

A. Introduction

1. **Title:** Cyber Security — Critical Cyber Asset Identification
2. **Number:** CIP-002-4
3. **Purpose:** NERC Standards CIP-002-4 through CIP-009-4 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.

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-002-4 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 the criteria in Attachment 1.

4. **Applicability:**
 - 4.1. Within the text of Standard CIP-002-4, “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 Entity.
 - 4.2. The following are exempt from Standard CIP-002-4:
 - 4.2.1 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

- R1.** Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary.
- R2.** Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
- R2.1.** The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- R2.2.** The Cyber Asset uses a routable protocol within a control center; or,
- R2.3.** The Cyber Asset is dial-up accessible.
- R3.** Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 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 risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

- M1.** The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.
- M2.** The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.
- M3.** The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- 1.1.1** Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.
- 1.1.2** ERO for Regional Entity.
- 1.1.3** Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits
Self-Certifications

- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.4. Data Retention

- 1.4.1** The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- 1.4.2** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

- 1.5.1** None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change “Control Center” to “control center”	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

- 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.
- 1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater.
- 1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes.
- 1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.
- 1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.
- 1.6. Transmission Facilities operated at 500 kV or higher.
- 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations.
- 1.8. Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).
- 1.9. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).
- 1.10. Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3.
- 1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.
- 1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).
- 1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes.
- 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator.
- 1.15. Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection.
- 1.16. Any additional assets that the Responsible Entity deems appropriate to include.