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)
9. Version 4 of CIP-002 posted for informal comment (December 29, 2009)
10. Version 1 of CIP-010 and CIP-011 posted for informal comment (May 3, 2010)

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Post for 45-day comment period and pre-ballot review.	7/26/2010
2. Conduct initial ballot.	8/30/2010
3. Post response to comments on initial ballot.	9/10/2010
4. Conduct Second Ballot	10/04/2010
5. Post response to comments on second ballot	10/29/2010
6. Conduct Third (recirculation) ballot.	11/08/2010
7. Submit standard to BOT for adoption.	12/10/2010
8. File standard with regulatory authorities.	12/24/2010

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.

BES Cyber System Component – One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.

BES Cyber System – One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.

Control Center – A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

- 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 real-time operational decisions regarding reliability and operability of the BES),
- Alarm monitoring and processing specific to operation and restoration function, or
- Coordination of BES restoration activities.

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

- Critical Assets
- Critical Cyber Assets
- Cyber Assets

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-010-1

3. **Purpose:** To identify and categorize BES Cyber Systems that execute or enable functions essential to reliable operation of the BES, for the application of cyber security requirements commensurate with the adverse impact that loss, compromise or misuse of those BES Cyber Systems could have on the reliability of the BES.

4. **Applicability:**

   4.1. Functional Entities:

   For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are 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. Distribution Provider

   4.1.11. NERC

   4.1.12. Regional Entity

   4.2. **Physical Facilities**

   4.2.1. All BES Facilities under NERC jurisdiction 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.

5. **Effective Date:** To be addressed as part of the implementation plan that is currently under development

B. Requirements

R1. Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in *CIP-010 – 1 Attachment I – Functions Essential to the Reliable Operation of the BES* to identify BES Cyber Systems for the application of security requirements. *(Violation Risk Factor: High)*

R2. Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in *CIP-010-1 Attachment II – Impact Categorization of BES Cyber Systems* to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES. *(Violation Risk Factor: High)*

R3. To ensure the application of adequate requirements on its BES Cyber Systems, each Responsible Entity shall: *(Violation Risk Factor: High)*

3.1. Review the identification and categorization of its BES Cyber Systems within 36 months of the last identification and categorization

3.2. Review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it owns

3.3. Update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of such change to the BES.

C. Measures

M1. Each Responsible Entity shall have evidence identifying and documenting each of its BES Cyber Systems that execute or enable functions defined *CIP-010 – 1 Attachment I – Functions Essential to the Reliable Operation of the BES* as required in R1.

M2. Each Responsible Entity shall have evidence identifying the categorization of each of its BES Cyber Systems that execute or enable functions defined in *CIP-010 – 1 Attachment I – Functions Essential to the Reliable Operation of the BES* categorized in accordance with *CIP-010 – 1 Attachment II – Impact Categorization of BES Cyber Systems* as required in R2.

M3. Each Responsible Entity shall have evidence that it has reviewed its identification and categorization of its BES Cyber Systems and updated the applicable documentation within 45 calendar days of the completion of the review or the completion of such change to the BES.

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. 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, R2 and R3, and Measures M1, M2 and M3 for a full calendar year or since the last audit, whichever is longer.

If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or as specified above, whichever is longer.

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

1.3. 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

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	5% or fewer BES Cyber Systems have not been identified.	More than 5% but less than or equal to 10% of BES Cyber Systems have not been identified.	More than 10% but less than or equal to 15% of BES Cyber Systems have not been identified.	More than 15% of BES Cyber Systems have not been identified.
R2	5% or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.	More than 5% but less than or equal to 10% of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.	More than 10% but less than or equal to 15% of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.	More than 15% of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.
R3	The Responsible Entity failed to update its documentation of BES Cyber Systems in accordance with Requirement R3 for more than 45, but less than or equal to 60 calendar days of the completion of the change.	The Responsible Entity failed to update its documentation of BES Cyber Systems in accordance with Requirement R3 for more than 60, but less than or equal to 70 calendar days of the completion of the change.	The Responsible Entity failed to update its documentation of BES Cyber Systems in accordance with Requirement R3 for more than 70, but less than or equal to 80 calendar days of the completion of the change.	The Responsible Entity failed to update its documentation of BES Cyber Systems in accordance with Requirement R3 for more than 80 calendar days following the completion of the change.

E. Regional Variances

None.

Version History

Version	Date	Action	Change Tracking
1.000	5/3/2010	Initial draft of Version 1 posted for informal comment.	

CIP-010-1 — Attachment I

Functions Essential to Reliable Operation of the Bulk Electric System

The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes.

Dynamic Response — Actions performed by BES elements or Facilities 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.

Balancing Load and Generation — Activities, actions and conditions for monitoring and controlling generation and load.

Controlling Frequency (Real Power) — Activities, actions and conditions to control frequency within defined bounds.

Controlling Voltage (Reactive Power) — Activities, actions and conditions to control voltage within defined bounds.

Managing Constraints — Activities, actions and conditions to maintain operation of BES elements within their design limits and constraints.

Monitoring & Control — Activities, actions and conditions that provide monitoring and control of BES elements.

Restoration of BES — Activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance.

Situational Awareness — Activities, actions and conditions to assess the current, expected, and anticipated state of the BES.

Inter-Entity Real-Time Coordination and Communication — Activities, actions and conditions for real-time coordination and communication between Responsible Entities' System Operators.

CIP-010-1 — Attachment II

Impact Categorization of BES Cyber Systems

1. High Impact Rating (H)

Each BES Cyber System that can affect operations for:

1.1. Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation Facilities), whose aggregate rated net Real Power capability exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group . In the case where no Contingency Reserve or total reserve sharing obligations have been established, Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW.

1.2. Synchronous condensers, static VAR compensators and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more.

1.3. Generation Facilities that are pre-designated as reliability "must run" assigned units that have Wide Area reliability impacts.

1.4. Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan.

1.5. Transmission Facilities with four or more Transmission lines operated at 300 kV or higher in the Eastern and Western Interconnections or operated at 200 kV or higher in the Texas and Quebec Interconnections.

1.6. Facilities required to support a primary Cranking Path used in a Transmission Operator's restoration plan per EOP-005.

1.7. Transmission Facilities, including Flexible AC Transmission Systems (FACTS), that, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more Interconnection Reliability Operating Limits (IROLs). Where IROLs are not used or are not available, Transmission Facilities, including FACTS, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in instability, uncontrolled separation or Cascading.

1.8. Transmission Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of generation Facilities, singularly or in combination, with aggregate rated capabilities described in Part 1.1 above.

1.9. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001 for Nuclear facilities.

1.10. Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements and that have impact beyond the local area.

1.11. BES Elements that perform automatic aggregate load shedding of 300 MW or more.

1.12. Reliability Coordinator functions performed by primary or backup Control Centers.

1.13. Balancing Authority functions performed by primary or backup Control Centers, of Transmission Facilities or generation Facilities, singularly or in combination, of 4,000 MW

or more in Eastern and Western Interconnections and 2,000 MW or more in the Texas and Quebec Interconnections.

1.14. Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations operating at 300 kV or above in the Eastern and Western Interconnections or operating at 200 kV and above in Texas and Quebec Interconnections or functionality that remotely controls a BES Cyber System with a High Impact Rating.

2. Medium Impact Rating (M)

BES Cyber Systems that can affect operations for:

2.1. Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to most current rated net Real Power capability of 1000 MW or more, not included in Section 1.

2.2. Synchronous condensers, static VAR compensators and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 500 MVAR or more, not included in Section 1.

2.3. Generation Facilities that are pre-designated as Reliability "must run" assigned units not identified in Part 1.3.

2.4. Transmission Facilities with four or more transmission lines operated at 200 kV or above in the Eastern and Western Interconnections, or 100 kV or above in the Texas and Quebec Interconnections, not included in Section 1.

2.5. Transmission Facilities that if destroyed, degraded, misused or otherwise rendered unavailable, would result in the loss of generation Facilities, singularly or in combination, with aggregate rated capabilities described in Part 2.1 above, not included in Section 1.

2.6. Transmission Facilities operated at 300 kV or higher in the Eastern and Western Interconnections or operated at 200 kV or higher in Texas and Quebec Interconnections not included in Section 1.

2.7. Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations operated at 200 kV or above in the Eastern and Western Interconnections and 100kV or above in the Texas and Quebec Interconnections, or functionality that remotely controls a BES Cyber System with a Medium Impact Rating, not included in Section 1.

2.8. Balancing Authority functions performed by primary or backup Control Centers, of Transmission Facilities or generation Facilities, singularly or in combination, of 2,000 MW or more in the Eastern and Western Interconnections and 1,000 MW or more in the Texas and Quebec Interconnections, not included in Section 1.

3. Low Impact Rating (L)

All other documented BES Cyber Systems that can affect operations and are not categorized in Section 1 as having a High Impact Rating or in Section 2 as having a Medium Impact Rating.