

This appendix establishes modifications to the FERC approved NERC standard CIP-002-5.1 for its specific application in New Brunswick. This appendix must be read with CIP-002-5.1 to determine a full understanding of the requirements of the standard for New Brunswick. Where the standard and appendix differ, the appendix shall prevail.

The term “BES Cyber Asset” as used in this Appendix or CIP-002-5.1 means “BPS Cyber Asset” as defined in section G.

The term “BES Cyber System” as used in this Appendix or CIP-002-5.1 means “BPS Cyber System” as defined in section G.

A. Introduction

- 1. Title:** **Cyber Security – BES Cyber System Categorization**
- 2. Number:** CIP-002-5.1
- 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 bulk power system. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the bulk power system.
- 4. Applicability:**
 - 4.1. Functional Entities:** No New Brunswick modifications
 - 4.1.1.** No New Brunswick modifications
 - 4.1.2.** **Distribution Provider that owns** one or more of the following Facilities, systems, and equipment for the protection or restoration of the bulk power system:
 - 4.1.2.1.** No New Brunswick modifications
 - 4.1.2.1.1.** is part of a Load shedding program that is subject to one or

more requirements in a New Brunswick Energy and Utilities Board approved reliability standard or Regional Reliability Standard; and

4.1.2.1.2. No New Brunswick modifications

4.1.2.2. 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 New Brunswick Energy and Utilities Board approved reliability standard or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a New Brunswick Energy and Utilities Board approved reliability standard or Regional Reliability Standard.

4.1.2.4. No New Brunswick modifications

4.1.3. No New Brunswick modifications

4.1.4. No New Brunswick modifications

4.1.5. No New Brunswick modifications

4.1.6. No New Brunswick modifications

4.1.7. No New Brunswick modifications

4.1.8. No New Brunswick modifications

4.2. Facilities: No New Brunswick modifications

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 bulk power system:

4.2.1.1. No New Brunswick modifications

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a New

Brunswick Energy and Utilities
Board approved reliability
standard or Regional Reliability
Standard; and

4.2.1.1.2. No New Brunswick
modifications

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 New Brunswick Energy and
Utilities Board approved reliability
standard 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 New
Brunswick Energy and Utilities Board
approved reliability standard or Regional
Reliability Standard.

4.2.1.4. No New Brunswick modifications

**4.2.2. Responsible Entities listed in 4.1 other
than Distribution Providers:** All bulk power
system Facilities.

4.2.3. Exemptions: No New Brunswick modifications

4.2.3.1. No New Brunswick modifications

4.2.3.2. No New Brunswick modifications

4.2.3.3. No New Brunswick modifications

4.2.3.4. No New Brunswick modifications

5. Effective Dates:

1. No New Brunswick modifications

2. No New Brunswick modifications

6. 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, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the bulk power 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 power 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

No New Brunswick modifications

Reliable Operation of the Bulk Power System

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the bulk power system. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any bulk power system 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 bulk power system. 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 bulk power system. 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 bulk power system 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 for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and 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

bulk power system is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

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

No New Brunswick modifications

Electronic Access Control or Monitoring Systems (“EACMS”) –No New Brunswick modifications

Physical Access Control Systems (“PACS”) – No New Brunswick modifications

Protected Cyber Assets (“PCA”) – No New Brunswick modifications

B. Requirements and Measures

R1. No New Brunswick modifications;

- i.** No New Brunswick modifications
- ii.** No New Brunswick modifications
- iii.** No New Brunswick modifications
- iv.** Special Protection Systems that support the reliable operation of the bulk power system; and
- v.** No New Brunswick modifications

1.1. No New Brunswick modifications

1.2. No New Brunswick modifications

1.3. No New Brunswick modifications

M1. No New Brunswick modifications

R2. No New Brunswick modifications

2.1 No New Brunswick modifications

2.2 No New Brunswick modifications

M2. No New Brunswick modifications

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The New Brunswick Energy and Utilities Board shall serve as the Compliance Enforcement Authority (“CEA”).

1.2. Evidence Retention:

No New Brunswick modifications

1.3. Compliance Monitoring and Assessment Processes:

- No New Brunswick modifications

1.4. Additional Compliance Information

- No New Brunswick modifications

NB Appendix
CIP-002-5.1-NB-0 - Cyber Security – BES Cyber System Categorization

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	High	For Responsible Entities with more than a total of 40 bulk power system assets in Requirement R1, five percent or fewer bulk power system assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer bulk power system assets, 2 or fewer bulk power system assets in Requirement R1, have not been considered according to Requirement R1; OR No New Brunswick	For Responsible Entities with more than a total of 40 bulk power system assets in Requirement R1, more than five percent but less than or equal to 10 percent of bulk power system assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer bulk power system assets, more than two, but fewer than or equal to four bulk power system assets in Requirement R1, have not been considered according to	For Responsible Entities with more than a total of 40 bulk power system assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of bulk power system assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer bulk power system assets, more than four, but fewer than or equal to six bulk power system assets in Requirement R1, have not been considered according to	For Responsible Entities with more than a total of 40 bulk power system assets in Requirement R1, more than 15 percent of bulk power system assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer bulk power system assets, more than six bulk power system assets in Requirement R1, have not been considered according to Requirement R1; OR No New Brunswick

NB Appendix
CIP-002-5.1-NB-0 - Cyber Security – BES Cyber System Categorization

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			modifications OR No New Brunswick modifications OR No New Brunswick modifications OR No New Brunswick modifications	Requirement R1; OR No New Brunswick modifications OR No New Brunswick modifications OR No New Brunswick modifications OR No New Brunswick modifications	Requirement R1; OR No New Brunswick modifications OR No New Brunswick modifications OR No New Brunswick modifications OR No New Brunswick modifications	modifications OR No New Brunswick modifications OR No New Brunswick modifications OR No New Brunswick modifications
R2	Operations Planning	Lower	No New Brunswick modifications			

D. Regional Variances

No New Brunswick modifications

E. Interpretations

No New Brunswick modifications

F. Associated Documents

No New Brunswick modifications

G. New Brunswick Definitions

BPS Cyber Asset: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the bulk power system. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BPS Cyber Asset is included in one or more BPS Cyber Systems. (A Cyber Asset is not a BPS Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BPS Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

BPS Cyber System: One or more BPS Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

CIP-002-5.1 - Attachment 1

Impact Rating Criteria

No New Brunswick modifications

1. High Impact Rating (H)

No New Brunswick modifications

1.1. No New Brunswick modifications

1.2. No New Brunswick modifications

1.3. No New Brunswick modifications

1.4. No New Brunswick modifications

2. Medium Impact Rating (M)

No New Brunswick modifications

2.1. No New Brunswick modifications

2.2. Each bulk power system 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. No New Brunswick modifications

2.4. No New Brunswick modifications

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing bulk power system 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
No New Brunswick modifications	

- 2.6. No New Brunswick modifications
- 2.7. No New Brunswick modifications
- 2.8. No New Brunswick modifications
- 2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates bulk power system 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 or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a New Brunswick Energy and Utilities Board approved reliability standard or regional reliability standard.
- 2.11. No New Brunswick modifications
- 2.12. No New Brunswick modifications
- 2.13. No New Brunswick modifications
- 3. **Low Impact Rating (L)**
 - No New Brunswick modifications
 - 3.1. No New Brunswick modifications
 - 3.2. No New Brunswick modifications

- 3.3.** No New Brunswick modifications
- 3.4.** No New Brunswick modifications
- 3.5.** Special Protection Systems that support the reliable operation of the bulk power system.
- 3.6.** No New Brunswick modifications

Guidelines and Technical Basis

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

No New Brunswick modifications

Section “4.1. Functional Entities” is a list of 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 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.

No New Brunswick modifications

No New Brunswick modifications

CIP-002-5.1

No New Brunswick modifications

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of bulk power system 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-002-5.1. The concept includes a number of named bulk power system reliability operating services. These named services include:

- Dynamic Response to bulk power system conditions

- Balancing Load and Generation

- Controlling Frequency (Real Power)

- Controlling Voltage (Reactive Power)

- Managing Constraints

- Monitoring & Control

- Restoration of bulk power system

- Situational Awareness

- Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the bulk power system is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the

NB Appendix
Guidelines and Technical Basis

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 bulk power system 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	GOP	GO
Dynamic Response	No New Brunswick modifications						
Balancing Load & Generation							
Controlling Frequency							
Controlling Voltage							
Managing Constraints							
Monitoring and Control							
Restoration							
Situation Awareness							
Inter-Entity coordination							

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by bulk power system Elements or subsystems which are automatically triggered to initiate a response to a bulk power system 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 bulk power system are:

- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications

Balancing Load and Generation

No New Brunswick modifications

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 bulk power system. Aspects of the Controlling Frequency function include, but are not limited to:

- No New Brunswick modifications
- No New Brunswick modifications

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 bulk power system. Aspects of the Controlling Voltage function include, but are not limited to:

- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications

Managing Constraints

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

Managing Constraints include, but are not limited to:

- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of bulk power system Elements. An example aspect of the Control and Operation function is:

- No New Brunswick modifications

Restoration of Bulk Power System

The Restoration of bulk power system 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 bulk power system function include, but are not limited to:

- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications

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 bulk power system and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications

- No New Brunswick modifications

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 bulk power system. Aspects of the Inter-Entity Coordination and Communication function include:

- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications

Applicability to Distribution Providers

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 New Brunswick Energy and Utilities Board approved reliability standard EOP- 005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the bulk power system. 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 of the bulk power system assets supported by these BES Cyber Systems.

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

Attachment 1

Overall Application

No New Brunswick modifications

- When the drafting team uses the term “Facilities”, 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 power 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 bulk power system. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports bulk power system 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 bulk power system 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 bulk power system, 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-002-5.1, these groups of Facilities, systems, and equipment are sometimes designated as bulk power system assets. For example, an identified bulk power system 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.
- No New Brunswick modifications
- No New Brunswick modifications

High Impact Rating (H)

No New Brunswick modifications

Medium Impact Rating (M)

Generation

No New Brunswick modifications

- No New Brunswick modifications
 - In 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 or Transmission Planner as necessary to avoid bulk power system Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a “long term” reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. 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.
- If it is determined through System studies that a unit must run in order to preserve the reliability of the bulk power system,

such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

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 Regional Entity/RR0. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications

Transmission

No New Brunswick modifications

- Criteria 2.2, 2.4 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 (IROs). 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 bulk power system. 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.
- 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 bulk power system, Facilities

in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

No New Brunswick modifications

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

- No New Brunswick modifications
- No New Brunswick modifications

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 bulk power system, 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

No New Brunswick modifications

- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications
- 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 bulk power

system 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.

- No New Brunswick modifications

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 power 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.

No New Brunswick modifications

No New Brunswick modifications

- No New Brunswick modifications
- No New Brunswick modifications

Low Impact Rating (L)

No New Brunswick modifications

Restoration Facilities

- No New Brunswick modifications
- No New Brunswick modifications
- No New Brunswick modifications

Weighing the risks to overall bulk power system reliability, the drafting team determined that this re- categorization represents the option that would be the least detrimental to restoration function and, thus, overall bulk power system 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.

No New Brunswick modifications

Regarding concerns of communication to bulk power system 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.”

- No New Brunswick modifications

Use Case: CIP Process Flow

No New Brunswick modifications

Rationale:

No New Brunswick modifications

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the bulk power 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 bulk power system. 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.

Rationale for 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 bulk power system. The CIP Senior Manager’s approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

**NB Appendix
Guidelines and Technical Basis**

Version History (maintained by NBEUB)

Version	NBEUB Approval Date	NB Appendix Effective Date	Change Tracking	Comments
0	06/25/14	07/01/16	1. Bulk Electric System(BES)replaced with "bulk power system" throughout 2. Revised Section A, Attachment 1 and the Guidelines to replace "NERC" with "New Brunswick Energy and Utilities Board approved reliability standard" 3. Revised Section C to clarify the NBEUB as the entity having the compliance enforcement authority for NB 4. Revised the Guidelines to remove reference to NERC for functional entities	Approved Under NBEUB Matter 246