



**TEXAS
REGIONAL
ENTITY™**

An Independent Division of ERCOT

Identifying Critical Assets: Guidelines

Presented by Christopher Humphreys
CIP Manager

Presentation from the NERC Joint OC/PC/CIPC September 10, 2008 Meeting

Background

- **FERC Order 706 directs either NERC or the Regional Entities to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk Power System. (§ 255)**
- **CIPC (Critical Infrastructure Protection Committee) directed the Risk Assessment Working Group (RAWG) to create a Risk Assessment guideline.**

Background

- **The three tenets of Information Security are: confidentiality, integrity & availability.**
- This guideline focuses on availability and integrity.
- Availability (or traditional view of reliability) is largely provided by adequate capacity and redundancy (e.g. N-1 concept).
- Integrity ensures that assets are not compromised or that unauthorized modifications are not made. More than one asset might be comprised at the same time. *Concepts such as redundancy and N-1 do not ensure integrity.*

Guideline

- **The draft guideline is titled “Identifying Critical Assets”.**
- **The guideline is based on:**
 - Critical Assets identification,
 - Support for Standard CIP-002-1, and
 - Applicability as expressed in CIP-002-1.
- **This guideline should NOT be interpreted as a standard.**
- **It is a reference document (a guideline in support of a standard).**
- **Critical Cyber Assets will be dealt with in a later companion guideline (Volume 2).**

Guideline

- **The RAWG focus has been on technical content and clarifying issues based on their collective knowledge and experience. Industry comments welcomed to complete the guideline.**
- **Strategic issues including impact on various entities associated with the risk assessment guidelines must be dealt with by the various NERC committees.**
- **This guideline is organized from a functional entity perspective under generation, transmission, etc.:**
 - Different than CIP-002-1 R1.2
 - Example: A generator owner or generator operator would look under the generation evaluation criteria table.
 - This approach more easily allows criteria specific to generation, etc.

Guideline Purpose

- **This guideline provides a methodology to help identify BES assets which are critical assets as described in CIP-002-1 R2.**
- **This methodology is intended to provide a basis for making a reasonable determination of whether or not the loss or *compromise* of an applicable BES asset would affect the reliability or operability of the BES.**

Guideline Applicability

- **Risk assessment should focus on BES as a whole & not risk to a Responsible Entity's individual asset.**
- **In developing a risk-based assessment methodology, threats and vulnerabilities are assumed to exist – it essentially becomes an “Impact Analysis”, or**
- **A simple question is: “Does an asset if destroyed, degraded, *compromised* or otherwise rendered unavailable, impact the reliability of the Bulk Electric System?”**

Guideline Definitions

- **NERC glossary terms:**
 - Critical Assets
 - Cyber Assets
 - Critical Cyber Assets
 - Element
 - Interconnection Reliability Operating Limit (IROL)
- **Additional Defined Terms:**
 - Control Center
 - Transmission Elements
 - Reliability of BES
 - Common Mode Impact

Reliability of BES Definition

- **For purposes of CIP-002, Reliability of the BES is defined as:**
 - The extent which BES assets are operated within equipment and electric system thermal, voltage, frequency, and stability limits such that instability, uncontrolled separation, cascading failures, of such a system will not occur as a result of a sudden disturbance, including a cyber-security incident or unanticipated failure of system elements.

Guideline Overall Approach

- **The process of identifying Critical Assets in this guidance document consists of the following four steps:**
 1. Determination of asset types that should be evaluated.
 2. Defining assets.
 3. Listing critical functions.
 4. Documentation of assessment.

1. Determination of Asset Types that Should be Evaluated

- **An entity should first identify all of the BES assets for which it is responsible.**
- **BES assets to be evaluated against the risk-based criteria may include facilities, systems, or equipment.**
- **Facility types, systems and equipment that may be evaluated include:**
 - Transmission Substations
 - Generation Resources
 - Control Centers
 - Systems

1. Determination of Asset Types that Should be Evaluated (continued)

- **Systems that perform a function essential to maintaining reliable operation of the BES.**
- **This includes systems that *support wide-area* reliability through one or more of the following:**
 - Situational awareness,
 - Supervising and control capability,
 - Special Protection Systems,
 - Systems essential to BES restoration,
 - Systems performing automatic load shedding, or
 - Other systems that may perform a function directly related to BES system reliability.

1. Determination of Asset Types that Should be Evaluated (continued)

- **Any single applicable criteria makes the asset potentially a critical asset.**
- **Systems with scope and/or potential impact limited to a single non-critical BES facility are not expected to be evaluated independently as Critical Assets.**
 - 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 in Volume Two if its associated generation resource is a Critical Asset.

2. Defining Assets

- **Critical Assets will primarily be identified either as facilities or special systems impacting the BES. The evaluation criteria presented in Section 3 are specific to facilities and systems.**
 - An entity could consider identifying specific equipment within facilities as critical.
 - Generation facilities should consider any common mode impact.
 - Special considerations for Control Centers.
 - Switchyards for generation facilities.

3. Listing Essential Functions

- **Identify all Critical Assets**
 - All essential functions should be identified.
 - Important in the assessment of Critical Cyber Assets.

4. Documentation of Assessment

- **Documentation of the evaluation should include all of the following:**
 - Identification of the assets considered.
 - Identification of the assets considered Critical Assets.
 - Method or evaluation criteria used to determine why were or were not considered to be Critical Assets.
 - List of the essential functions that each Critical Asset performs.
- **Reasonable basis supporting an evaluation include engineering evaluations, authoritative studies, and specific equipment use or designations that support the BES.**

Timeline for CIP Guideline Approval

- **Guideline development will follow the new guideline process.**
- **June 2008 - draft guideline sent to the Critical Infrastructure Protection Committee (CIPC) for conceptual review and comment.**
- **Summer 2008 - WG revised the guideline based on the comments received. Feedback was not provided for the comments received due to the dynamic and iterative nature of the development process.**
- **August 2008 - revised draft guideline sent to CIPC.**

Timeline for CIP Guideline Approval (continued)

- **September 2008 - presentations and discussion with NERC Operations Committee, Planning Committee, and CIPC.**
- **CIPC approval.**
- **Posting, industry comments followed by responses, guideline revision and CIPC approval.**
- **Additional industry comments, etc. followed by industry voting.**
- **April - June 2009 final guideline approval by CIPC.**



**TEXAS
REGIONAL
ENTITY™**

An Independent Division of ERCOT

Questions?

