Standard Development Timeline

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

Note: On September 21, 2012, this draft was revised to clarify references from "generator interface facility" to "generator interconnection Facility" in Attachment 1, criteria 2.4, 2.5, and 2.8. As noted on page 33 of the consideration of comments, form A, the SDT intended to use "generator interconnection Facility." It also corrects instances of incorrect functional model references from "Generation Operator" to "Generator Operator" and corrects the numbering format in Attachment 1, section 3.

No other changes were made to this standard or any of the other CIP V5 standards currently posted, except for a conforming change from "Generation Operator" to "Generator Operator" in the definitions document.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-day formal comment period. An initial concept paper, ~~-~~Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5~~-~~, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ~~first~~ ballot.~~–~~ A second posting of Version 5 ~~reverts to the original organization of the standards, with some changes, and~~was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – ~~The Version 5~~ CIP ~~Cyber Security Standards, except for CIP-003-5, Requirement R2,~~ 002-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. ~~CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.~~[1]
2. In those jurisdictions where no regulatory approval is required~~, the Version 5~~ CIP ~~Cyber Security Standards, except for CIP-003-5, Requirement R2,~~ 002-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, ~~and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval,~~ or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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.	

~~[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.~~

3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

~~4.~~1. Title: Cyber Security — BES Cyber System Categorization

~~5.~~2. Number: CIP-002-5

~~6.~~3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets 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 reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

~~7.~~4. Applicability:

4.1. Functional Entities: ~~———~~ For the purpose of the requirements contained herein, the following list of ~~Functional Entities~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

4.1.1. Balancing Authority

~~7.1.1. Distribution Provider that owns Facilities described in 4.2.2~~

~~7.1.2. Generator Operator~~

~~7.1.3. Generator Owner~~

~~7.1.4. Interchange Coordinator~~

~~7.1.5. Load-Serving Entity that owns Facilities described in 4.2.1~~

~~7.1.6. Reliability Coordinator~~

~~7.1.7. Transmission Operator~~

~~7.1.8. Transmission Owner~~

~~4.2. Facilities:~~

~~7.2.1. Load Serving Entity:~~ ~~One~~one or more of the ~~UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard~~following Facilities, systems, and ~~that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.~~

~~4.2.2~~**4.1.2. ~~Distribution Provider: One or more of the Systems or programs designed, installed, and operated~~**equipment for the protection or restoration of the BES:

4.1.2.1. ~~A~~ Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS ~~System~~) system that~~:~~:

4.1.2.1.1. is part of a Load shedding program ~~required by~~that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ~~that~~

~~4.1.2.1.~~4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. ~~A~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. ~~A~~Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

~~1.~~4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers ~~and Load-Serving Entities:~~ :

~~4.2.3~~All BES Facilities.

~~4.2.4~~**4.2.3. Exemptions:** The following are exempt from Standard CIP-002-5:

~~4.2.4.1~~**4.2.3.1.** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.4.2~~**4.2.3.2.** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.4.3~~**4.2.3.3.** ~~In nuclear plants, the Systems~~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.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~8.~~5. Background:

This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, ~~Systems~~systems, and equipment~~:~~, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

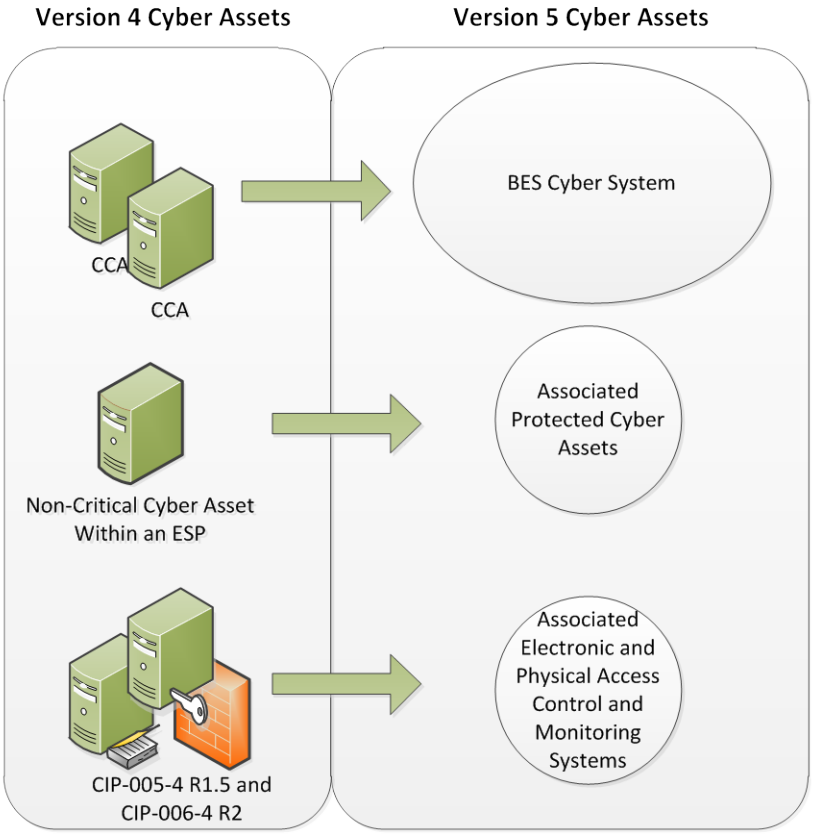
Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300

MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets~~. So~~ , and it becomes clearer in the requirement

that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System~~.~~ within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify ~~them~~BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems ~~and their associated BES Cyber Assets~~ for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, ~~Parts~~Criteria 1.1 to 1.4 and ~~Parts~~Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the ~~rest~~remainder of the Version 5 CIP Cyber Security Standards.

~~Associated~~ Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their ~~proximity~~location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ~~–~~("PACS")~~–~~ Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

~~**Rationale – R1:**~~

~~BES Cyber Systems and their associated BES Cyber Assets have varying impact on the reliable operation of the BES. Once they have been identified, they must be categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to categorize these BES Cyber Systems in accordance with their impact on the BES. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.~~

~~The configuration of the BES is subject to changes due to new demands and requirements for Bulk Power and to environmental changes and operational events. When changes to the BES are planned, the effect of these changes on the set of identified and categorized BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them.~~

Rationale – R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

R1. Each Responsible Entity shall~~:~~ implement a process that considers each of the following assets for purposes of parts R1.1 through R1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

1. ~~Identify Facilities,~~ Control Centers and backup Control Centers;
2. Transmission substations and stations;
3. Generation resources;
4. Systems~~, or equipment that meet the criteria~~ and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration;

5. Special Protection Systems that support the reliable operation of the Bulk Electric System; and

6. For Distribution Providers, Protection Systems specified in ~~CIP-002-5,~~ Applicability section 4.2.1 above.

~~**1.1.**~~**R1.1.** Identify each of the high impact BES Cyber Systems according to Attachment 1~~ – Impact Rating Criteria Parts 1.1 to~~, Section 1~~.4 and Parts 2.1 to 2.11;~~, if any, at each asset;

~~**1.2.**~~**R1.2.** Identify each ~~high~~of the medium impact BES Cyber ~~System and its associated BES Cyber Asset(s) used for the Facilities,~~ Systems~~, or equipment identified in Requirement R1 Part 1.1~~ according to ~~the criteria contained in CIP-002-5,~~ Attachment 1~~ – Impact Rating Criteria;~~, Section 2, if any, at each asset; and

~~**3.**~~ Identify each ~~medium~~asset that contains a low impact BES Cyber System ~~and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1~~ according to ~~the criteria contained in CIP-002-5,~~ Attachment 1~~ – Impact Rating Criteria;~~

- ~~BES Cyber Systems which are not included in high impact or medium impact shall default to the category of low impact and do not require discrete identification; and~~

~~**1.4.**~~**R1.3.** ~~Review (and update as needed) the identification in Requirement R1, Parts 1.1, 1.2, and 1.3 within 60 calendar days of when a change to BES Elements or Facilities~~, Section 3, if any (a discrete list of low impact BES Cyber Systems is ~~placed into operation, which is planned to be in service for more than six calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category.~~not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, ~~Parts 1.1, 1.2 and 1.3, and a list of changes to the BES (with a date for each change) that cause a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.~~ and Parts R1.1 and R1.2.

Rationale – R2

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

R2. The Responsible Entity shall ~~have~~: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

R2.1 Review (and update as needed) the identification in Requirement R1 and its parts at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

~~**R2.**~~**R2.2** Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once ~~each calendar year, not to exceed~~every 15 calendar months ~~between approvals~~, even if it has no identified items in Requirement R1~~, Parts 1.1, 1.2, or 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*~~.

~~**M2.**~~ **M2.** Acceptable evidence includes, but is not limited to, electronic or physical dated ~~and signed~~ records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate ~~review and update, where applicable, the identification and categorization of Facilities, Systems,~~approve the identifications required in Requirement R1 and ~~equipment, and their associated BES Cyber Systems and BES Cyber Assets,~~its parts at least once ~~each calendar year, not to exceed~~every 15 calendar months ~~between occurrences~~, even if it has none identified in Requirement R1~~, Parts 1.1, 1.2, or 1.3~~ and its parts, as required by ~~requirement~~Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~entity~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

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

- Each Responsible Entity shall retain ~~data or~~ evidence ~~for~~of each requirement in this standard for three calendar years ~~or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

~~Table of Compliance Elements~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	
~~R1~~	~~Operations Planning~~	~~High~~	~~For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, five percent or fewer Facilities have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1;~~ ~~Or~~ ~~For Responsible Entities with a total of 40 or fewer Facilities, 2 or fewer Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1;~~ ~~Or~~ ~~For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer of high and medium impact BES Cyber Systems have not been identified or categorized or have been incorrectly~~	~~For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than five percent but less than or equal to 10 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1;~~ ~~Or~~ ~~For Responsible Entities with a total of 40 or fewer Facilities, more than two, but fewer than four Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1;~~ ~~Or~~ ~~For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Assets, more than five percent but less than or equal to 10 percent~~	~~For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than 10 percent but less than or equal to 15 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1;~~ ~~Or~~ ~~For Responsible Entities with a total of 40 or fewer Facilities, more than four, but fewer than six Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1;~~ ~~For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Assets, more than 10 percent but less than or equal to 15 percent~~	~~Fo En th Fa Re 1.1 pe ha id be id Re 1.1 Or Fo En 40 m in Pa be ha id Re 1.1 Or Fo En th hi im Sy pe BE ha ca be~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	
			~~categorized at a lower category;~~ ~~Or~~ ~~For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Assets, five or fewer high and medium impact BES Cyber Assets have not been identified or categorized or have been incorrectly categorized at a lower category;~~ ~~Or~~ ~~The Responsible Entity failed to update its documentation of high and medium impact BES Cyber Assets in accordance with Requirement R1, Part 1.4 for more than 60, but less than or equal to 70 calendar days following the completion of the change.~~	~~of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category;~~ ~~Or~~ ~~For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Assets, more than five but less than or equal to 10 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category;~~ ~~Or~~ ~~The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with Requirement R1, Part 1.4 for more than 70, but less than or equal to 80 calendar days following the completion of the change.~~	~~of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category;~~ ~~Or~~ ~~For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category;~~ ~~Or~~ ~~The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with Requirement R1, Part 1.4 for more than 90, but less than or equal to 100 calendar days following the completion of the change.~~	~~ca~~ ~~ca~~ ~~Or~~ ~~Fo~~ ~~En~~ ~~10~~ ~~mo~~ ~~Cy~~ ~~th~~ ~~Cy~~ ~~no~~ ~~or~~ ~~inc~~ ~~at~~ ~~Or~~ ~~Th~~ ~~fai~~ ~~de~~ ~~Cy~~ ~~ac~~ ~~Re~~ ~~1.~~ ~~ca~~ ~~fo~~ ~~co~~ ~~ch~~
~~R2~~	~~Operations Planning~~	~~Lower~~	~~The Responsible Entity failed to complete its annual review or approval by the CIP~~	~~The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager~~	~~The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager~~	~~Th~~ ~~fai~~ ~~an~~ ~~ap~~ ~~Se~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	
			~~Senior Manager according to Requirement R2 for more than 30, but less than or equal to 40 calendar days of the latest required date.~~	~~according to Requirement R2 for more than 40, but less than or equal to 50 calendar days of the latest required date.~~	~~according to Requirement R2 for more than 50, but less than or equal to 60 calendar days of the latest required date.~~	~~ac Re mo da re~~

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center~~,~~ or backup Control Center~~, and associated data centers~~ used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center~~,~~ or backup Control Center~~, and associated data centers~~ used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of ~~1500~~3000 MW in a single Interconnection, or 2) ~~that includes control of~~for one or more of the ~~generation~~ assets that meet ~~criteria~~criterion 2.3, 2.6, ~~and~~or 2.9.

1.3. Each Control Center~~,~~ or backup Control Center~~, and associated data centers~~ used to perform the functional obligations of the Transmission Operator~~, that includes control of~~ for one or more of the assets that meet ~~criteria~~criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center~~,~~ or backup Control Center~~, and associated data centers~~ used to perform the functional obligations of the ~~Generation~~ Generator Operator ~~that includes control~~ for one or more of the assets that meet criterion 2.1~~) for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection or 2) that includes control of one or more of the generation assets that meet criteria~~, 2.3, 2.6, ~~and~~or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1~~,~~ above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of

1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary~~,~~ to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation that ~~are operating between 200 kV and 499 kV, are~~is connected to three or more other Transmission stations or substations~~,~~ and ~~which possess~~has an "aggregate weighted values" exceeding 3000 according to the table below. The "aggregate weighted value" for a ~~Transmission Facility~~single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming ~~or~~and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
~~100kV to 199 kV~~less than 200 kV (not applicable)	~~0~~ (not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, ~~Parts~~criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS~~)~~), or automated switching ~~Systems~~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 or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each ~~System~~system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing ~~Under Voltage Load Shedding~~ undervoltage load shedding (UVLS) or ~~Under Frequency Load Shedding~~underfrequency load shedding (UFLS~~), as required by its regional~~) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control ~~Centers and associated data centers~~Center or backup Control Center, not already included in High Impact Rating (H~~),~~) above, ~~that: (1)~~used to perform the functional obligations of ~~Balancing Authority or Transmission~~the Generator Operator~~, or (2) control~~ for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding ~~300~~1500 MW ~~or more~~in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of ~~BES~~the Transmission Operator not included in High Impact Rating (H), above.

~~**2.11.**~~**2.13.** Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, 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.

3. Low Impact Rating (L)

~~Each BES Cyber System associated with:~~

~~**3.1.** BES Facilities not categorized in Section 1 as having a High Impact Rating (H) or Section 2 as having a Medium Impact Rating (M).~~

~~**3.2.** Blackstart Resources.~~

~~**3.3.** Elements in the Cranking Path and initial switching requirements.~~

BES Cyber Systems ~~that are~~ not included in ~~high impact~~Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

4.1. Control Centers and ~~medium impact shall default to the category of low impact~~backup Control Centers.

4.2. Transmission substations and ~~do not require discrete identification~~stations.

4.3. Generation resources.

4.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

4.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

4.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A~~-~~ BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	~~LSE~~	GOP	GO
Dynamic Response		X	X	X	X	~~X~~	X	X
Balancing Load & Generation	X	X	X	X	X	~~X~~	X	X
Controlling Frequency		X					X	X
Controlling Voltage			X	X	X	~~X~~		X
Managing Constraints	X		X				X	
Monitoring and Control			X				X	
Restoration			X				X	
Situation Awareness	X	X	X				X	
Inter-Entity coordination	X	X	X	X			X	X

Dynamic Response

The Dynamic Response Operating Service 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. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, ~~x formers~~transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays ~~&~~, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP~~,LSE~~)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP~~,LSE~~)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service 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 Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA) ~~(RC)~~
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP~~,LSE~~)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP~~,LSE~~)

- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service 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 (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service 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:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

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) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control 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
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service 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:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure 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:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day ~~&~~and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure 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:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers ~~and Load Serving Entities~~

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

~~Similarly, it is expected that only Load-Serving Entities that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. These qualifications are based on the requirements for registration as a Load Serving Entity. Additional qualifications for thresholds in Attachment 1, as specified in Section 4 of CIP-002, also apply.~~

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems ~~and their associated BES Cyber Assets~~ according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of

the impact that the ~~Facilities, Systems and equipment~~BES assets that these BES Cyber Systems support, on the reliable operation of the BES.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for ~~Facilities, Systems and equipment~~BES assets not specified in ~~Parts~~Attachment 1, Criteria 1.1 – 1.4 and ~~Parts~~Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1. ~~While the criteria are based on the scope of the BES Facilities, Systems and equipment, this is used here as a measure of the impact of the BES Cyber System for the purpose of categorization.~~

- When the drafting team uses the term "Facilities", ~~it leaves~~there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5, these groups of Facilities, systems, and equipment are designated as BES Assets. For example, an identified BES Asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers and associated data centers, that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or ~~Generation~~ Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, ~~Parts~~Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named ~~Functional Entities~~functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are ~~parts~~criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- ~~Part~~Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used

1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units ~~with capability higher than 1500 MW~~ are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In ~~Part~~Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid BES Adverse Reliability Impacts in the ~~long term~~ planning horizon of one year or more are categorized as medium impact. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  ~~In the specification of the "long-term planning horizon," in this criterion, the drafting team sought to ensure that such BES Facilities would be designated in the time horizon described in the NERC document "Time Horizons," which defines long-term planning horizon as "a planning horizon of one year or longer."~~

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, ~~or a Category D contingency as defined in TPL-004,~~ then BES Cyber Systems for that unit are categorized as medium impact.

  ~~Part~~The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the RRO which coordinates actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability

Coordinators or other necessary party), usually in the form of a formal agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  ~~-~~IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- ~~Part~~Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- ~~Part~~Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the ~~Transmission Operator or Balancing Authority, and Generation~~ Generator Operator for an aggregate generation of ~~300~~1500 MW or higher in a single interconnection, and ~~which~~that have not already been included in Part 1. The value of 300 MW is the same value used for UFLS and UVLS. ~~This ensures that Control Centers for significant impact are included. Smaller Control Centers that qualify for the definition of generation Control Centers, but which are really controlling local generation for small downstream generation facilities and do not meet the 300 MW threshold are categorized as low impact.~~

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

~~Parts~~

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as

stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 ~~2.11~~ through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). ~~Part~~Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- ~~Part~~Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in ~~Part 1~~Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it ~~doesn't~~does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- ~~Part~~Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

- 230 kV –> 700 MVA
- 345 kV –> 1,300 MVA
- 500 kV –> 2,000 MVA
- 765 kV –> 3,000 MVA

~~In the case of~~In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

- For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location~~.~~ or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers ~~would~~may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

  ~~Part~~
- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.
- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

- ~~Part~~Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- ~~Part~~Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in ~~Parts~~Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- ~~Part~~Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- ~~Part~~Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of ~~Part~~Criterion 2.~~12~~10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those ~~Under Frequency Load Shedding~~ underfrequency load shedding (UFLS) ~~facilities~~Facilities and ~~Systems~~systems and ~~Under Voltage Load Shedding~~ undervoltage load shedding (UVLS) ~~Systems~~systems and Elements that would be ~~implemented as part of~~ subject to a regional ~~load~~Load shedding requirement to prevent Adverse Reliability Impact. These include automated ~~Under Frequency Load Shedding Systems~~UFLS systems or ~~Under Voltage Load Shedding Systems~~UVLS systems that are capable of ~~load~~Load shedding 300 MW or more. It should be noted that those qualifying ~~Systems~~systems which require a human operator to arm the ~~System~~system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW ~~rating~~Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  ~~Within an operational environment, the drafting team understands that the real-time impact to the Bulk Electric System of a loss of load, or the equivalent amount of generation, will be similar, with loss of load resulting in a frequency high condition and a loss of generation resulting in a frequency low condition.~~ This particular threshold (300 MW) was

provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market.

~~Part 2.11~~The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of ~~Balancing Authorities or Transmission Operators not already categorized as high impact and at generation Control Centers that control generation of 300 MW or more. These include Control Centers for Transmission Owners which perform the function obligation of a Transmission Operator.~~a Transmission Operator and that have not already been categorized as high impact.

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that ~~these~~low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and

other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

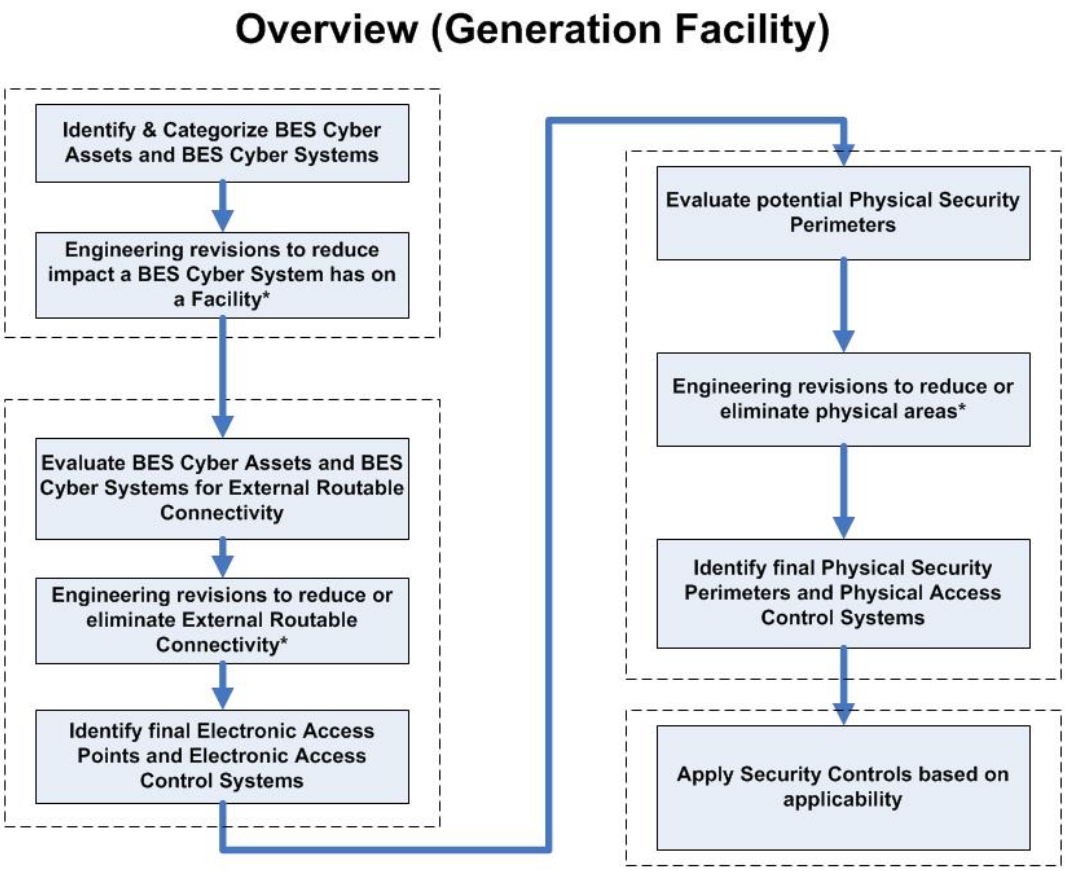
Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements 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, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.