

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAR posted for comment (March 20, 2008 – April 19, 2008).
2. Revised SAR and response to comments approved by SC (July 10, 2008).
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by NERC Board of Trustees (May 6, 2009).
6. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 3 of CIP-002 to CIP-009 final ballot (December 14, 2009)
8. Version 3 of CIP-002 to CIP-009 approved by NERC Board of Trustees (December 16, 2009)

Proposed Action Plan and Description of Current Draft:

This is the initial draft of Version 4 of the proposed CIP-002 standard and is being submitted to the industry for feedback as part of an informal comment period. Industry feedback will be utilized by the drafting team to refine the draft standard for formal industry review in February 2010.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Post for 45-day comment period and pre-ballot review.	March 15, 2010
2. Conduct initial ballot.	May 24, 2010
3. Post response to comments on initial ballot.	June 21, 2010
4. Conduct recirculation ballot.	June 21, 2010
5. Submit standard to BOT for adoption.	To be determined.
6. File standard with regulatory authorities.	To be determined.

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data.

BES Cyber System — A Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.

Bulk Electric System Subsystem (BES Subsystem) — A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used to generate energy, transport energy or ensure the ability to generate or transport energy.

Generation Subsystem — Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

Transmission Subsystem — Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

Control Center — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES 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 BES 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 BES reliability or operability data for the support of real-time operations
- BES 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 BES restoration activities.

High BES Impact

BES Subsystems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable:

- they could directly cause, contribute to, or create an unacceptable risk of-
 - BES instability; and/or
 - BES separation; and/or
 - a cascading sequence of failures.or
- in a planning time frame, they could, under emergency, abnormal, or restorative conditions, directly cause, contribute to, or create an unacceptable risk of-
 - instability; and/or
 - separation; and/or
 - a cascading sequence of failures;or
could hinder restoration to a normal condition.

Medium BES Impact

BES Subsystems have Medium BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could:

- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES; or
- in a planning time frame, under emergency, abnormal, or restorative conditions,
 - directly affect the electrical state or the capability of the BES; or
 - directly affect the ability to effectively monitor and control the BES.

Low BES Impact

BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could **not**:

- directly cause, contribute to, or create an unacceptable risk of BES instability; or BES separation; or a cascading sequence of failures.
- hinder restoration to a normal condition.
- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES;

Terms to be retired from the *Reliability Standards Glossary of Terms* once the standards that use those terms are replaced:

1. Critical Assets
2. Critical Cyber Assets
3. Cyber Assets

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization
2. **Number:** CIP-002-4
3. **Purpose:** To identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the Bulk Electric System (BES) as a basis for applying security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES.
4. **Applicability:**
 - 4.1. **Functional Entities:**

For purposes of the requirements contained herein, the listing of Functional Entities will be collectively referred to as “Responsible Entities.” In situations where a specific Functional Entity or subset of Functional Entities are used, the Functional Entity(ies) will be specified explicitly.

 - 4.1.1 Reliability Coordinator.
 - 4.1.2 Balancing Authority.
 - 4.1.3 Interchange Coordinator.
 - 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.
5. **Physical Facilities:**
 - 5.1. All BES facilities,(including those structures, components, equipment and systems of facilities within a nuclear generation plant not regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission).
6. **Effective Date:** The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the eighth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

- R1.** As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize the BES Subsystems under its ownership by applying the criteria in *CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems. (Violation Risk Factor: High)*
- 1.1** The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change.
 - 1.2** The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems where required by Attachment 1.
- R2.** To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem(s) for use in identifying appropriate security controls for their assets, each Responsible Entity that owns any Generation Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide the following information to those Transmission Subsystem owners directly interconnected to that Generation Subsystem: *(Violation Risk Factor: High)*
- 2.1.** Description of the Generation Subsystem that includes Facility designation(s), or name(s), location, and other identifiers needed to identify the Facility(ies)
 - 2.2.** The Responsible Entity name
 - 2.3.** The BES impact categorization level
- R3.** As a step in assigning appropriate security controls for its assets, each Responsible Entity shall categorize and document BES Cyber Systems as follows: *(Violation Risk Factor: High)*
- 3.1.** Each Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R1 that has the potential to adversely impact any of the functions identified in *CIP-002 — Attachment 2 — Functions Critical to the Reliable Operation of the Bulk Electric System.*
 - 3.2.** For each BES Cyber System the Responsible Entity shall assign the same BES impact to the BES Cyber System as is assigned to the associated BES Subsystem. Where a BES Cyber System is associated with more than one BES Subsystem and the BES Subsystems have different BES impacts, the responsible entity shall assign the BES impact of the BES Cyber System to be the highest BES impact categorization level assigned to the associated BES Subsystems.

C. Measures

- M1.** The Responsible Entity shall have evidence, including its dated categorized list of BES Subsystems, to show that it has a categorized list of BES Subsystems as required by R1.
- M1.1.** The Responsible Entity shall have evidence that it updated its categorized list, if applicable, within 30 calendar days as a result of the commissioning of any new BES subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric as required by Requirement R1, Part 1.1.
- M1.2.** For each BES Subsystem where a Responsible Entity uses an engineering analysis or assessment method required by Attachment1, the Responsible Entity shall have evidence, such as a copy of the engineering analysis or assessment method used or a copy of the dated email transmittal, electronic voice recording, or other evidence to show that it received the approval of its Reliability Coordinator or Reliability Assurer for use of that method.
- M2.** The Responsible Entity shall have evidence of notifications as required by Requirement R2.
- M3.** The Responsible Entity shall have evidence, including its categorized list of BES Cyber Systems and the associated BES Subsystem impact categorizations as evidence that its BES Cyber Systems have been assigned BES impact categories as required by 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. Data Retention

Each Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence for Requirements R1 through R3, Measures M1 through M3 for a full calendar year or since the last update, whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant.

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

1.4. Compliance Monitoring and Assessment Processes

1.4.1 Compliance Audits

1.4.2 Self-Certifications

1.4.3 Spot Checking

1.4.4 Compliance Violation Investigations

1.4.5 Self-Reporting

1.4.6 Complaints

1.5. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
1	One or more Low Impact BES Subsystems has not been categorized.	<p>One or more Medium Impact BES Subsystems have not been categorized or have been miscategorized as Low Impact.</p> <p>OR</p> <p>The Responsible Entity failed to update its categorized list of BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 30, but within less than or equal to 40 calendar days of the completion of the change.</p>	<p>One High Impact BES Subsystem has not been categorized or has been miscategorized as Medium or Low Impact.</p> <p>OR</p> <p>The Responsible Entity failed to update its categorized list of BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 40, but within less than or equal to 50 calendar days of the completion of the change.</p>	<p>More than one High Impact BES Subsystems has not been categorized or has been miscategorized as Medium or Low Impact.</p> <p>OR</p> <p>The Responsible Entity failed to update its categorized list of BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 50 calendar days following the completion of the change.</p> <p>OR</p> <p>The Responsible Entity has not categorized any BES Subsystems it owns.</p>
2		The Responsible Entity has failed to notify its directly interconnected Transmission Subsystem owner(s) of its impact categorization level within 31 to 60 days of the categorization.	The Responsible Entity has failed to notify its directly interconnected Transmission Subsystem owner(s) of its impact categorization level within 61 to 90 days of the categorization.	The Responsible Entity has failed to notify its directly interconnected Transmission Subsystem owner(s) of its impact categorization for more than 90 days after the categorization.
3	Five or more Low Impact BES Cyber Systems have not been categorized.	Three or more Medium Impact BES Subsystems have not been categorized or have been miscategorized as Low Impact.	The Responsible Entity has not assigned an impact category to one High impact BES Cyber System or has miscategorized one High Impact BES Cyber System as Medium or Low Impact.	The Responsible Entity has not assigned an impact category to more than one High impact BES Cyber System or more than one High Impact BES Cyber Systems has been miscategorized as Medium or Low.

Standard CIP-002-4 — Cyber Security — BES Cyber System Categorization

				<p>OR</p> <p>The Responsible Entity has not performed and documented a categorization of any of the BES Cyber Systems it owns.</p> <p>OR</p> <p>The Responsible Entity does not have a list of all its BES Cyber Systems.</p>
--	--	--	--	---

E. Regional Variances

None.

Version History

Version	Date	Action	Change Tracking
4	12/29/2009	Initial draft of Version 4 Use of new format standard template	

CIP-002 — Attachment 1

Criteria for BES Impact Categorization of BES Subsystems

1. High BES Impact (H)

- 1.1. Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more, unless it has been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage or frequency support, in which case such Subsystems may be categorized as Medium BES Impact.
- 1.2. Each Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligations.
- 1.3. Each Generation Subsystem that has been pre-designated as Reliability “must run” units.
- 1.4. Each blackstart Generation Subsystem that has been included in the regional blackstart capability plan.
- 1.5. Each Transmission Subsystem that contains switching stations operated at 300 kV or higher in the Eastern and Western Interconnections, or operated at 200 KV or higher in other Interconnections, with 3 or more transmission lines leaving the station , unless it has been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Reliability Assurer, either for voltage or frequency stability support.
- 1.6. Each Transmission Subsystem comprising the Cranking Paths.
- 1.7. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in exceeding one or more Interconnection Reliability Operating Limits (IROLs) or exceeding limits requiring transmission loading relief (TLR), as determined by an engineering evaluation or other assessment method.
- 1.8. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 1, High Impact Subsystems, including as notified by the Generation Owner.
- 1.9. Each Transmission Subsystem identified as essential to meeting Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001 for High Impact Nuclear facilities as determined under Criteria 1.1 through 1.4 above.
- 1.10. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in voltage collapse as determined through an engineering evaluation or other assessment method.
- 1.11. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in electric system collapse due to frequency related instability as determined through an engineering evaluation or other assessment method.
- 1.12. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in complete operational failure of the transmission system or separation or Cascading outages.

- 1.13. Each Protection System, Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem operated at 300 kV and above in the Eastern and Western Interconnections, or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have an Adverse Reliability Impact.
- 1.14. Each BES Subsystem that performs automatic load shedding of 300 MW or more.
- 1.15. Each Control Center and backup Control Center performing Reliability Coordinator functions.
- 1.16. Each Control Center and backup Control Center performing Balancing Authority or Transmission Operator functions for transmission assets or generation assets of 2,000 MW or more.

2. Medium BES Impact (M)

- 2.1. Each Generation Subsystem with aggregate rated name-plate generation of 1000 MVA or more, not already included in section 1 above, unless it has been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage or frequency support.
- 2.2. Each Transmission Subsystem that contains switching stations operated at 200 kV or higher in the Eastern and Western Interconnections, or 100 kV or higher in other Interconnections, not already included in section 1 above, with 3 or more transmission lines leaving the station, unless they have been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage or frequency stability support.
- 2.3. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 2, Medium BES Impact.
- 2.4. Each Transmission Subsystem identified as essential to meeting Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001-1 for Medium Impact Nuclear facilities as determined under Criterion 2.1 above.
- 2.5. Each Protection System, Special Protection System (SPS) or Remedial Action Scheme (RAS) Subsystem operated at less than 300 kV in the Eastern and Western Interconnections, or less than 200 kV in other Interconnections that have an Adverse Reliability Impact.
- 2.6. Control Centers and backup Control Centers controlling transmission assets or generation of 1,000 MW or more, not included above.

3. Low BES Impact (L)

All other BES Subsystems on the list not mapped to Section 1 High BES Impact or Section 2 Medium BES Impact.

CIP-002 — Attachment 2

Functions Critical to the Reliable Operation of the Bulk Electric System

1. Dynamic response
2. Balancing Load and Generation
3. Controlling Frequency (real power)
4. Controlling Voltage (reactive power)
5. Managing Constraints
6. Control & Operation
7. Restoration of BES
8. Situational awareness
9. Inter-Entity coordination and communication

1. Dynamic Response

The Dynamic Response function includes those actions performed by BES elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition.

Aspects of BES Dynamic Response include, but are not limited to:

- Spinning reserve (contingency reserves)
 - Providing actual reserves
 - Monitoring that reserves are sufficient
- Governor Response
 - Control system used to actuate governor response
- Protection Systems (transmission & generation)
 - Line, bus, x-former, generator
 - Zone protection
 - Breaker protection
 - current, frequency, speed, phase
- Special Protection Systems or Remedial Action Schemes
 - Sensors, relays & breakers, possibly software
- Under and Over Frequency relay protection (includes automatic load shedding)
 - Sensors, relays & breakers
- Under and Over Voltage relay protection (includes automatic load shedding)
 - Sensors, relays & breakers
- Power System Stabilizers

2. Balancing Load and Generation

The Balancing Load and Generation function includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time.

Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of ACE
 - Field data sources (real time tie flows, frequency sources, time error, etc)
 - Software used to perform calculation
- Unit commitment
 - Know generation status & capability & restrictions (must runs, minimum run times, ramp, heat rates, etc) , load schedules
- Load management
 - Ability to identify load change need
 - Ability to implement load changes
- Demand Response
 - Ability to identify load change need
 - Ability to implement load changes
- Manually Initiated Load shedding
 - Ability to identify load change need
 - Ability to implement load changes
- Non-spinning reserve (contingency reserve)
 - Know generation status, capability, ramp rate, start time
 - Start units and provide energy

3. Controlling Frequency (real power)

The function of Controlling Frequency includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES.

Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
 - ACE, current generator output, ramp rate, unit characteristics
 - Software to calculate unit adjustments
 - Transmit adjustments to individual units
 - Unit controls implementing adjustments
- Regulation (regulating reserves)
 - Frequency source, schedule
 - Governor control system

4. Controlling Voltage (reactive power)

The function of Controlling Voltage includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES.

Aspects of the Controlling Voltage function include, but are not limited to:

- AVR (Automatic Voltage Regulation)
 - Sensors, stator control system, feedback
- Capacitive resources

- Status, control (manual or auto), feedback
- Inductive resources (transformer tap changer, or inductors)
 - Status, control (manual or auto), feedback
- SVC (Static VAR Compensators)
 - Status, computations, control (manual or auto), feedback

5. Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES.

Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC)
- Interchange schedules
- Generation re-dispatch and unit commit
- Identify and monitor SOL's & IROL's
- Identify and monitor Flowgates

6. Control & Operation

Control & Operation includes those activities, actions and conditions that provide monitoring and control of BES elements.

An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches (such as SCADA)

7. Restoration of BES

The Restoration of BES function includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance.

Aspects of the Restoration of BES function include, but are not limited to:

- Blackstart restoration including planned cranking path
- Off-site power for nuclear facilities.

8. Situational Awareness

The Situational Awareness function includes activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions.

Aspects of the Situation Awareness function include, but are not limited to:

- Monitoring and alerting (such as EMS alarms)
- Change management
- Current Day & Next Day planning
- Contingency Analysis

- Frequency monitoring

9. Inter-Entity Coordination and Communication

The Inter-Entity coordination and communication function includes activities, actions and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES.

Aspects of the Inter-Entity Coordination and Communication function include, but are not limited to:

- Scheduled interchange
- Facility operational data and status
- Operational directives