applicable NERC Reliability Standards addressing Facility Ratings.

b) Planned or controlled interruption of electric supply to radial customers or some local Network customers, connected to or supplied by the Faulted element or by the affected area, may occur in certain areas without impacting the overall reliability of the interconnected transmission systems. To prepare for the next contingency, system adjustments are permitted, including curtailments of contracted Firm (non-recallable reserved) electric power Transfers.

c) Depending on system design and expected system impacts, the controlled interruption of electric supply to customers (load shedding), the planned removal from service of certain generators, and/or the curtailment of contracted Firm (non-recallable reserved) electric power transfers may be necessary to maintain the overall reliability of the interconnected transmission systems.

d) A number of extreme contingencies that are listed under Category D and judged to be critical by the transmission planning entity(ies) will be selected for evaluation. It is not expected that all possible facility outages under each listed contingency of Category D will be evaluated.

e) Normal clearing is when the protection system operates as designed and the Fault is cleared in the time normally expected with proper functioning of the installed protection systems. Delayed clearing of a Fault is due to failure of any protection system component such as a relay, circuit breaker, or current transformer, and not because of an intentional design delay.

f) System assessments may exclude these events where multiple circuit towers are used over short distances (e.g., station entrance, river crossings) in accordance with Regional exemption criteria.

NPCC Document A-2

NORTHEAST POWER COORDINATING COUNCIL

1515 BROADWAY, NEW YORK, NY 10036-8901 TELEPHONE: (212) 840-1070 FAX: (212) 302-2782

Basic Criteria for Design and Operation Of Interconnected Power Systems

Adopted by the Members of the Northeast Power Coordinating Council September 20, 1967, based on recommendation by the Operating Procedure Coordinating Committee and the System Design Coordinating Committee, in accordance with paragraph IV, subheading (a), of NPCC's Memorandum of Agreement dated January 19, 1966 as amended to date.

Revised:	July 31, 1970
Revised:	June 6, 1975
Revised:	May 14, 1980
Revised:	March 2, 1984
Revised:	October 26, 1990
Revised:	August 9, 1995
Revised:	May 6, 2004

1.0 Introduction

The objective of these criteria is to provide a "design-based approach" to ensure the **bulk power system** is designed and operated to a level of reliability such that the loss of a major portion of the system, or unintentional separation of a major portion of the system, will not result from any design **contingencies** referenced in Sections 5.1 and 5.2. In NPCC the technique for assuring the reliability of the **bulk power system** is to require that it be designed and operated to withstand representative **contingencies** as specified in these criteria. Analyses of simulations of these **contingencies** include assessment of the potential for widespread cascading outages due to overloads, instability or voltage collapse. Loss of small portions of a system (such as radial portions) may be tolerated provided these do not jeopardize the reliability of the remaining **bulk power system**. (Terms in bold typeface are defined in the Glossary located in Document A-7, the *NPCC Glossary of Terms*).

Criteria described in this document are to be used in the design and operation of the **bulk power system.** These criteria meet or exceed the North American Electric Reliability Council (NERC) policies and standards. These criteria are applicable to all entities which are part of or make use of the **bulk power system.** The Council member whose system is used to connect a non-member system to the **bulk power system** shall assure that, whenever it enters into arrangements or contractual agreements with non-members whose system could have a **significant adverse impact** on service reliability on the interconnected **bulk power system** in Northeastern North America, the terms of such arrangements or contractual agreements are consistent with criteria established by the Council, NERC, or the Regional Reliability Councils established in areas in which the facilities used for such arrangements are located.

The characteristics of a reliable **bulk power system** include adequate **resources** and transmission to reliably meet projected customer electricity demand and energy requirements as prescribed in this document and include:

a. Consideration of a balanced relationship among the fuel type, capacity, physical characteristics (peaking/baseload/etc.), and location of **resources**.

b. Consideration of a balanced relationship among transmission system **elements** to avoid excessive dependence on any one transmission circuit, structure, right-of-way, or substation.

c. Transmission systems should provide flexibility in switching arrangements, voltage control, and other control measures.

It is the responsibility of each **Area** to ascertain that its portion of the **bulk power system** is designed and operated in conformance with these criteria. The Council provides a forum for coordinating the design and operations of its five **Areas.**

Through committees, task forces, and working groups the Council shall conduct regional and interregional studies, and assess and monitor **Area** studies and operations to assure conformance to the criteria.

2.0 General Requirements

Area, Member system or local conditions may require criteria which are more stringent than those set out herein. Any constraints imposed by these more stringent criteria will be observed. It is also recognized that the Basic Criteria are not necessarily applicable to those **elements** that are not a part of the **bulk power system** or in the portions of a member system where instability or overloads will not jeopardize the reliability of the remaining **bulk power system.**

2.1 Design Criteria

The design criteria will be used in the assessment of the **bulk power system** of each of the NPCC member systems and each NPCC **Area**, and in the reliability testing at the member system, **Area**, and Regional Council levels.

Design studies shall assume power flow conditions utilizing transfers, load and generation conditions which stress the system. Transfer capability studies shall be based on the load and generation conditions expected to exist for the period under study. All reclosing facilities shall be assumed in service unless it is known that such facilities will be rendered inoperative.

A **special protection system (SPS)** shall be used judiciously and when employed, shall be installed, consistent with good system design and operating policy.

A SPS may be used to provide protection for infrequent contingencies, or for temporary conditions that may exist such as project delays, unusual

combinations of system demand and equipment outages or availability, or specific equipment maintenance outages. An **SPS** may also be applied to preserve system integrity in the event of **severe facility outages** and extreme **contingencies.** The decision to employ an **SPS** shall take into account the complexity of the scheme and the consequences of correct or incorrect operation as well as its benefits.

The requirements of **special protection systems** are defined in the NPCC *Bulk Power System Protection Criteria*, (Document A-5), and the *Special Protection System Criteria*, (Document A-11).

2.2 Operating Criteria

Coordination among and within the **Areas** of NPCC is essential to the reliability of interconnected operations. Timely information concerning system conditions shall be transmitted by the NPCC **Areas** to other NPCC **Areas** or systems as needed to assure reliable operation of the **bulk power system**.

The operating criteria represent the application of the design criteria to inter-**Area**, intra-**Area** (inter-system) and intra-system operation.

The operating criteria define the minimum level of reliability that shall apply to inter-**Area** operation. Where inter-**Area** reliability is affected, each **Area** shall establish limits and operate so that the **contingencies** stated in Section 6.1 and 6.2 can be withstood without causing a **significant adverse impact** on other **Areas**.

When adequate **bulk power system** facilities are not available, **special protection systems** (SPS) may be employed to maintain system security. Two categories of transmission transfer capabilities, normal and emergency, are applicable. Normal transfer capabilities are to be observed unless an **emergency** is declared.

2.3 System Analysis and Modeling Data Exchange Requirements

It is the responsibility of NPCC, its **Areas** and NPCC Members to protect the proprietary nature of the following information and to ensure it is used only for purposes of efficient and reliable system operation and design. Also, any sharing of such information must not violate anti-trust laws.

For reliability purposes, **Areas** shall share and coordinate forecast system information and real time information to enable and enhance the analysis

and modeling of the interconnected **bulk power system** by security application software on energy management systems. Each member within an NPCC **Area** shall provide needed information to its **Area** representative as required. Analysis and modeling of the interconnected power system is required for reliable design and operation. Data needed to analyze and model the electric system and its component facilities must be developed, maintained, and made available for use in interconnected operating and planning studies, including data for fault level analysis.

Areas and member systems shall maintain and submit, as needed, data in accordance with applicable NPCC Procedures.

Data submitted for analysis representing physical or control characteristics of equipment shall be verified through appropriate methods. System analysis and modeling data must be reviewed annually, and verified on a periodic basis. Generation equipment, and its component controllers, shall be tested to verify data.

Areas shall install dynamic recording devices and provide recorded data necessary to enhance analysis of wide area system disturbances and validate system simulation models. These devices should be time synchronized and should have sufficient data storage to permit a few minutes of data to be collected. Information provided by these recordings would be used in tandem, when appropriate, with shorter time scale readings from fault recorders and sequence of events recorders (SER), as described in the *Bulk Power System Protection Criteria* (Document A-5), paragraph 2.7.2.

3.0 Resource Adequacy - Design Criteria

Each **Area's** probability (or risk) of disconnecting any **firm load** due to resource deficiencies shall be, on average, not more than once in ten years. Compliance with this criteria shall be evaluated probabilistically, such that the **loss of load expectation** [**LOLE**] of disconnecting **firm load** due to resource deficiencies shall be, on average, no more than 0.1 day per year. This evaluation shall make due allowance for demand uncertainty, scheduled outages and deratings, forced outages and deratings, assistance over interconnections with neighboring **Areas** and **Regions**, transmission transfer capabilities, and capacity and/or load relief from available operating procedures.

4.0 Resource Adequacy - Operating Criteria

Each **Area** shall have procedures in place to schedule outages and deratings of **resources** in such a manner that the available **resources** will be adequate to meet the **Area**'s forecasted load and reserve requirements, in accordance with the NPCC *Operating Reserve Criteria* (Document A-6).

For consistent evaluation and reporting of **resource** adequacy, it is necessary to measure the net capability of generating units and loads utilized as a **resource** of each Area on a regular basis.

5.0 Transmission Design Criteria

The portion of the **bulk power system** in each **Area** and of each member system shall be designed with sufficient transmission capability to serve forecasted loads under the conditions noted in Sections 5.1 and 5.2. These criteria will also apply after any critical generator, transmission circuit, transformer, series or shunt compensating device or HVdc pole has already been lost, assuming that the **Area** generation and power flows are adjusted between outages by the use of **ten-minute reserve** and where available, phase angle regulator control and HVdc control.

Anticipated transfers of power from one **Area** to another, as well as within **Areas**, shall be considered in the design of inter-**Area** and intra-**Area** transmission facilities. Transmission transfer capabilities shall be determined in accordance with the conditions noted in Sections 5.1 and 5.2.

5.1 Stability Assessment

Stability of the **bulk power system** shall be maintained during and following the most severe of the **contingencies** stated below, **with due regard to reclosing**. For each of the **contingencies** below that involves a fault, stability shall be maintained when the simulation is based on **fault clearing** initiated by the **"system A" protection group**, and also shall be maintained when the simulation is based on **fault clearing** initiated by the **"system B" protection group**.

a. A permanent three-phase fault on any generator, transmission circuit, transformer or bus section with **normal fault clearing**.

b. Simultaneous permanent phase to ground faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with **normal fault clearing**. If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded. Other similar situations can be excluded on the basis of acceptable risk, provided that the Reliability Coordinating Committee specifically accepts each request for exclusion.

c. A permanent phase to ground fault on any transmission circuit, transformer, or bus section with **delayed fault clearing.**

d. Loss of any **element** without a fault.

e. A permanent phase to ground fault on a circuit breaker with **normal fault clearing. (Normal fault clearing** time for this condition may not always be high speed.)

f. Simultaneous permanent loss of both poles of a direct current bipolar facility without an ac fault

g. The failure of a circuit breaker to operate when initiated by an SPS following: loss of any **element** without a fault; or a permanent phase to ground fault, with **normal fault clearing,** on any transmission circuit, transformer or bus section.

5.2 Steady State Assessment

a. Each **Area** shall design its system in accordance with these criteria and its own voltage control procedures and criteria, and coordinate these with adjacent **Areas** and **control areas.** Adequate reactive power resources and appropriate controls shall be installed in each **Area** to maintain voltages within normal limits for predisturbance conditions, and within **applicable emergency limits** for the system conditions that exist following the **contingencies** specified in 5.1.

b. Line and equipment loadings shall be within normal limits for predisturbance conditions and within **applicable emergency limits** for the system conditions that exist following the **contingencies** specified in 5.1.

5.3 Fault Current Assessment

Each **Area** shall establish procedures and implement a system design that ensures equipment capabilities are adequate for fault current levels with all transmission and generation facilities in service for all potential operating conditions, and coordinate these procedures with adjacent **Areas** and **Regions**.

6.0 Transmission Operating Criteria

Scheduled outages of facilities that affect inter-**Area** reliability shall be coordinated sufficiently in advance of the outage to permit the affected **Areas** to maintain reliability. Each **Area** shall notify adjacent **Areas** of scheduled or forced outages of any facility on the NPCC Transmission Facilities Notification List and of any other condition which may impact on inter-**Area** reliability. Work on facilities which impact inter-**Area** reliability shall be expedited.

Individual **Areas** shall be operated in a manner such that the **contingencies** noted in Section 6.1 and 6.2 can be sustained and do not adversely affect other **Areas**.

Appropriate adjustments shall be made to **Area** operations to accommodate the impact of **protection group** outages, including the outage of a **protection group** which is part of a Type I **special protection system**. For typical periods of forced outage or maintenance of a **protection group**, it can be assumed, unless there are indications to the contrary, that the remaining **protection** will function as designed. If the **protection group** will be out of service for an extended period of time, additional adjustments to operations may be appropriate considering other system conditions and the consequences of possible failure of the remaining **protection group**.

6.1 Normal Transfers

Pre-**contingency** voltages, line and equipment loadings shall be within normal limits. Unless specific instructions describing alternate action are in effect, normal transfers shall be such that manual reclosing of a faulted **element** can be carried out before any manual system adjustment, without affecting the stability of the **bulk power system**.

Stability of the **bulk power system** shall be maintained during and following the most severe of the **contingencies** stated below, **with due regard to reclosing.** For each of the **contingencies** stated below that involves a fault, stability shall be maintained when the simulation is based on **fault clearing** initiated by the **"system A" protection group**, and also shall be maintained when the simulation is based on **fault clearing** initiated by the **"system B" protection group**.

a. A permanent three-phase fault on any generator, transmission circuit, transformer or bus section, with **normal fault clearing.**

b. Simultaneous permanent phase to ground faults on different phases of each of two adjacent transmission circuits on a multiple circuit tower, with **normal fault clearing.** If multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded. Other similar situations can be excluded on the basis of acceptable risk, provided that the Reliability Coordinating Committee specifically accepts each request for exclusion.

c. A permanent phase to ground fault on any transmission circuit, transformer, or bus section with **delayed fault clearing**.

d. Loss of any **element** without a fault.

e. A permanent phase to ground fault on a circuit breaker, with **normal fault clearing. (Normal fault clearing** time for this condition may not always be high speed.)

f. Simultaneous permanent loss of both poles of a direct current bipolar facility without an ac fault.

g. The failure of a circuit breaker to operate when initiated by an SPS following: loss of any **element** without a fault; or a permanent phase to ground fault, with **normal fault clearing**, on any transmission circuit, transformer or bus section.

Reactive power resources shall be maintained in each **Area** in order to maintain voltages within normal limits for predisturbance conditions, and within **applicable emergency limits** for the system conditions that exist following the **contingencies** specified in the foregoing. Adjoining **Areas** shall mutually agree upon procedures of inter-Area voltage control.

Line and equipment loadings shall be within normal limits for predisturbance conditions and within **applicable emergency limits** for the system conditions that exist following the **contingencies** specified in the foregoing.

Since **contingencies** b, c, e, f, and g, are not confined to the loss of a single **element**, individual **Areas** may choose to permit a higher post **contingency** flow on remaining facilities than for **contingencies** a and d. This is permissible providing operating procedures are documented to accomplish corrective actions, the loadings are sustainable for at least the anticipated time required to effect such action, and other **Areas** will not be subjected to the higher flows without prior agreement.

6.2 Emergency Transfers

When **firm load** cannot be supplied within normal limits in an **Area**, or a portion of an **Area**, transfers may be increased to the point where pre-**contingency** voltages, line and equipment loadings are within **applicable emergency limits**. Emergency transfer levels may require generation adjustment before manually reclosing faulted **elements**.

Stability of the **bulk power system** shall be maintained during and following the most severe of the following **contingencies**, and **with due regard to reclosing**:

a. A permanent three-phase fault on any generator, transmission circuit, transformer or bus section, with **normal fault clearing**.

b. The loss of any **element** without a fault.

Immediately following the most severe of these **contingencies**, voltages, line and equipment loadings will be within **applicable emergency limits**.

6.3 Post Contingency Operation

Immediately after the occurrence of a **contingency**, the status of the **bulk power system** must be assessed and transfer levels must be adjusted, if necessary, to prepare for the next **contingency**. If the readjustment of generation, load resources, phase angle regulators, and direct current facilities, is not adequate to restore the system to a secure state, then other measures such as voltage reduction and shedding of firm load may be required. System adjustments shall be completed as quickly as possible, but in all cases within 30 minutes after the occurrence of the **contingency**.

Voltage reduction need not be initiated and firm load need not be shed to observe a post **contingency** loading requirement until the **contingency** occurs, provided that adequate response time for this action is available after the **contingency** occurs and other measures will maintain post **contingency** loadings within **applicable emergency limits**.

Emergency measures, including the pre-contingency disconnection of **firm load** if necessary, must be implemented to limit transfers to within the requirements of 6.2 above.

6.4 Operation Under High Risk Conditions

Operating to the **contingencies** listed in Sections 6.1 and 6.2 is considered to provide an acceptable level of **bulk power system** security. Under certain unusual conditions, such as severe weather, the expectation of occurrence of some **contingencies**, and the associated consequences, may be judged to be temporarily, but significantly, greater than the long-term average expectation. When these conditions, referred to as high risk conditions, are judged to exist in an **Area**, consideration should be given to operating in a more conservative manner than that required by the provisions of Sections 6.1 and 6.2.

7.0 Extreme Contingency Assessment

Extreme **contingency** assessment recognizes that the **bulk power system** can be subjected to events which exceed, in severity, the **contingencies** listed in Section 5.1. One of the objectives of extreme **contingency** assessment is to determine, through planning studies, the effects of extreme **contingencies** on system performance. This is done in order to obtain an indication of system strength, or to determine the extent of a

widespread system disturbance, even though extreme **contingencies** do have low probabilities of occurrence.

The specified extreme **contingencies** listed below are intended to serve as a means of identifying some of those particular situations that could result in widespread **bulk power system** shutdown. It is the responsibility of each **Area** to identify additional extreme contingencies, if any, to be assessed.

Assessment of the extreme **contingencies** listed below shall examine post **contingency** steady state conditions, as well as stability, overload cascading and voltage collapse. Pre-**contingency** load flows chosen for analysis shall reflect reasonable power transfer conditions within **Areas**, or from **Area** to **Area**

Analytical studies shall be conducted to determine the effect of the following extreme **contingencies**:

a. Loss of the entire capability of a generating station.

b. Loss of all transmission circuits emanating from a generating station, switching station, dc terminal or substation

c. Loss of all transmission circuits on a common right-of-way.

d. Permanent three-phase fault on any generator, transmission circuit, transformer, or bus section, with **delayed fault clearing** and **with due regard to reclosing**.

e. The sudden dropping of a large load or major load center.

f. The effect of severe power swings arising from disturbances outside the Council's interconnected systems.

g. Failure of a **special protection system**, to operate when required following the normal **contingencies** listed in Section 5.1.

h. The operation or partial operation of a special protection system for an event or condition for which it was not intended to operate.

i. Sudden loss of fuel delivery system to multiple plants, (i.e. gas pipeline contingencies, including both gas transmission lines and gas mains.)

Note: The requirement of this section is to perform extreme contingency assessments. In the case where extreme contingency assessment concludes there are serious consequences, an evaluation of implementing a change to design or operating practices to address such contingencies must be conducted, and measures may be utilized where appropriate to reduce the likelihood of such contingencies or to mitigate the consequences indicated in the assessment of such contingencies.

8.0 Extreme System Conditions Assessment

The **bulk power system** can be subjected to wide range of other than normal system conditions that have low probability of occurrence. One of the objectives of extreme system conditions assessment is to determine, through planning studies, the impact of these conditions on expected steady-state and dynamic system performance. This is done in order to obtain an indication of system robustness or to determine the extent of a widespread adverse system response. Each **Area** has the responsibility to incorporate special simulation testing to assess the impact of extreme system conditions.

For example, analytical studies shall be conducted to determine the effect of design contingencies under the following extreme conditions:

a. Peak load conditions resulting from extreme weather conditions with applicable rating of electrical elements.

b. Generating unit(s) fuel shortage, (i.e. gas supply adequacy)

After due assessment of extreme system conditions, measures may be utilized, where appropriate, to mitigate the consequences that are indicated as a result of testing for such system conditions.

Lead Task Force:	Task Force on Coordination of Planning
Reviewed for concurrence by:	TFCO, TFSP, TFSS and TFIST Chairman
Review frequency:	4 years
References:	*Bulk Power System Protection Criteria* (Document A-5)
	Operating Reserve Criteria (Document A-6)
	NPCC Glossary of Terms (Document A-7)
	Special Protection System Criteria (Document A-11)

Document A-5

NORTHEAST POWER COORDINATING COUNCIL, INC.
1515 BROADWAY, NEW YORK, NY 10036-8901 TELEPHONE: (212) 840-1070 FAX: (212) 302-2782

Bulk Power System Protection Criteria

Adopted by the Members of the Northeast Power Coordinating Council on May 21, 2007 based on recommendation by the Reliability Coordinating Committee, in accordance with paragraph VIII, subheading (a), of NPCC Bylaws dated May 18, 2006 as amended to date.

Revised: February 29, 1980
Revised: May 9, 1983
Revised: February 2, 1987
Revised: June 9, 1989
Revised: October 26, 1990
Revised: August 9, 1995
Revised: September, 1998
Revised: November 14, 2002
Revised: January 30, 2006
Revised: May 21, 2007

Document A-5

TABLE OF CONTENTS

1.0 INTRODUCTION 1

1.1 APPLICABILITY 1

1.1.1 New Facilities 1

1.1.2 Existing Facilities 1

1.2 RESPONSIBILITY 2

2.0 GENERAL CRITERIA 2

2.1 ISSUES AFFECTING DEPENDABILITY 2

2.4 OPERATING TIME 3

2.5 THIS SECTION IS INTENTIONALLY LEFT BLANK. 4

2.6 PROTECTION SYSTEM TESTING AND MAINTENANCE 4

2.7 ANALYSIS OF PROTECTION PERFORMANCE 4

3.0 EQUIPMENT AND DESIGN CONSIDERATIONS 4

3.1 CURRENT TRANSFORMERS 4

3.2 VOLTAGE TRANSFORMERS AND POTENTIAL DEVICES 5

3.3 THIS SECTION IS INTENTIONALLY LEFT BLANK. 6

3.4 THIS SECTION IS INTENTIONALLY LEFT BLANK. 6

3.5 BATTERIES AND DIRECT CURRENT (DC) SUPPLY 6

3.6 STATION SERVICE AC SUPPLY 7

3.7 CIRCUIT BREAKERS 7

3.8 TELEPROTECTION 7

3.9 THIS SECTION IS INTENTIONALLY LEFT BLANK. 8

3.10 ENVIRONMENT 8

3.11 GROUNDING 8

4.0 SPECIFIC APPLICATION CONSIDERATIONS 8

4.1 TRANSMISSION LINE PROTECTION 8

4.2 THIS SECTION IS INTENTIONALLY LEFT BLANK. 8

4.3 BREAKER FAILURE PROTECTION 8

4.4 GENERATING STATION PROTECTION 9

4.5 AUTOMATIC UNDERFREQUENCY LOAD SHEDDING PROTECTION SYSTEMS 9

4.6 HVDC SYSTEMS PROTECTION 9

4.7 THIS SECTION IS INTENTIONALLY LEFT BLANK. 9

4.8 THIS SECTION IS INTENTIONALLY LEFT BLANK. 9

5.0 REPORTING OF PROTECTION SYSTEMS 10

Document A-5

Note:

Terms in bold typeface are defined in the *NPCC Glossary of Terms* (Document A-7)

1.0 Introduction

This document establishes the **protection** criteria, for **protection** of the NPCC **bulk power system**. It is not a design specification. It is recognized that certain **Areas** or member systems may choose to apply more rigid criteria because of local considerations. Guidance for consideration in the implementation of these criteria is provided in Document B-5.

Compliance with these criteria will be reviewed by TFSP in accordance with NPCC *Procedure for Reporting and Reviewing Proposed Protection Systems for the Bulk Power System* (Document C-22).

1.1 Applicability

1.1.1 New Facilities

These criteria shall apply to all new **Bulk Power System** facilities.

1.1.2 Existing Facilities

It is the responsibility of individual companies to assess the **protection systems** at existing facilities and to make modifications which are required to meet the intent of these criteria as follows:

1.1.2.1 Planned Renewal or Upgrade to Existing Facilities

It is recognized that there may be portions of the **bulk power system,** which existed prior to each member's adoption of the *Bulk Power System Protection Criteria* (Document A-5) that do not meet these criteria. If any **protection systems** or sub-systems of these facilities are replaced as part of a planned renewal or upgrade to the facility and do not meet all of these criteria, then an assessment shall be conducted for those criteria that are not met. The result of this assessment shall be reported on the appropriate C22 forms.

1.1.2.2 Facility Classification Upgraded to **Bulk Power System**

These criteria apply to all existing facilities which become classified as **bulk power system**. A

mitigation plan shall be required to bring such a facility into compliance with these criteria

1.1.2.3 Additions to **Bulk Power System** Facilities

If a **bulk power system element** is added to an existing **bulk power system** facility that is recognized under section 1.1.2.1, Planned Renewal or Upgrade to Existing Facilities, these criteria apply to the **protection systems** for the new **element**.

1.1.2.4 "In-kind" Replacement of **Bulk Power System** Equipment

If a **bulk power system element** (e.g., breaker, transformer, capacitor bank, reactor, etc.) or a **protective relay** is replaced "in-kind" as a result of an unplanned event, then it is not required to upgrade the associated protection system to comply with these criteria.

1.2 Responsibility

Whenever changes are anticipated in generating sources, transmission facilities, or operating conditions, members shall review those **protection system** applications (i.e., settings, ac and dc supplies) which can reasonably be expected to be impacted by those changes.

2.0 General Criteria

Due consideration shall be given to dependability and security. For those **protective relays** intended for removal of **faults** from the **bulk power system**, dependability is paramount, and the redundancy provisions of the criteria shall apply. For **Protective relays** installed for reasons other than **fault** sensing such as overload, etc., security is paramount, and the redundancy provisions of the criteria do not apply. The relative effect on the **bulk power system** of a failure of a **protection system** to operate when desired versus an unintended operation shall be weighed carefully in selecting design parameters as follows:

2.1 Issues Affecting Dependability

2.1.1 Except as identified otherwise in these criteria, all **elements** of the **bulk power system** shall be protected by two **protection**

groups, each of which is independently capable of performing the specified protective function for that **element**. This requirement also applies during energization of the **element**.

2.1.2 Except as identified otherwise in these criteria, the two **protection groups** shall not share the same component.

2.1.3 Means shall be provided to trip all necessary local and remote breakers in the event that a breaker fails to clear a **fault**. This **protection** need not be duplicated.

2.2 Issues Affecting Security

2.2.1 **Protection systems** shall be designed to isolate only the faulted **element**, except in those circumstances where additional **elements** are tripped intentionally to preserve system integrity, or where isolating additional **elements** has no impact outside the local area.

2.3 Issues Affecting Dependability and Security

2.3.1 The thermal capability of all **protection system** components shall be adequate to withstand rated maximum short time and continuous loading of the associated **protected elements**.

2.3.2 Communication link availability, critical switch positions, and trip circuit integrity, shall be monitored to allow prompt attention by appropriate operating authorities.

2.3.3 When remote access to **protection systems** is possible, the design shall include security measures to minimize the probability of unauthorized access to the **protection systems**.

2.3.4 Short Circuit Models used to assess **protection** scheme design and to develop **protection** settings shall take into account minimum and maximum fault levels and mutual effects of parallel transmission lines. Details of neighboring systems shall be modeled wherever they can affect results significantly.

2.4 Operating Time

Bulk power system protection shall take corrective action within times determined by studies with due regard to security, dependability and selectivity.

2.5 This section is intentionally left blank.

2.6 **Protection System** Testing and Maintenance

2.6.1 **Protection systems** shall be maintained in accordance with the *Maintenance Criteria for Bulk Power System Protection* (Document A-4).

2.6.2 The design of **protection systems** both in terms of circuitry and physical arrangement shall facilitate periodic testing and maintenance.

2.6.3 Each **protection group** shall be functionally tested to verify the dependability and security aspects of the design, when initially placed in service and when modifications are made.

2.7 Analysis of **Protection** Performance

2.7.1 **Bulk power system** automatic operations shall be analyzed to determine proper **protection system** performance. Corrective measures shall be taken promptly if a **protection group** fails to operate or operates incorrectly.

2.7.2 Event and fault recording capability shall be provided to permit analysis of system disturbances and **protection system** performance.

2.7.3 Internal clocks in event and **fault** recording equipment shall be time synchronized to within 2 milliseconds or less of Universal Coordinated Time scale. The time zone shall be clearly identified as either universal time zone or local time zone.

2.7.4 Each **protective relay** which trips **Bulk Power System** equipment shall provide separate target indication.

3.0 Equipment and Design Considerations

3.1 Current Transformers

Current transformers (CTs) associated with **protection systems** shall have adequate steady-state and transient characteristics for their intended function as follows:

3.1.1 The output of each current transformer secondary winding shall be designed to remain within acceptable limits for the connected burdens under all anticipated **fault** currents to ensure correct operation of the **protection system**.

3.1.2 The thermal and mechanical capabilities of the CT at the operating tap shall be adequate to prevent damage under maximum **fault** conditions and normal or **emergency** system loading conditions.

3.1.3 For **protection groups** to be independent, they shall be supplied from separate current transformer secondary windings.

3.1.4 Interconnected current transformer secondary wiring shall be grounded at only one point.

3.1.5 Current transformers shall be connected so that adjacent **protection** zones overlap.

3.2 Voltage Transformers and Potential Devices

Voltage transformers and potential devices associated with **protection systems** shall have adequate steady-state and transient characteristics for their intended functions as follows:

3.2.1 Voltage transformers and potential devices shall have adequate volt-ampere capacity to supply the connected burden while maintaining their **relay** accuracy over their specified primary voltage range.

3.2.2 The two **protection groups** protecting an **element** shall be supplied from separate voltage sources. The two **protection groups** may be supplied from separate secondary windings on one transformer or potential device, provided all of the following requirements are met:

- Complete loss of one or more phase voltages does not prevent all tripping of the protected **element**;
- Each secondary winding has sufficient capacity to permit fuse **protection** of the circuit;
- Each secondary winding circuit is adequately fuse protected.

3.2.3 The wiring from each voltage transformer secondary winding shall not be grounded at more than one point.

3.3 This section is intentionally left blank.

3.4 This section is intentionally left blank.

3.5 Batteries and Direct Current (dc) Supply

DC supplies associated with **protection** shall be designed to have a high degree of dependability as follows:

3.5.1 No single battery or dc power supply failure shall prevent both independent **protection groups** from performing the intended function. Each battery shall be provided with its own charger.

3.5.2 Each station battery shall have sufficient capacity to permit operation of the station, in the event of a loss of its battery charger or the ac supply source, for the period of time necessary to transfer the **load** to the other station battery or re-establish the supply source. Each station battery and its associated charger shall have sufficient capacity to supply the total dc **load** of the station.

3.5.3 A transfer arrangement shall be provided to permit connecting the total **load** to either station battery without creating areas where, prior to failure of either a station battery or a charger, a single event can disable both dc supplies.

3.5.4 The battery chargers and all dc circuits shall be protected against short circuits. All protective devices shall be coordinated to minimize the number of dc circuits interrupted.

3.5.5 Dc systems shall be continuously monitored to detect abnormal voltage levels (both high and low), dc grounds, and loss of ac to the battery chargers, in order to allow prompt attention by the appropriate operating authorities.

3.5.6 **Protection groups** dc sources shall be continuously monitored to detect loss of voltage in order to allow prompt attention by the appropriate operating authorities.

3.6 Station Service ac Supply

On **bulk power system** facilities, there shall be two sources of station service ac supply, each capable of carrying at least all the critical **loads** associated with **protection systems**.

3.7 Circuit Breakers

No single trip coil failure shall prevent both independent **protection groups** from performing the intended function. The design of a breaker with two trip coils shall be such that the breaker will operate if both trip coils are energized simultaneously. The correct operation of this design shall be verified by tests.

3.8 **Teleprotection**

Communication facilities required for **teleprotection** shall be designed to have a level of performance consistent with that required of the **protection system**, and shall meet the following:

3.8.1 Where each of the two **protection groups** protecting the same **bulk power system element** requires a communication channel, the equipment and channel for each group shall be separated physically and designed to minimize the risk of both **protection groups** being disabled simultaneously by a single event or condition.

3.8.2 **Teleprotection** equipment shall be monitored to detect loss of equipment and/or channel to allow prompt attention by the appropriate operating authorities.

3.8.3 **Teleprotection** systems shall be provided with means to test for proper signal adequacy.

3.8.4 **Teleprotection** equipment shall be powered by the substation batteries or other sources independent from the power system.

3.8.5 Except as identified otherwise in these criteria, the two **teleprotection** groups shall not share the same component.

3.8.5.1 The use of a single communication tower for the radio communication systems used by the two groups protecting a single **element**, is permitted.

3.9 This section is intentionally left blank.

3.10 Environment

3.10.1 Each separate **protection group** and **Teleprotection** protecting the same system **element** shall be on different non-adjacent vertical mounting assemblies or enclosures.

3.10.2 In the event a common raceway is used, cabling for separate groups protecting the same system **element** shall be separated by a fire barrier.

3.11 Grounding

Station grounding is critical to the correct operation of **protection systems**. The design of the ground grid directly impacts proper **protection system** operation and the probability of false operation from **fault** currents or transient voltages.

3.11.1 Each member shall have established as part of its substation design procedures or specifications, a mandatory method of designing the substation ground grid, which:

- Can be traced to a recognized calculation methodology
- Considers cable shielding
- Considers equipment grounding

4.0 Specific Application Considerations

4.1 Transmission Line **Protection**

4.1.1 **Protection system** settings shall not constitute a loading limitation as per NERC requirement/standard. In cases where NERC approved exceptions are used the limits thus imposed shall be adhered to as system operating constraints.

4.1.2 A **pilot protection** shall be so designed that its failure or misoperation will not affect the operation of any other **pilot protection** on that same **element**.

4.2 This section is intentionally left blank.

4.3 Breaker Failure **Protection**

Means shall be provided to trip all necessary local and remote breakers in the event that a breaker fails to clear a **fault** as follows:

4.3.1 Breaker failure **protection** shall be initiated by each of the **protection groups** which trip the breaker, with the optional exception of a breaker failure **protection** in an adjacent zone.

4.3.2 Fault current detectors shall be used to determine if a breaker has failed to interrupt a fault.

4.4 Generating Station **Protection**

All under- and over-frequency **protection systems** designed to disconnect generators from the power system shall be coordinated with automatic underfrequency **load shedding** programs, in accordance with the *Emergency Operation Criteria* (Document A-3).

4.5 Automatic Underfrequency **Load Shedding Protection Systems**

The criteria for the operation of these **Protection Systems** are detailed in the *Emergency Operation Criteria* (Document A-3) and the *Automatic Underfrequency Load Shedding Program Relaying Guide* (Document B-7).

4.6 HVdc Systems **Protection**

4.6.1 The ac portion of an HVdc converter station, up to the valve-side terminals of the converter transformers, shall be protected in accordance with these criteria.

4.6.2 Multiple commutation failures, unordered power reversals, and **faults** in the converter bridges and the dc portion of the HVdc link which are severe enough to disturb the **bulk power system** shall be detected by more than one independent control or **protection group** and appropriate corrective action shall be taken, in accordance with the considerations in these criteria.

4.7 This section is intentionally left blank.

4.8 This section is intentionally left blank.

5.0 Reporting of Protection Systems

5.1 Each member shall provide the Task Force on System Protection (TFSP) with advance notification of any of the member's new **bulk power system protection** facilities, or significant changes in the member's existing **bulk power system protection** facilities.

5.2 Each member shall also provide the TFSP with advance notification of non-member **protection** facilities as required per NPCC Inc. Bylaws Section IX A (2) (c).

5.3 Each new or revised **protection system** shall be reported to the TFSP in accordance with the *Procedure for Reporting and Reviewing Proposed Protection Systems for the Bulk Power System* (Document C-22).

Prepared by: Task Force on System Protection

Review frequency: 3 years

References:

Bulk Power System Protection Guide (Document B-5)

Basic Criteria for the Design and Operation of the Interconnected Power Systems (Document A-2)

Emergency Operation Criteria (Document A-3)

Maintenance Criteria for Bulk Power System Protection (Document A-4)

NPCC Glossary of Terms (Document A-7)

Special Protection Systems Criteria (Document A-11)

Automatic Underfrequency Load Shedding Program Relaying Guide (Document B-7)

Procedure for Reporting and Reviewing Proposed Protection Systems for the Bulk Power System (Document C-22)

Security Guidelines for Protection Systems IEDs (Document B-24)

For Information: NPCC Working Group Report entitled, "Telecommunications for Bulk Power System Protection" dated March 1992

Document A-10

NORTHEAST POWER COORDINATING COUNCIL, INC.
1515 BROADWAY, NEW YORK, NY 10036-8901 TELEPHONE: (212) 840-1070 FAX: (212) 302-2782

Classification of Bulk Power System Elements

Adopted by the Members of the Northeast Power Coordinating Council Inc., this April 28, 2007 based on recommendation by the Reliability Coordinating Committee, in accordance with Section VIII of the NPCC Inc. Bylaws dated May 18, 2006 as amended to date.

1.0 Introduction

The NPCC *Basic Criteria for Design and Operation of Interconnected Power Systems* (Document A-2) and related criteria documents define specific requirements applicable to design, operation, and **protection** of the **bulk power system**. This *Classification of Bulk Power System Elements* (Document A-10) provides the methodology for the identification of those elements of the interconnected NPCC Region to which NPCC **bulk power system** criteria are applicable.

Each **Area** has an existing list of **bulk power system** elements. The methodology in this document is used to classify elements of the **bulk power system** and may result in elements being added to or removed from the existing lists.
The methodology in this document is based on the following principles:

- The objective is to determine which **elements,** or parts thereof, are part of the **bulk power system**. In practice however, the analysis is performed on a *bus* basis. Results of the analysis for a *bus* can be applied to determine which **elements** or portions thereof connected to the *bus* are part of the **bulk power system**.

- It is applicable to all voltage levels. **Elements** shall not automatically be included or excluded from the **bulk power system** based on voltage class. Application of this methodology may be omitted at *buses* that are already classified as part of the **bulk power system**, and at *buses* that can be logically excluded from the **bulk power system** based on study results at other *buses*.

- **Areas** may adopt methodologies that exceed the requirements set forth in this document for their own purposes. However, NPCC criteria and compliance monitoring shall consider only the system elements that qualify as **bulk power system** elements under the NPCC criteria.

(Terms that appear in bold typeface through out the document are defined in the Glossary located in Document A-7, the *NPCC Glossary of Terms.*)

The Classification of Bulk Power System Elements are based on three defined terms; **bulk power system**, **local area**, and **significant adverse impact**. Definitions for these are included in Document A-7, the NPCC *Glossary of Terms.*

Within this document, the term *bus* refers to an electrical node within a substation to which multiple elements are connected. In some cases faults may be cleared locally by circuit breakers located at another bus within the same substation. The examples in Figure 1 depict two such configurations. In some configurations a *bus* may include more than one physical bus, such as in a breaker-and-a-half arrangement or a single-line-single-breaker arrangement, where two physical buses are connected through a bus-tie breaker. The examples in Figure 2 depict two of many possible configurations. Regardless of the impedance between them, two switchyards at the same voltage level that are connected by an open bus-tie breaker or have separate control buildings are considered as two *buses*.

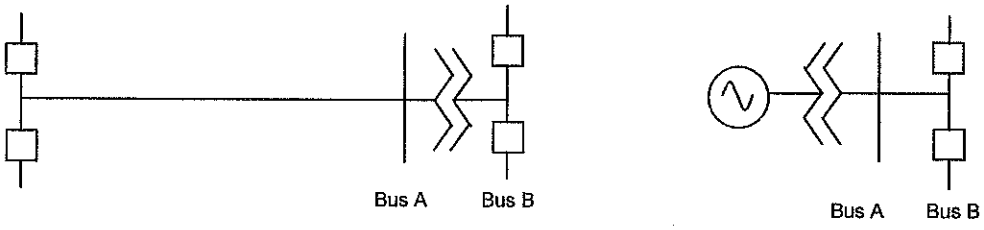

Figure 1 – Configurations where Bus A and Bus B are tested as two separate buses.

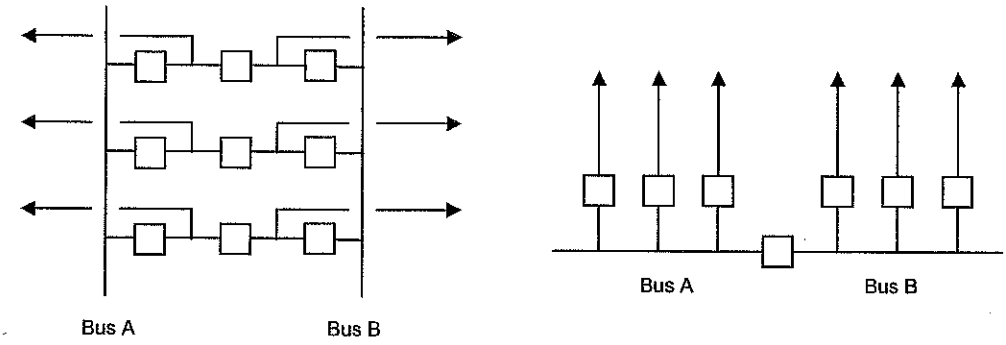

Figure 2 – Configurations where Bus A and Bus B are tested as one bus.

2.0 Classification of Bulk Power System Elements

2.1 Testing Conditions

Studies conducted for the purpose of determining the **elements** of the **bulk power system** shall assume power flow conditions utilizing transfers, **load** and **generation** conditions which stress the system in a manner critical to the classification of the *bus* to be tested. These studies shall be based on the interface limits, **load** and **generation** conditions expected to exist for the period under study. All **reclosing** facilities shall be assumed in service unless it is known that such facilities will be rendered inoperative.

2.2 Test Methodology

These criteria utilize both **transient stability** analysis and steady-state power flow analysis to determine the impact on system performance resulting from power system **faults**. The criteria steps are ordered to reduce the required number of simulations. **Fault clearing** by the remote **protection** is acceptable.

A **transient stability** test is used first to identify *buses* at which **faults** may cause a **significant adverse impact** outside the **local area**. This test is done based on either conservative **fault clearing** time assumptions, or actual **fault clearing** times at remote terminals. Either actual or conservative **fault clearing** times may be used.

The test is based on application of a *bus* **fault** at a single voltage level that is un-cleared locally. Tripping of un-faulted elements as a consequence of the **fault** is part of the test and does not constitute a **significant adverse impact**. Operation of **Special Protection Systems**, including undervoltage load shedding, shall be taken into account in these tests.

For those buses which are not classified as **bulk power system elements** in the first test, a power flow test is used to identify buses at which **faults** may cause a **significant adverse impact** outside the **local area** based on steady-state parameters such as post-contingency thermal loading and voltage.
If either the transient stability test or the power flow test identifies **a significant adverse impact**, then a determination must be made as to whether the **significant adverse impact** is contained within the **local area.** Determination that a **significant adverse impact** is contained within a **local area** is made by **Area(s)**, and affirmed by NPCC.

Transient Stability Based Test

1. The Transient Stability Based Test may be conducted either by simulating an extended fault assuming a conservative clearing time at remote terminals, or by using actual clearing times, as stated in option (a) or (b) below:

   a) Apply a three-phase **fault** at the bus, uncleared locally[1], and simulate tripping of the remote terminals of all transmission lines that will open to interrupt the **fault**. Remote clearing times shall be based on a conservative estimate of **fault clearing** times assuming no communications from the station under test to the remote terminals. Transformers connected to the *bus* shall not be tripped.

[1] Local clearing includes operation of all circuit breakers required to clear the fault at one substation and may include operation of circuit breakers at another bus, as defined in Section 1.0.

If the **fault** has a **significant adverse impact** outside the **local area**, then the *bus* is classified as part of the **bulk power system**, or option (b) may be used to classify the bus. Otherwise, continue with the Power Flow Based Test in Step 2.

b) Apply a three-phase **fault** at the *bus*, uncleared locally[1] and simulate tripping of the remote terminals of all elements that will open to interrupt the **fault**. Remote clearing times shall be based on designed fault clearing times, assuming no communications from the station under test to the remote terminals.

   Transformers connected to the *bus* shall be tripped by operation of independent remote protection groups capable of clearing a fault on the bus under test.

If the **fault** has a **significant adverse impact** outside the **local area,** the *bus* is classified as part of the **bulk power system**. Otherwise, continue with the Power Flow Based Test in step 2.
Some **protection groups** (e.g. directional comparison blocking) at remote terminals may provide high-speed **fault clearing** for faults at the bus under test. In order to test the effects of longer **fault clearing** times for fault conditions when these remote **protection groups** would not provide high-speed **fault clearing**, for either test (a) or (b) above:

- High-speed **fault clearing** at remote terminals must be ignored; or
- Testing must vary the placement of the 3-phase **fault** on the elements connected to the bus under test to include locations beyond the reach of the high-speed tripping relay element at the remote terminal.

If a *bus* is classified as part of the **bulk power system** in step 1, the **protective relay** settings may be reviewed to determine whether the *bus* could be classified as "non-bulk" if faster remote fault clearing can be achieved. If **protective relay** settings are modified, an assessment shall be conducted to ensure that the faster clearing time does not compromise the security of the **protection system**.

Power Flow Based Test

2. For those buses not already classified as part of the bulk power system in step 1, simulate the post-contingency steady-state conditions following a

fault at a *bus* that is un-cleared locally and cleared by tripping of the remote terminals of all elements that may open to interrupt the **fault**.

In cases where transformers are connected to the *bus*, the transformers shall be tripped by operation of independent remote protection groups capable of clearing a fault on the bus under test. In cases where the transformer would not be tripped, all elements connected to the same buses as the transformer terminals shall be tripped.

If the **fault** has a **significant adverse impact** outside the **local area**, the *bus* is classified as part of the **bulk power system**. Note that Step 2 can be done prior to Step 1. If a bus is classified as part of the **bulk power system** by the Power Flow Based Test, the Transient Stability Based Test need not be done for that *bus*.

Utilization of Test Results to Classify on an Element-by-Element Basis.

3. Classification of **bulk power system elements** is achieved by applying the results of the above tests to the **elements** connected to the tested *bus*:

   - An **element** with only one terminal such as a generator, shunt reactor, or capacitor bank, is classified as part of the **bulk power system** if the *bus* at which it is connected is classified as part of the **bulk power system**.

   - An **element** with multiple terminals such as a transformer or transmission line, is classified as part of the **bulk power system** if all terminals are connected to *buses* that are classified as part of the **bulk power system**. If all terminals are not connected to **bulk power system** *buses*, application of **faults** between the terminals may be used to determine what portion of the element is part of the **bulk power system.**

3.0 Application and List Maintenance

Each Area shall be responsible for application of the *Classification of Bulk Power System Elements* as described in this document, and shall maintain a list of **bulk power system** elements. These lists will be compiled into the "NPCC Inc. BPS List" and maintained by the Task Force on System Studies (TFSS) and presented as an informational item to the Reliability Coordinating (RCC) annually. The **Areas** shall review and update their lists as necessary at least every three years. Application of NPCC criteria and compliance monitoring shall be based upon these lists of **bulk power system elements**.

3.1 Elements upgraded to BPS

Existing system elements that are reclassified as BPS as a result of system changes shall be presented to and approved by the TFSS. If design and construction is required as a result of the reclassification, a proposed implementation plan shall be included. Once the BPS element and implementation plan are approved by TFSS, it will be added to the NPCC Inc. BPS list with the appropriate comments and information.

3.2 Elements downgraded from BPS

After obtaining TFSS approval, elements that are reclassified as no longer being part of the BPS as a result of system changes will be removed from the NPCC Inc. BPS list.

Lead Task Force:	Task Force on System Studies
Reviewed for concurrence by:	TFCO, TFSP, TFCP, and TFIST
Review frequency:	4 years
References:	*Basic Criteria for Design and Operation of Interconnected Power Systems* (Document A-2)
	NPCC Glossary of Terms (Document A-7)