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.

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).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-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. ~~This version (~~A first posting of Version 5~~)~~ was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards, with some changes, and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~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 ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~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.

[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.

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.~~Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
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 ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — BES Cyber ~~Asset and BES Cyber~~ System Categorization

2. Number: CIP-002-5

3. Purpose: To identify and categorize BES Cyber ~~Assets and BES Cyber~~ Systems ~~that execute or enable functions essential to reliable operation of the BES,~~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 ~~Assets~~Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems ~~could have on the reliability of~~support appropriate protection against compromises that could lead to misoperation or instability in 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 Balancing Authority

4.1.2 Distribution Provider that owns Facilities ~~that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~ **described in 4.2.2**

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~
- ~~A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard~~
- ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities ~~that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~ **described in 4.2.1**

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~

- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~4.1.7 NERC~~

~~4.1.8 Regional Entity~~

~~4.1.9~~4.1.7 **Reliability Coordinator**

~~4.1.10~~4.1.8 **Transmission Operator**

~~4.1.11~~4.1.9 **Transmission Owner**

4.2. Facilities:

~~4.2.1~~ **Load Serving Entity:** One or more ~~Facilities~~of the UFLS or UVLS Systems that are part of ~~any of the following systems or programs designed, installed, and operated for the protection of the BES:~~

- ~~4.2.1~~ ~~A UFLS~~a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

4.2.2 Distribution ~~Providers~~Provider: One or more ~~Facilities that are part of any of the following systems~~of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- ~~A~~ UFLS ~~program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS~~or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- ~~A~~ Special Protection System or Remedial Action Scheme ~~required by a NERC or Regional Reliability Standard~~
- ~~A Transmission~~ where the Special Protection System ~~required by a NERC~~ or Remedial Action Scheme is required by a NERC or Regional Reliability Standard

- ~~Its Transmission Operator's restoration plan~~

- ~~**All other**~~ A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard

- 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.

4.2.3 Responsible Entities~~:~~ listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

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

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

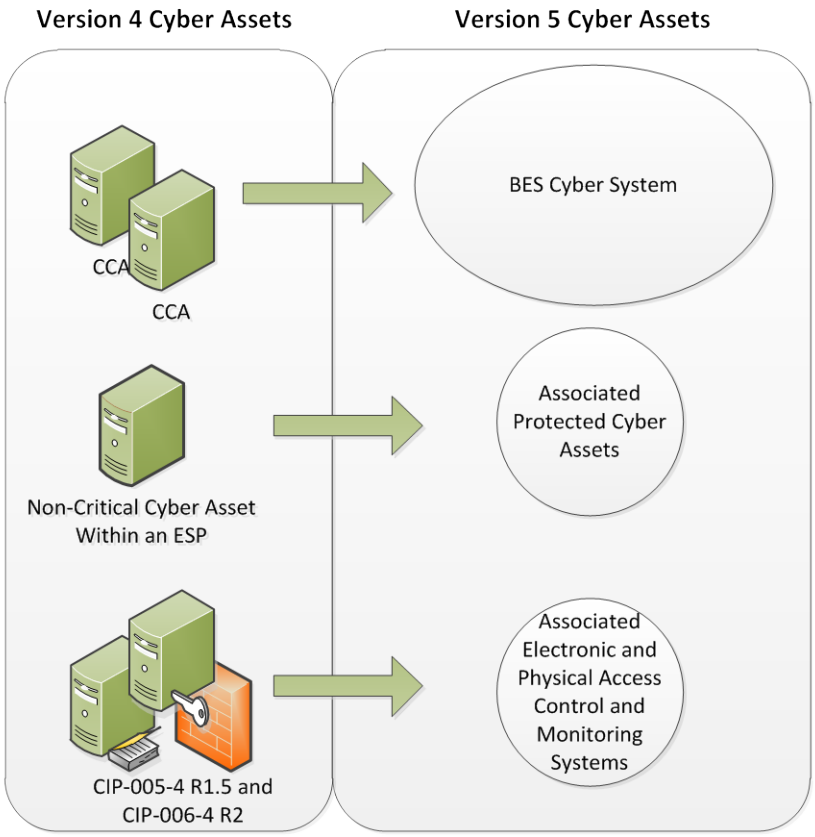
4.2.4.3 In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

5. Background:

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

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 ~~this~~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 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. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or ~~they~~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.

~~**BES Reliability Operating Services**~~

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber ~~Assets and BES Cyber~~ Systems that would impact the reliable operation of the BES. In order to identify them, Responsible Entities determine whether the BES Cyber ~~Assets~~Systems perform or support any BES ~~Reliability Operating Service. These services are functions that provide services~~reliability function according to those reliability tasks identified for ~~the reliable operation of the BES and are based on the functions defined~~functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber ~~Assets~~Systems and their associated BES Cyber ~~Systems~~Assets that perform or support ~~BES Reliability Operating Services.~~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 ~~reliability and operability~~reliable operation of the BES. To provide a better defined time horizon than "~~real~~Real-time~~",~~" BES Cyber Assets are those ~~cyber assets~~Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the ~~BES Reliability Operating Services~~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~~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 ~~and their BES Cyber Assets~~ 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~~high impact and ~~Medium~~medium impact categories. All ~~other~~ BES Cyber Systems ~~are deemed~~for Facilities not included in Attachment 1 – Impact Rating Criteria, Parts 1.1 to 1.4 and Parts 2.1 to 2.11 default to be ~~Low Impact~~low impact.

This general process of categorization of BES Cyber Systems ~~and BES Cyber Assets~~ based on impact on the ~~BES Reliability Operating Services~~reliable operation of the BES is consistent with risk management approaches for the purpose of application of

cyber security ~~controls~~requirements in the rest of Version 5 ~~cyber~~ Cyber Security Standards.

Associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their proximity within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security ~~standards.~~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 – 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 – Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets – 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.

~~**Rationale – R1:**~~

~~Cyber Assets and Cyber Systems have varying impact on the reliability and operability 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 I provides a set of "bright-line" criteria that the Responsible Entity must use to categorize these BES Cyber Assets and 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 Assets and BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them.~~

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.

R1. Each Responsible Entity ~~that owns BES Cyber Assets and BES Cyber Systems~~ shall ~~identify and categorize its High and Medium~~: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

1.1. Identify Facilities, Systems, or equipment that meet the criteria specified in CIP-002-5, Attachment 1 – Impact Rating Criteria Parts 1.1 to 1.4 and Parts 2.1 to 2.11;

1.2. Identify each high impact BES Cyber ~~Assets~~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~~1 – Impact ~~*Categorization of*~~Rating Criteria;

1.3. Identify each medium impact BES Cyber ~~*Assets*~~System and its associated BES Cyber Asset(s) used for the Facilities, Systems~~. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed~~, or equipment identified in Requirement R1 Part 1.1 according to ~~be Low~~the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;

~~**R1.**~~• 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~~. *[Violation Risk Factor: High][Time Horizon: Operations Planning]*~~; and

~~**Rationale – R2**~~

~~The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The mis-categorization or non-categorization of a BES Cyber System or BES Cyber Asset 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.~~

Rationale – R2

The lists required by Requirement R1 are reviewed once a year 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.

~~**1.1.**~~**1.4.** ~~Update~~Review (and update as needed) the identification in Requirement R1, Parts 1.1, 1.2, and ~~categorization~~1.3 within ~~30~~60 calendar days of when a change to BES Elements ~~and~~or Facilities is placed into operation, ~~that~~which is ~~intended~~planned to be in service for more than ~~6~~six calendar months and ~~that~~ causes a change in the identification or categorization of the BES Cyber ~~Assets or BES Cyber~~ Systems from a lower to a higher impact category.

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists ~~identifying the categorization of each of its BES Cyber Assets and BES Cyber Systems in the High and Medium categories as~~ required ~~in R1~~ 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. ~~Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.~~

R2. The Responsible Entity shall have its CIP Senior Manager or delegate approve the ~~identification and categorization~~identifications required by Requirement R1 ~~initially upon the effective date of the standard and~~ at least once each calendar year ~~thereafter~~, not to exceed 15 calendar months between approvals, even if it has no

identified ~~High~~items in Requirement R1, Parts 1.1, 1.2, or ~~Medium BES Cyber Assets or BES Cyber Systems~~1.3. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning~~]~~].*

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate review and update, where applicable, the identification and categorization of ~~BES Cyber Assets~~Facilities, Systems, and equipment, and their associated BES Cyber Systems and BES Cyber ~~Systems initially upon the effective date of the standard and~~ Assets, at least once each ~~subsequent~~ calendar year, not to exceed 15 calendar months between occurrences, even if it has ~~no~~none identified ~~High or Medium BES Cyber Assets~~in Requirement R1, Parts 1.1, 1.2, or ~~BES Cyber Systems. (~~1.3, as required by requirement R2~~)~~.

~~B.~~C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity~~; or~~
- ~~If the Responsible Entity works for~~ shall serve as the Compliance Enforcement Authority ("CEA") unless the ~~Regional Entity, then the~~ applicable entity is owned, operated, or controlled by the Regional Entity ~~will establish an agreement with~~. In such cases the ERO or ~~another~~a Regional entity approved by ~~the ERO and FERC (i.e., another Regional Entity) to be responsible for compliance enforcement.~~
- ~~If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and~~ FERC or other applicable governmental ~~authorities shall serve as the Compliance Enforcement Authority.~~
- ~~If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC~~authority shall serve as the ~~Compliance Enforcement Authority~~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 may ask an entity to provide other evidence to show that it was ~~complaint~~compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for 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 ~~found compliant~~mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority 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	Severe VSL
R 1	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	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	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	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than 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 six 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

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			with more than a total of 100 ~~High~~high and ~~Medium Impact~~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 categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Assets, ~~5%~~five or fewer ~~of High~~high and ~~Medium Impact~~medium impact BES Cyber Assets have not been identified or categorized or have been incorrectly categorized at a lower	1.1; Or For Responsible Entities with more than a total of 100 ~~High~~high and ~~Medium Impact~~medium impact BES Cyber Assets, more than ~~5%~~five percent but less than or equal to 10~~%~~ percent 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~~high and ~~Medium Impact~~medium impact and BES Cyber Assets, more than ~~5~~five but less than or equal to 10 identified BES Cyber Assets have not been	1.1; For Responsible Entities with more than a total of 100 ~~High~~high or ~~Medium Impact~~medium impact BES Cyber Assets, more than 10~~%~~ percent but less than or equal to 15~~%~~ percent 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~~high or ~~Medium Impact~~medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been	with more than a total of 100 ~~High~~high and ~~Medium Impact~~medium impact BES Cyber ~~Assets~~Systems, more than 15~~%~~ percent of identified BES Cyber ~~Assets~~Systems 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~~high and ~~Medium Impact~~medium impact BES Cyber ~~Assets~~Systems, more than 15 identified BES Cyber ~~Assets~~Systems have not been categorized or have been incorrectly categorized at a lower category;

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			category; ~~Or~~ ~~For Responsible Entities with a total of 100 or fewer High and Medium Impact BES Cyber Assets, 5 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~~high and ~~Medium Impact~~medium impact BES Cyber Assets in accordance with ~~part~~Requirement R1, Part 1.~~1~~4 for more than ~~30~~60, but less than or equal to ~~40~~70 calendar	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 ~~part~~Requirement R1, Part 1.~~1~~4 for more than ~~40~~70, but less than or equal to ~~50~~80 calendar days following the completion of the change.	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 ~~part~~Requirement R1, Part 1.~~1~~4 for more than ~~50~~90, but less than or equal to ~~60~~100 calendar days following the completion of the change.	Or The Responsible Entity failed to update its documentation of BES Cyber ~~Assets~~Systems in accordance with ~~part~~Requirement R1, Part 1.~~1~~4 for more than ~~60~~100 calendar days following the completion of the change.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			days following the completion of the change.			
R 2	Operations Planning	Lower	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to ~~requirement~~Requirement R2 for more than 30, but less than or equal to 40 calendar days of the latest required date.	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to ~~requirement~~Requirement R2 for more than 40, but less than or equal to 50 calendar days of the latest required date.	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to ~~requirement~~Requirement R2 for more than 50, but less than or equal to 60 calendar days of the latest required date.	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to ~~requirement~~Requirement R2 for more than 60 calendar days of the latest required date.

~~C.~~D. Regional Variances

None.

~~D.~~E. Interpretations

None.

~~E.~~F. Associated Documents

None.

CIP-002-5 - Attachment ~~I~~1

~~Impact Categorization of BES Cyber Assets and BES Cyber Systems~~

Impact Rating Criteria

1. High Impact Rating (H)

Each BES Cyber ~~Asset or BES Cyber~~ System ~~that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services~~ used by and located at:

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 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 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 ~~or Transmission Owner~~, that includes control of one or more of the assets ~~identified in~~ that meet criteria 2.2, 2.4, 2.5, 2.~~6, 2.~~7, 2.8, 2.9, or 2.10~~, 2.11 or 2.12 below~~.

1.4 Each Control Center ~~or~~, backup Control Center, and associated data centers used to perform the functional obligations of the Generation Operator that includes control 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 ~~identified in~~that meet criteria 2.~~1, 2.~~3, 2.~~4, or~~6, and 2.~~12, below~~9.

2. Medium Impact Rating (M)

Each BES Cyber ~~Asset or BES Cyber~~ System, not included in Section 1, above, ~~that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for~~associated with the following:

2.1. ~~**2.1. Generation**~~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. ~~**2.2.** An~~Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate ~~net~~ 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. ~~**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 ~~BES~~an Adverse Reliability ~~Impacts~~Impact in the ~~long-term~~ planning horizon~~.~~ of more than one year.

~~**2.4.** Each Blackstart Resource identified in its Transmission Operator's restoration plan.~~

~~**2.5.** The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource~~

- ~~Up to and including the first interconnection point of the generation unit(s) to be started, or~~
- ~~up to the point on the Cranking Path where two or more path options exist and including any single failure points in the Cranking Path to and including the first interconnection point of the generation unit(s) to be started, or~~
- ~~up to and including the point on the Cranking Path where two or more path options exist to two or more independent generation unit(s) to be started as identified in its Transmission Operator's restoration plan.~~

2.4. ~~**2.6.**~~ Transmission Facilities operated at 500 kV or higher.

2.5. ~~**2.7.**~~ Transmission Facilities ~~operating at 200 kV or higher, but at less than 500 kV,~~ at a single station or substation that ~~is~~ are operating between 200 kV and 499 kV, are connected to three or more ~~transmission~~ other Transmission stations or substations ~~and where the "total weighted aggregate value" of all~~, and which possess "aggregate weighted values" exceeding 3000. The "aggregate weighted value" for a Transmission Facility is determined by summing the "weight value per line" shown in the table below for each incoming or outgoing BES Transmission ~~Lines at a single~~Line that is connected to another Transmission station or substation ~~operated at 200 KV or higher connected to other transmission stations or substations, including incoming and outgoing lines, exceeds a value of 3,000. The following "weight value per line" operated at the associated voltage value of a line will be used for the determination of the total weighted aggregate value~~.

Voltage Value of a Line	Weight Value per Line
100kV to 199 kV	0 (not applicable)
200 kV to 299 kV	700

300 kV to 499 kV	1300

~~2.8.~~

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 ~~Authority~~Coordinator or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

~~In the WECC Region, Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of SOLs and their contingencies for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System".~~

~~**2.9.** Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs), and their associated contingencies.~~

~~In the WECC Region, Flexible AC Transmission Systems (FACTS), at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of SOLs and their contingencies for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System."~~

2.7. ~~**2.10.**~~ Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. ~~**2.11.**~~ Transmission 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 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching ~~system~~Systems 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.

~~In the WECC Region, each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed,~~

~~degraded, misused or otherwise rendered unavailable, would cause one or more System Operating Limits (SOLs) violations for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System" and each RAS listed in the most current table titled " Major WECC Remedial Action Schemes (RAS)."~~

2.10. ~~**2.12.** Each system or Facility that performs automatic load shedding~~Each 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 (UVLS) or Under Frequency Load Shedding (UFLS~~)~~), as required by its regional load shedding program.

2.11. ~~**2.13.**~~ Control Centers and associated data centers not included in High Impact Rating (H), above, that: (1) perform ~~(1)~~ the functional obligations of ~~Transmission Operators~~Balancing Authority or Transmission ~~Owners;~~Operator, or (2) ~~generation~~ control ~~centers that control~~an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.

3. Low Impact Rating (L)

~~All other~~Each BES Cyber ~~Assets and~~ System associated with:

3.1. BES ~~Cyber Systems~~ 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 and medium impact shall default to the category of low impact and do not require discrete identification.

Guidelines and Technical Basis

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 ~~one or more~~the reliable operation of the BES ~~**Reliability Operating Services**.~~" ~~The new term BES Reliability Operating Service is a defined NERC Glossary term that in turn includes a number of defined named BES Reliability Operating Services. These named, defined services include:~~."

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 performs which reliability ~~operations~~operating service, ~~which determines what each entity needs~~as a process to ~~address with their CIP program.~~identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable ~~Reliability Operations Services~~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~~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 ~~should~~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, generators (TO, TOP, GO, GOP)
  - Zone protection for breaker failure (TO, TOP)
  - Breaker protection (TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays & breakers, possibly software (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 ~~Flowgates~~Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES ~~elements~~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)
- Coordination

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~~, but are not limited to~~:

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

Inter-Entity Coordination~~ and Communication~~

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~~, but are not limited to~~:

- 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~~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:

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~~Systems are assumed to be vulnerable) and a probability of threat of 1 (100~~%).~~ percent). The criteria in ~~attachment~~Attachment 1 provide a measure of the impact that the Facilities, Systems and equipment that these BES Cyber Systems support, on the ~~reliability and operability~~reliable operation of the BES.

Responsible Entities are required to identify and categorize those ~~systems~~ BES Cyber Systems that have high and medium impact. ~~Other BES~~ BES Cyber Systems for Facilities, Systems and ~~BES Cyber Assets are deemed~~equipment not specified in Parts 1.1 – 1.4 and Parts 2.1 – 2.11 default to ~~be~~ 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 ~~asset~~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 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 ~~support~~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 ~~support~~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 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.
- ~~A~~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), ~~Transmission Owner (TO)~~ or Generation Operator (GOP), as defined in the NERC Functional Model~~.~~, and as scoped by the qualification in Attachment 1, Parts 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above~~-~~named 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 ~~must~~would be subject to categorization as ~~High Impact.~~high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities.

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

Medium Impact Rating (M)

Generation

The criteria in Attachment ~~1, Medium Impact~~1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are parts 2.1, 2.3, 2.~~4~~6, 2.~~5, 2.11~~9, and 2.~~13~~11.

- Part 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 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~~Part 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 are categorized as ~~Medium Impact.~~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~~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~~System studies that a unit must run in order to preserve the reliability of the BES, such as due to a ~~category~~Category C3 contingency as defined in TPL-003, or a ~~category~~Category D contingency as defined in TPL-004, then BES Cyber Systems for that unit ~~must be~~are categorized as ~~Medium Impact~~medium impact.

  ~~In part 2.4, BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan are categorized as Medium 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.~~

- Part 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.

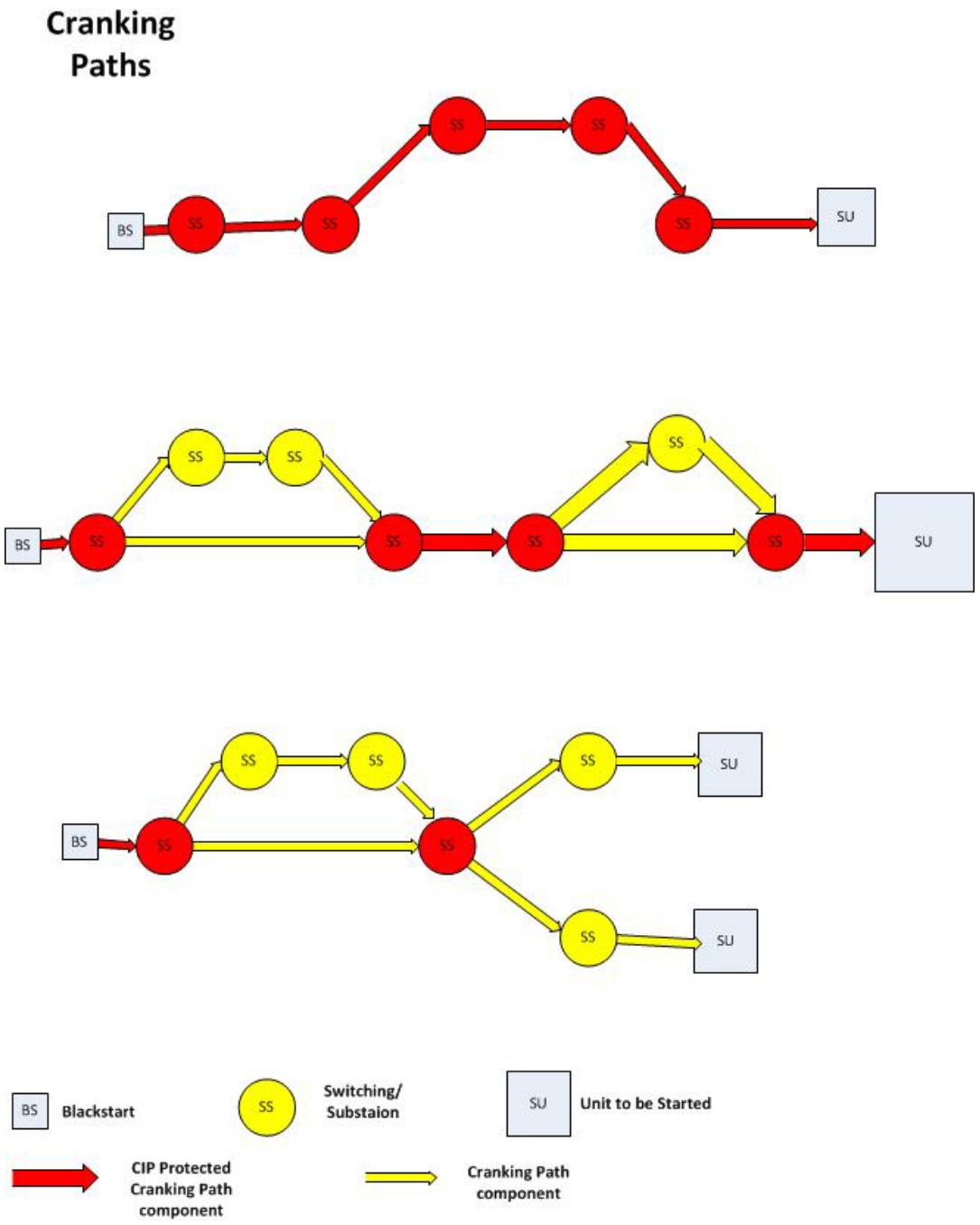
- ~~This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.~~ ~~While the definition of Blackstart Resource includes the fact that it is in a Transmission Operator's Restoration Plan, the drafting team included the term in the criterion for clarity.~~

  ~~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."~~

- ~~Part 2.5 categorizes BES Cyber Systems for Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, with the qualifications stated in the requirement part. This criterion 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. The drafting team further qualified the Facilities to be designated as subject to BES Cyber System categorization as only those in the Cranking Path up to the point where two or more paths exist to the units to be started and subject to the qualifications in the requirement part.~~

  ~~Distribution Providers should note that they may have BES Cyber Systems that must be categorized as Medium Impact if they have facilities listed in the Transmission Operator's Restoration Plan.~~

  ~~The following illustrates the parts of the Cranking Path that are subject to CIP Cranking Path criterion.~~



- Part 2.~~11~~9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as ~~Medium Impact.~~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 Operators which own BES Cyber Systems for such ~~systems~~Systems and schemes ~~must~~ designate them as ~~Medium Impact~~medium impact.

- Part 2.~~13~~11 categorizes as ~~Medium Impact~~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 Operator for an aggregate generation of 300 MW or higher~~.~~, and which have not already 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~~low impact.

Transmission

Parts 2.~~1, 2.~~, 2~~, .~~.4-2.~~5 2.13~~11 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~~System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). ~~For the WECC region where IROLs are not defined, alternative criteria are defined.~~

- ~~Part 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. In the case of BES Cyber Systems and BES Cyber Assets owned by Transmission Owners and Operators, this part identifies as Medium Impact those BES Cyber Systems for Transmission Facilities that provide the generation interconnection for Generation of 1500 MW or more to the Transmission system. The intent is to ensure the availability of Facilities necessary to support those generation facilities.~~

- Part 2.2 includes BES Cyber Systems for those Facilities in Transmission ~~systems~~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.

- ~~In Part 2.5, the intent is to ensure that BES Cyber Systems for the Cranking Paths and other BES Transmission Facilities required to support the Transmission Operator's restoration plan required by EOP-005-2 receive consideration for protection from cyber threats. Transmission Owners and Operators own and operate a large number of these Facilities. EOP-005-2 specifies Facilities that comprise the "Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started".~~

  ~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in 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."~~

- ~~Part 2.6~~Part 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~~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 1.1) 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~~medium impact BES Cyber System because it doesn't significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Part 2.~~7~~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

  ~~Parts 2.8 and 2.9~~In the case of autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location. 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 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 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.

~~Alternate thresholds are used for WECC, where IROLs are not used.~~

- Part 2.~~10~~7 is sourced from the NUC-001 NERC standard 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 2.~~11~~8 designates as ~~Medium Impact~~medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Parts 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).

- Part 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching ~~systems~~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.

~~For the WECC region, alternative thresholds are defined because IROLs are not defined for the region.~~

- Part 2.~~12~~10 designates as ~~Medium Impact~~medium impact those BES Cyber Systems for ~~systems~~Systems or ~~Facilities~~Elements that ~~are capable of performing~~perform automatic ~~load~~Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of ~~criterion~~Part 2.~~13~~12, and chose the term "Each" to represent that the criterion applied to a discrete ~~system~~System or Facility. In the drafting of this criterion, the drafting team sought to include only those ~~systems~~Systems that did not require human operator initiation, and targeted in particular those Under Frequency Load Shedding (UFLS) facilities and ~~systems~~Systems and Under Voltage Load

Shedding (UVLS) ~~facilities~~Systems and ~~systems~~Elements that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. These include automated Under Frequency Load Shedding ~~systems~~Systems or Under Voltage Load Shedding Systems that are capable of 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.~~ medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW rating 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~~, 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.

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.~~13~~11 categorizes as ~~Medium Impact~~ medium impact those ~~cyber systems~~ BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of Balancing Authorities or Transmission Operators ~~and Owners Control Centers~~ not already categorized as ~~High Impact~~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.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that these 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.

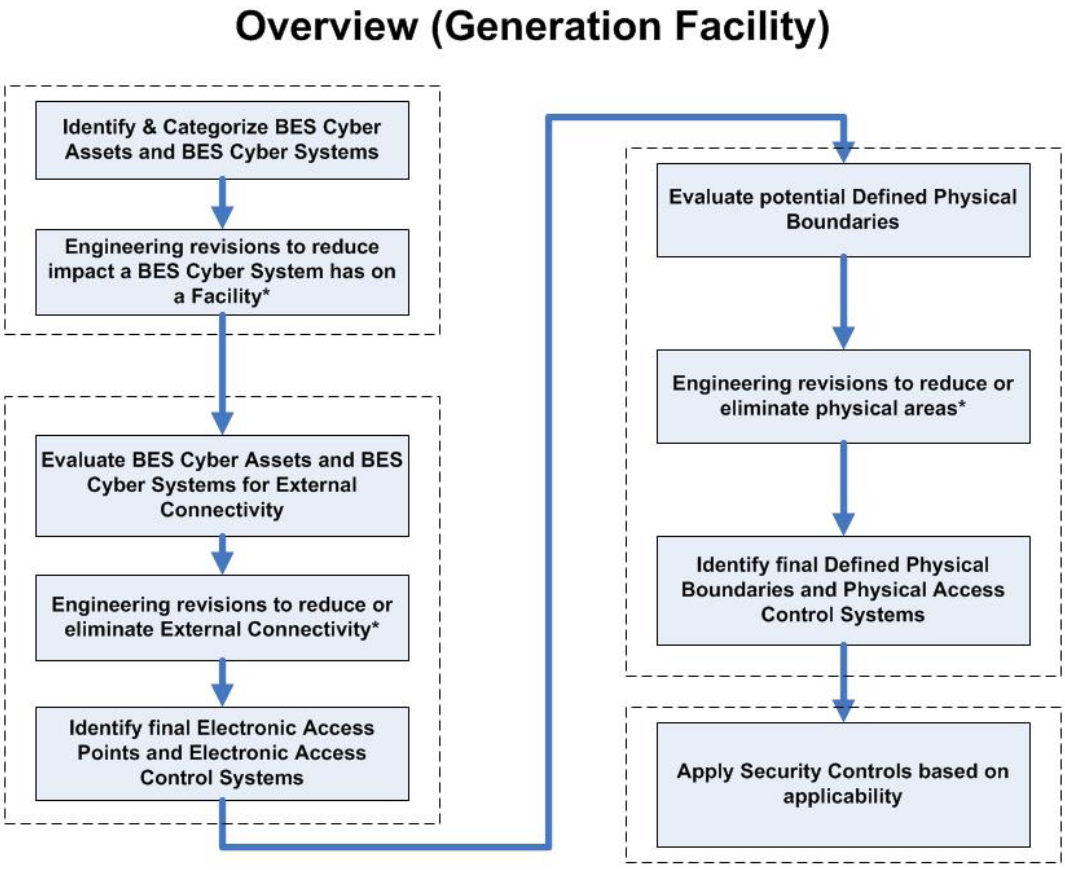
Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific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