NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note: The guideline was developed for CIP-002-1 but is also applicable to CIP-002-2 and CIP-002-3.

Security Guideline for the Electricity Sector: Identifying Critical Assets

Disclaimer:

This supporting document may explain or facilitate implementation of reliability standard CIP-002-1 — Critical Cyber Asset Identification but this supporting document does not contain mandatory requirements subject to compliance review.

Preamble:

It is in the public interest for NERC to develop guidelines that are useful for improving the reliability of the Bulk Power System (BPS)[1]. Guidelines provide suggested guidance on a particular topic for use by BPS users, owners, and operators according to each entity's facts and circumstances and do not provide binding norms, establish mandatory reliability standards, or create parameters by which compliance to standards is monitored or enforced.

This Guideline provides a methodology to identify Critical Assets that are essential to the reliability or operability of the BPS. The resulting list of Critical Assets is used as input to identify Critical Cyber Assets.

Purpose:

This Guideline is intended to inform the entity on the application of risk-based methodologies used under NERC Reliability Standard CIP-002-1 for identification of Critical Assets.

Applicability:

NERC Standard CIP-002-1 requires that applicable Responsible Entities identify and document a "risk-based" methodology that complies with CIP-002-1 R1 to identify Critical Assets. Application of the risk-based assessment must result in a list of Critical Assets (i.e., facilities, systems and equipment), even if such list is null. This list consists of assets that if destroyed, degraded, compromised (e.g., misused) or otherwise rendered unavailable would unacceptably affect the reliability or operability of the BPS as a whole (i.e., not just risk to the Responsible Entity). Unacceptable effects result in failure of the BPS to meet the characteristics that are defined for an Adequate Level of Reliability.

[1] Note: For purposes of this document, the terms "Bulk Power System" and "Bulk Electric System" are considered to be identical. FERC, in Order 693, paragraph 75, states that for an initial period it will rely on the NERC definition of BES.

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Figure 1 illustrates a commonly accepted definition of risk. As shown, *risk* is a function of *impact* or *consequences* and the *probability of occurrence* of a security event.

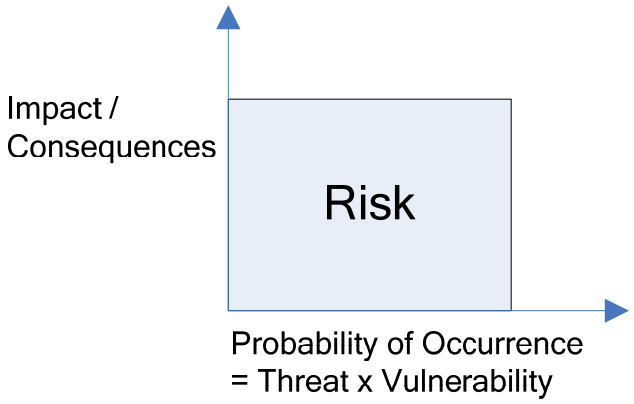

Figure 1

The *probability of occurrence* of a security event is determined by considering the Threat against a particular facility or system and the *vulnerability* of that facility or system to that *threat*.

A commonly used definition of threat is "the potential for a threat-source to successfully exercise (accidentally trigger or intentionally exploit) a specific vulnerability" according to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30[2], *Risk Management Guide for Information Technology Systems*, which discusses a variety of threat sources, motivations, and actions. Quantitatively determining threat is a difficult and subjective task. For example, the physical threat to an obscure low power substation would clearly seem to be different than that of a denial-of-service cyber threat on a transmission grid control system. However, the difference can be difficult to characterize or quantify. A simplifying approach is to assume that the potential for threats always exist.

Likewise, according to NIST, a vulnerability is "a weakness that can be accidentally triggered or intentionally exploited." Quantifying vulnerabilities is also difficult and dynamic. Cyber hackers discover new vulnerabilities every day. Therefore, it is conservative to assume that vulnerabilities will always be present in any network or physical protection scheme.

While traditional risk assessment normally considers both the probability of the loss of an asset and the impact or consequences if the asset is lost, this approach to Critical Asset

[2] NIST SP800-30 July 2002 is just one of a number of authoritative sources that describe risk concepts and define risk related terms. The definition from page 12 cited here is used only because it is useful in describing the applicability of this guideline.

identification considers that the asset has been lost. This guideline uses a simplifying approach and assumes that the potential for threats and vulnerabilities always exists (i.e., the probability of occurrence = 1.0). The risk-based assessment essentially becomes an impact analysis. Impacts can be intentional or unintentional, affecting not only an asset's availability but also its functional integrity. Compromise may include effects that are not immediately apparent. Impact analysis should consider BPS operations under different conditions.

Definitions:

Glossary of Terms Used in Reliability Standards:

Please refer to the NERC *Glossary of Terms Used in Reliability Standards* for the formal definition of the following terms:

- **Cascading**
- **Cranking Path**
- **Critical Assets**
- **Cyber Assets**
- **Critical Cyber Assets**
- **Element**
- **Facility**
- **Interconnection Reliability Operating Limit (IROL)**
- **Protection System**
- **Remedial Action Scheme**
- **Special Protection System**
- **Supervisory Control and Data Acquisition**
- **System Operating Limit**
- **Transmission**
- **Wide Area**

Additional Terms Used in the Document:

Terms defined in this section are not currently defined in the NERC Glossary and apply only to this Guideline.

Control Center — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BPS assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following:

- Supervisory control of BPS assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems
- Acquisition, aggregation, processing, inter-utility exchange, or display of BPS reliability or operability data
- BPS and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make operational decisions regarding reliability and operability of the BPS)
- Alarm monitoring and processing
- Coordination of BPS restoration activities.

Control Room — A Control Room operates control systems limited to controlling one or more of the following, and is typically located within the facility it controls:

- A single generation plant with one or more generation units, and potentially the BPS Elements of Transmission located within its associated switchyard
- A single transmission substation.

Adequate Level of Reliability[3] — "The Bulk Power System ("System") will achieve an adequate level of reliability when it possesses the following characteristics:

1. The System is controlled to stay within acceptable limits during normal conditions;
2. The System performs acceptably after credible Contingencies;
3. The System limits the impact and scope of instability and Cascading outages when they occur;
4. The System's Facilities are protected from unacceptable damage by operating them within Facility Ratings;
5. The System's integrity can be restored promptly if it is lost; and
6. The System has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components."

Common Mode Impact — Impact on multiple components, systems, units or facilities with identical, similar or related functions due to a single event.

[3] From NERC's May 5, 2008 filing to FERC to define "Adequate Level of Reliability". Additional information about each of the six characteristics is available at http://www.nerc.com/files/Adequate_Level_of_Reliability_Defintion_05052008.pdf.

Guideline Details:

This Guideline defines which assets should be evaluated, provides risk-based evaluation guidance for determining Critical Assets, and describes reasonable bases that could be used to support that determination. The process of identifying Critical Assets in this Guideline consists of the following five steps:

A. Determination of asset types
   Defines which assets should be evaluated

B. Consideration in defining assets
   Describes how and at what level of detail Critical Assets should be defined and special considerations with respect to asset types.

C. Application of evaluation guidance
   Defines the evaluation guidance that could be used to determine if an asset is a Critical Asset

D. Listing essential functions
   Discusses listing the essential functions of the asset

E. Documentation of assessment
   Discusses what should be documented and what forms a basis for determining whether an asset is critical

The identification process and subsequent evaluations should be performed in consultation with system operators and planning engineers using system studies, analysis, simulations and/or historical experience.

A. Determination of Asset Types

An entity should begin by identifying all of the BPS assets for which it is responsible. BPS assets to be evaluated against the risk-based guidance include facilities, systems, or equipment.

Assets to be evaluated per CIP-002-1, R1.2 are organized by type corresponding to the organization of the evaluation guidance provided in Section C:

- Transmission Substations — Assets containing BPS Elements of Transmission (i.e., CIP-002-1, R1.2.2).
- Generation Resources — Assets owned or operated by a Responsible Entity that meet criteria for their inclusion into the NERC compliance registry[4] (i.e., CIP-002-1, R1.2.3).

[4] Per Statement of NERC Compliance Registry Criteria (Rev 5.0)

- Control Centers — Assets capable of performing primary or backup control functions (i.e., CIP-002-1, R1.2.1).
- Special Systems — Systems performing a function essential to maintaining reliability or operability of the BPS, that if destroyed, degraded or compromised may cause unacceptable effects resulting in failure of the BPS to meet the characteristics that are defined for an Adequate Level of Reliability (i.e., CIP-002-1, R1.2.4, R1.2.5, and R1.2.6). This typically includes assets that support BPS reliability through one or more of the following:
    - Systems providing information used to make real-time operational decisions.
    - Supervisory and control capability,
    - Special Protection systems,
    - Systems essential to BPS restoration,
    - Systems performing automatic load shedding,
    - Other systems that may perform a function directly related to the reliability or operability of the BPS.

    Systems with scope and/or potential impact limited to a single BPS Facility are not expected to be evaluated independently. For example, a control system with scope limited to a single generation resource would not be evaluated as a Critical Asset. However, it may receive additional evaluation if its associated generation resource is a Critical Asset. Similarly, Protection Systems associated with critical Elements of Transmission may receive additional consideration when identifying Critical Cyber Assets.

An entity may wish to perform Critical Asset identification at a lower-level resolution by identifying the specific equipment within facilities or systems capable of influencing the BPS. Identification of Critical Assets at the equipment level may facilitate a more directed approach to ensuring that the appropriate equipment is afforded the protection outlined in the CIP standards. For example, an entity may wish to evaluate the specific Elements of Transmission within a substation.

B. Considerations in Defining Assets

Assets should primarily be defined either as facilities or special systems impacting the reliability or operability of the BPS as identified in CIP-002-1 R1.2. The evaluation guidance presented in Section C is specific to facilities and systems. Systems or equipment that are elements of a facility should be considered part of the asset and not evaluated separately from the facility. However, an entity may also consider identifying specific equipment within facilities if the facilities can be separated into separate assets (e.g., transmission and distribution assets within the same substation facility).

Individual generation units should not be considered separate facilities if there is a support or control system shared among them which could impact the function of the station and ultimately impact the reliability or operability of the BPS. If common support or control systems affect multiple units regardless of their location, then the units as a set should be evaluated together because of the potential for Common Mode Impact. Careful consideration of Common Mode Impacts is important because effects can appear as if stemming from independent causes.

Elements of Transmission on the premises of a generating resource should not be overlooked in the evaluation of assets.

Dedicated control equipment (e.g., a Control Room) that impacts only assets within a facility should be evaluated as part of that facility. However, a Control Center, regardless of its location, should be evaluated separately according to the guidance described in Section C, Table C-3.

In general, coordination and communication with other Responsible Entities may be important in determining the criticality of shared or interconnected assets. Coordination or interconnection agreements between Responsible Entities may be considered as one way to communicate the identification of Critical Assets serving both Responsible Entities. It is suggested that the owners of interconnected assets coordinate the Critical Asset designation of both facilities (i.e., generators, transmission substations, and Control Centers). If two separate Responsible Entities' assessment methodologies result in differing assessments of the same asset, the Responsible Entities should establish agreements to resolve the differences.

C. Application of Evaluation Guidance:

CIP- 002 R1 requires each Responsible Entity to identify its Critical Assets, but does not require the same evaluation criteria to be applied to all asset types. The Responsible Entity is responsible for establishing a reasonable set of criteria for evaluation of each of the asset types listed in CIP-002-1 R1.2.1 through R1.2.7.

The following tables (i.e., C-1, C-2, C-3, and C-4) are provided as evaluation guidance for determining the criticality of four assets types (i.e., Transmission Substations, Generator Resources, Control Centers and Special Systems). The evaluation criteria for each of these asset types are correlated to one or more of the six BPS characteristics that support an Adequate Level of Reliability (ALR) per the filed NERC definition. Loss or compromise of a BPS asset affecting one or more of these characteristics represents unacceptable consequences. Assessment of impact to an ALR characteristic provides one possible basis for determining whether or not an asset is critical. Following this example methodology, if

an asset is evaluated under varying conditions (e.g., demand, transmission configuration) and fails to meet any single criteria, then it should be considered critical.

To ensure evaluation criteria are applicable to their unique circumstances, Responsible Entities are encouraged to involve system operators and planning engineers in the development of their evaluation methodologies. Additionally, for Responsible Entities without a wide-area view, cooperation with Reliability Coordinators, Balancing Authorities, and other BPS asset owners may ensure better results than working in isolation. Cooperation may include sharing evaluation approaches, issues and results.

Table C-1 Evaluation Guidance for Transmission Substations		
Example Criteria	**Description**	**ALR**
Essential to BPS restoration.	Elements of Transmission critical to BPS restoration, including transmission substations used for initial system restoration (i.e., identified as part of the likely to be used Cranking Path) as documented in the regional system restoration plan developed pursuant to the EOP standards (e.g., EOP-005-2), unless specifically excluded by engineering assessment. Note that Elements of Transmission critical to BPS restoration may rely on transmission substations that are less than 100kV (e.g., blackstart generation connected at 69kV) which therefore should be evaluated.	5
Essential to critical generation for the BPS.	Elements of Transmission or a transmission substation, the loss of compromise of which, as determined by an engineering evaluation or other assessment method, that results in the loss of generation identified as a Critical Asset for the BPS. Elements of Transmission associated with critical generation may rely on transmission substations that are less than 100kV (e.g., blackstart generation connected at 69kV) which therefore should be considered.	1 & 6
Essential for voltage or frequency support or stability of the BPS	Elements of Transmission or a transmission substation, the loss or compromise of which, as determined by an engineering evaluation or other assessment method that are essential for voltage or frequency support. Impacts to be considered include: • Voltage collapse • Voltage going below the under-voltage load shed points established to mitigate the risk of voltage collapse or voltage instability in the BPS (e.g., PRC-010-1) • Exceeding voltage limits that result in a Category D event as discussed in TPL-004. • Frequency going below the under-frequency load shed points • System collapse due to frequency-related instability • Complete operational failure or shutdown of the BPS for which the entity is responsible causing Wide Area instability • Separation or Cascading outages affecting a Wide Area of the BPS. or Elements of Transmission or a transmission substation, the loss of which, as determined by an engineering evaluation or other assessment method, that may result in an Interconnection Reliability Operating Limit (IROL) violation (FAC-011-1).	1, 2, 3, 4 & 6

Table C-2 Evaluation Guidance for Generation Resources[5]		
Example Criteria	**Description**	**ALR**
Essential generation for the BPS.	A single unit or combination of units (i.e., failure due to Common Mode Impact) whose loss or compromise could violate any of the following regional obligations defined by Balancing Authority, Reliability Coordinator or Regional Reliability Assurer[6] (refer to BAL-002-0 R1)[7]: • Output exceeds Reserve Sharing Group obligation • Output exceeds Contingency Reserve obligation • Must-run units A possible exception is generation that is tripped by a Remedial Action Scheme (RAS) or Special Protection System (SPS), only if the function of the RAS or SPS is to protect the BPS.	1, 2, & 6

[5] Only operational generators (i.e., not mothballed) should be considered.
[6] See NERC Functional Model Version 4
[7] Criteria should be established in such a manner as to not exclude all generation from consideration

Table C-2 Evaluation Guidance for Generation Resources[5]		
Example Criteria	**Description**	**ALR**
Essential to mitigate known BPS constraint(s), including voltage or frequency support or stability.	A combination of units (e.g., failure due to Common Mode Impact) that, if destroyed, degraded, or otherwise rendered unavailable, has been determined through an engineering study to be essential to the BPS reliability, either for voltage or frequency support. Impacts to be considered include: • Voltage collapse • Voltage going below the under-voltage load shed points established to mitigate the risk of voltage collapse or voltage instability in the BPS (e.g., PRC-010-1) • Exceeding limits that result in a Category D event as discussed in TPL-004 • Frequency going below the under-frequency load shed points without recovering in a reasonable period (e.g., a half hour) once load is shed • System collapse due to frequency-related instability • Complete operational failure or shutdown of the BPS for which the entity is responsible causing Wide Area instability • Separation or Cascading outages affecting a Wide Area of the BPS or The loss of generation, as determined by an engineering evaluation or other assessment method, resulting in an Interconnection Reliability Operating Limit (IROL) violation (FAC-011-1).	1, 2 & 3
Essential to BPS restoration.	Blackstart Resources[8], which are essential to the initial BPS restoration described in the regional restoration plan (consideration of generation as part of a cranking path is presented in Table C-1), unless specifically excluded by engineering assessment.	5

[8] The term "Blackstart Resources" is a new term from EOP-005-2.

Table C-3 Evaluation Guidance for Control Centers		
Example Criteria	**Description**	**ALR**
Essential by virtue of their functions supporting reliability or operability of the BPS.	Primary and backup Control Centers owned, operated or employed by Responsible Entities (e.g., Balancing Authorities, Interchange Authorities, Transmission Operators, Reliability Coordinators), the loss or compromise of which could cause Transmission, Generation or Special Systems to exceed their evaluation criteria.	1,2,3,4,5 & 6
Essential for providing information used by a Responsible Entity to make real-time operational decisions regarding reliability and operability of the BPS.	The loss or compromise of any of the following functions associated with real-time status, value or alarm data: • collection, • aggregation, • processing or • display at a Responsible Entity's primary or backup Control Center determined by an engineering evaluation or other assessment method to impact reliability or operability of the BPS (e.g., Loss or compromise of Control Center could cause Transmission, Generation or Special Systems to exceed their evaluation criteria.)	1,2,3,4,5 & 6
Essential for real-time inter-utility data exchange critical to reliable BPS operation.	The loss or compromise of inter-utility data exchange functions of a Responsible Entity's primary or backup Control Center determined by engineering evaluation or other assessment to impact the reliability or operability of the BPS (e.g., Loss or compromise of Control Center could cause Transmission, Generation or Special Systems to exceed their evaluation criteria.)	1,2,3,4,5 & 6
Essential for control or data acquisition for a BPS asset determined to be a Critical Asset.	Loss or compromise of supervisory control or data acquisition functions of a Responsible Entity's primary or backup Control Center for a BPS asset determined to be a Critical Asset.	1,2,3,4,5 & 6
Essential Control Center functionality for a set of BPS assets determined to collectively impact reliability and operability of the BPS.	Loss or compromise of supervisory control or data acquisition functions of a Responsible Entity's primary or backup Control Center for a set of BPS assets determined by engineering evaluation or other assessment to collectively cause Transmission, Generation or Special Systems to exceed their evaluation criteria.	1,2,3,4,5 & 6

Table C-4 Evaluation Guidance for Special Systems		
Example Criteria	**Description**	**ALR**
Remedial Action Scheme /Special Protection System that supports the reliability or operability of the BPS.	A RAS or SPS supporting the reliability or operability of the BPS (e.g., loss or compromise of RAS or SPS that could cause Transmission or Generation to exceed their evaluation criteria).	2, 3, & 5
System critical to automatic load shedding supporting the reliability or operability of the BPS.	Systems, not already evaluated as part of another asset type, that are critical to automatic load shedding of 300 MW or more that support the reliability or operability of the BPS. Note that any system, including a centralized system, with the capability to affect 300 MW of load shedding should be addressed.	2 & 3
Demand-Side Management (DSM), or Direct Control Load Management (DCLM), that supports the reliability or operability of the BPS.	Loss or compromise of centralized portion of the Demand-Side Management (DSM), or Direct Control Load Management (DCLM), system determined by an engineering evaluation or other assessment to impact the reliability or operability of the BPS (e.g., loss or compromise of centralized portion of the DSM or DCLM that could cause Transmission or Generation to exceed their evaluation criteria).	2, 3 & 6
Essential by virtue of their functions to the BPS.	The system has specific equipment use or designations supporting the reliability or operability of the BPS. Examples may include: • Presence of reliability “must run” equipment • Static VAR Compensation mechanisms • Energy management systems • Supervisory Control and Data Acquisition systems • Substation automation and control systems • Protection System • Remote relay setting management system Engineering evaluation determines that loss or compromise of the system or supporting system to impacts reliability or operability of the BPS (e.g., loss or compromise could cause Transmission or Generation to exceed their evaluation criteria).	1,2,3,4,5 & 6

D. Listing Essential Functions

For facilities and systems determined to be Critical Assets, it is suggested that all essential function(s)[9] performed by that asset be identified and listed. The "Example Criteria" presented in the evaluations tables, C-1 through C-4, present example essential functions performed for the BPS by Critical Assets. Essential functions support the characteristics of ALR. Identification of essential functions for a facility can be done by identifying what evaluation guidance category and basis were used to determine that an asset was critical. Identification of all essential functions is important for facilities to be further assessed for identification of Critical Cyber Assets.

E. Documentation of Assessment

NERC CIP-002-1 R1 requires that the risk-based methodology used to identify Critical Assets be documented and CIP-002-1 R2 requires a list of Critical Assets be maintained and updated as necessary. The evaluation and basis for the judgments made about an asset's status should be documented. It is suggested that documentation of the evaluation should include: (1) identification of the assets considered, (2) identification of the assets considered Critical Assets, (3) method or basis used to determine why assets were or were not considered to be Critical Assets, and (4) a listing of the essential functions that each Critical Asset performs.

In addition to consulting with system operators and planning engineers or using historical experience, reasonable bases supporting an evaluation may include engineering assessments, authoritative studies, or specific equipment use or designations that support the BPS:

- Engineering Assessment — An engineering assessment or simulation provides a basis to determine the extent to which an asset supports reliability or operability of the BPS. Such an assessment should be performed under normal, as well as adverse, load conditions and may include system simulations, such as transient stability analysis, and steady state power flow analysis, or any other relevant modeling tools or techniques that may assist the assessment process.

  An engineering assessment may also be an exercise of professional judgment made by subject matter experts (e.g., engineering staff, operations staff, and engineering consultants) with detailed knowledge of the role and function of the BPS assets under evaluation. The professional judgment may include qualitative or quantitative inputs.

- Authoritative Studies and Sources — Existing authoritative studies and sources may be utilized to determine whether or not an asset is essential to performing a particular function. Examples include:

  - Previous studies performed to meet Transmission Planning (TPL) and Transmission Operations (TOP) standards
  - Regional and interregional transmission planning studies
  - System operating bulletins

[9] An asset may perform more than one essential function that may in turn be important to the identification of the Critical Cyber Assets.

- Specific Equipment Use or Designations Supporting the BPS — Specific equipment use or designations that may signify critical support to the BPS can also be used. Examples of equipment used may include:
  - Presence of reliability "must run" equipment
  - Static VAR Compensation mechanisms
  - Energy management systems
  - Supervisory Control and Data Acquisition systems
  - Substation automation and control systems
  - Protection System

When conducting an engineering assessment, consider that multiple assets can be simultaneously impacted or that assets can be damaged such that other asset outages may occur before the damaged asset can be returned to service. The fact that the BPS was developed to withstand the loss of any single asset should not be the basis for not protecting that asset. The assessment should consider consequences from the logical loss of connected assets (e.g., the loss of a substation resulting in the loss of an interconnected generator because it is connected to the substation). An assessment should also consider whether assets have a connection, especially a cyber connection, which introduces the possibilities for Common Mode Impact.

Redundancy should not be considered to reduce the criticality of any asset. Redundancy will only affect availability and reliability while not improving integrity and may in fact increase the assets' exposure to loss or compromise.

Responsible Entities that do have the internal capability (data availability or expertise) should perform the appropriate engineering assessment. Responsible Entities that do not have the internal capability to perform such an assessment should request the assistance of a third party capable of performing the assessment. Responsible Entities could coordinate with their regional Reliability Coordinator for guidance but should not pass off responsibility to their Reliability Coordinator, Balancing Authority or other Responsible Entities for determination of their Critical Assets. The ultimate responsibility for determination of Critical Assets still resides with the Registered Entity asset owner.

Appropriate communication and necessary cooperation among Responsible Entities is in the best interest of the BPS. When such communication and cooperation has occurred, this should be made part of the assessment documentation.

Related Documents and Links:

The references cited here are the versions that were approved when this document was written.

NERC Standard BAL-002-0, *Disturbance Control Performance, Resource and Demand Balancing, North American Electric Reliability Corporation,* February 2005.
http://www.nerc.com/files/BAL-002-0.pdf

NERC Standard CIP-002-1, *Cyber Security – Critical Asset Identification,* North American Electric Reliability Corporation, May 2006.
http://www.nerc.com/files/CIP-002-1.pdf

NERC Standard EOP-005-2, *System Restoration Plans*, Emergency Preparedness and Operations, North American Electric Reliability Corporation, August 2009.
http://www.nerc.com/files/EOP-005-2.pdf[10]

NERC Standard FAC-011-1, *System Operating Limits Methodology for the Operations Horizon,* Facility Design, Connection and Maintenance, North American Electric Reliability Corporation, November 2006.
http://www.nerc.com/files/FAC-011-1.pdf

NERC Standard TPL-004-0, *System Performance Following Extreme Events Resulting in the Loss of Two or More Bulk Electric System Elements (Category D),* North American Electric Reliability Corporation, April 2005.
http://www.nerc.com/files/TPL-004-0.pdf

NERC Functional Model Version 4, North American Electric Reliability Corporation, December 2008.
http://www.nerc.com/files/Functional_Model_V4_CLEAN_2008Dec01.pdf
NERC Functional Model Technical Document (Version 4), North American Electric Reliability Corporation, December 2008.
http://www.nerc.com/files/FM_Technical_Document_CLEAN_2008Dec01.pdf

NERC Glossary of Terms Used in Reliability Standards, February 2008.
http://www.nerc.com/files/Glossary_12Feb08.pdf

NERC Statement of Compliance Registry Criteria, Rev. 5, North American Electric Reliability Corporation, Sept 2007.
http://www.nerc.com/files/Statement_of_Compliance_Registry_Criteria_V4-0.pdf

NERC compliance filing to FERC of the Definition of "*Adequate Level of Reliability.*" May 5, 2008.
http://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf

[10] NERC Standard EOP-005-2 was approved by the NERC Board of Trustees during the final review of this Guideline. This footnote will be removed as soon as the standard is posted on the NERC web site.

NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems,* computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, July 2002.
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Revision History:

Date	Version Number	Reason/Comments
09/17/09	1.0	Final Approval by CIPC