

**A. Introduction**

- 1. Title:** Cyber Security — Critical Cyber Asset Identification
- 2. Number:** CIP-002-1a
- 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
1a	TBD	Added Appendix 1 Interpretations	TBD

Appendix 1

<b>Requirement Number and Text of Requirement</b>
<p>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:</p> <p>R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,</p> <p>R3.2. The Cyber Asset uses a routable protocol within a control center; or,</p> <p>R3.3. The Cyber Asset is dial-up accessible.</p>
<b>Question 1</b>
<p>Is the phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be assessed for inclusion in the list of Critical Cyber Assets using an entity’s critical cyber asset methodology?</p>
<b>Response to Question 1</b>
<p>The phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” is illustrative, not prescriptive. It simply provides examples of the types of Cyber Assets that should be considered. It does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types.</p>
<b>Question 2</b>
<p>What does the phrase, "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.</p>

## Response to Question 2

The word “essential” is not defined in the *Glossary of Terms used in NERC Reliability Standards*, but the well-understood meaning and ordinary usage of the word “essential” implies “inherent to” or “necessary.” The phrase “essential to the operation of the Critical Asset” means inherent to or necessary for the operation of the Critical Asset.

A Cyber Asset that “may” be used, but is not “required” (i.e., a Critical Asset cannot function as intended without the Cyber Asset), for the operation of a Critical Asset is not “essential to the operation of the Critical Asset” for purposes of Requirement R3. Similarly, a Cyber Asset that is merely “valuable to” the operation of a Critical Asset, but is not necessary for or inherent to the operation of that Critical Asset, is not “essential to the operation” of the Critical Asset.