

A. Introduction

1. **Title:** Cyber Security — Critical Cyber Asset Identification
2. **Number:** CIP-002-~~34~~
3. **Purpose:** NERC Standards CIP-002-~~34~~ through CIP-009-~~34~~ 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-~~34~~ 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~~the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-~~34~~, “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-~~34~~:

- 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 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. **Effective Date:** The first day of the ~~third~~eight calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first

day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

~~**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.R1.** 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 criteria contained in R1.CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall review update this list as necessary, and review it at least annually, and update it as necessary.~~

~~**R2.** Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement ~~R2R1~~, 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 update this list as necessary, and review it at least annually, and update it as necessary.~~

~~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, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.~~

For the purpose of Standard CIP-002-34, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,

- The Cyber Asset is dial-up accessible.
- R3.** Annual Approval — The senior manager or delegate(s) shall approve annually the ~~risk-based assessment methodology, the~~ list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, ~~R2~~, and ~~R3R2~~ 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 current risk-based assessment methodology documentation as specified in Requirement ~~R1~~.
- ~~M2.~~M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement ~~R2~~R1.
- ~~M3.~~M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement ~~R3~~R2.
- ~~M4.~~M3. The Responsible Entity shall make available its ~~approval~~ records of ~~annual~~ approvals as specified in Requirement ~~R4~~R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

~~1.1.1~~ 1.1.1 The Regional Entity ~~for Responsible Entities~~ shall serve as the Compliance Enforcement Authority with the following exceptions:

- ~~For entities~~ that do not ~~perform delegated taskwork~~ for the Regional Entity, ~~the Regional Entity shall serve as the Compliance Enforcement Authority.~~

~~1.1.1~~• ~~For Reliability Coordinators and other functional entities that work~~ for their Regional Entity, ~~the ERO shall serve as the Compliance Enforcement Authority.~~

~~1.1.2~~ — ERO for Regional Entity.

- ~~Third~~ For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~1.1.3~~ — For the ERO, a ~~third~~-party monitor without vested interest in the outcome for ~~NERC~~.

~~1.2.~~ 1.2. ~~the ERO shall serve as the~~ Compliance **Monitoring Period and Reset Time Frame**

~~1.2.1.1.2~~ 1.2.1.1.2 ~~Not applicable~~ Enforcement Authority.

~~1.3.1.2.~~ 1.3.1.2. **Compliance Monitoring and Enforcement Processes**

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4.1.3. Data Retention

1.4.1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002-~~34~~ 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.

1.4.2.1.3.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5.1.4. Additional Compliance Information

1.5.1.4.1 None.

2. Violation Severity Levels (~~Developed separately~~ To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/January 16/06, <u>2006</u>	R3.2 — Change “Control Center” to “control center”	03/24/06
2	Approved by NERC Board of Trustees <u>5/6/09</u>	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.	Revised
3		Changed <u>Updated version number</u> from CIP-002-2 to CIP-002-3: Changed all references to CIP Version “2” standards to CIP Version “3” standards. For Violation Severity Levels, changed, “To be developed later” to “Developed separately.”	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
<u>3</u>	<u>12/16/09</u>	<u>Approved by the NERC Board of Trustees</u>	<u>Update</u>

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 in a single Interconnection.
- 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 MVAR or greater.
- 1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.
- 1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.
- 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.
- 1.6. Transmission Facilities operated at 500 kV or higher.
- 1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.
- 1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.
- 1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.
- 1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of 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, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.
- 1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.
- 1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

- 1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.
- 1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.
- 1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.