

NB Appendix
CIP-007-5-NB-1 - Cyber Security – System Security Management

This appendix establishes modifications to the FERC approved NERC standard CIP-007-5 for its specific application in New Brunswick. This appendix must be read with CIP-007-5 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-007-5 means “BPS Cyber Asset” as defined in section G.

The term “BES Cyber System” as used in this Appendix or CIP-007-5 means “BPS Cyber System” as defined in section G.

A. Introduction

- 1. Title:** **Cyber Security – System Security Management**
- 2. Number:** CIP-007-5
- 3. Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise 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

4.2.3.5 No New Brunswick modifications

5. Effective Dates:

CIP-007-5 shall become effective at the same time that CIP-007-6 becomes effective in New Brunswick.

6. Background:

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

No New Brunswick modifications

No New Brunswick modifications

No New Brunswick modifications

Many references in the Applicability section 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.

“Applicable Systems” Columns in Tables:

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
- No New Brunswick modifications

B. Requirements and Measures

R1. No New Brunswick modifications

M1. No New Brunswick modifications

CIP-007-5 Table R1- Ports and Services			
Part	Applicable Systems	Requirements	Measures
1.1	No New Brunswick modifications		
1.2			

NB Appendix
CIP-007-5-NB-1 - Cyber Security – System Security Management

R2. No New Brunswick modifications

M2. No New Brunswick modifications

CIP-007-5 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.1	No New Brunswick modifications.		
2.2			
2.3			
2.4			

R3. No New Brunswick modifications

M3. No New Brunswick modifications

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	Applicable Systems	Requirements	Measures
3.1	No New Brunswick modifications		
3.2			
3.3			

NB Appendix
CIP-007-5-NB-1 - Cyber Security – System Security Management

R4. No New Brunswick modifications

M4. No New Brunswick modifications

CIP-007-5 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
4.1			
4.2			
4.3			
4.4			

No New Brunswick modifications

NB Appendix
CIP-007-5-NB-1 - Cyber Security – System Security Management

R5. No New Brunswick modifications

M5. No New Brunswick modifications

CIP-007-5 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.1		No New Brunswick modifications	
5.2			
5.3			
5.4			
5.5			
5.6			
5.7			

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

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.

1. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	No New Brunswick modifications					
R2						
R3						
R4						
R5						

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. Furthermore,

No New Brunswick modifications

Requirement R1:

No New Brunswick modifications

Requirement R2:

No New Brunswick modifications

2.1. No New Brunswick modifications

2.2. No New Brunswick modifications

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as “at next scheduled outage of at least two days duration.” “Mitigation plans” in the standard refers to internal

documents and are not to be confused with plans that are submitted to the New Brunswick Energy and Utilities Board in response to violations.

2.4. No New Brunswick modifications

Requirement R3:

3.1. No New Brunswick modifications

3.2. No New Brunswick modifications

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the bulk power system. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

No New Brunswick modifications

Requirement R5:

No New Brunswick modifications

5.1 No New Brunswick modifications

5.2 No New Brunswick modifications

5.4. No New Brunswick modifications

5.5. No New Brunswick modifications

5.6 No New Brunswick modifications

5.7 No New Brunswick modifications

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a bulk power system reliability task. In such cases, entities should configure authentication failure alerting.

**NB Appendix
Guidelines and Technical Basis**

Rationale:

No New Brunswick modifications

Rationale for R1:

No New Brunswick modifications

Rationale for R2:

No New Brunswick modifications

The remediation plan can be updated as necessary to maintain the reliability of the bulk power system, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: No New Brunswick modifications

Reference to prior version: No New Brunswick modifications

Change Rationale No New Brunswick modifications

Reference to prior version: No New Brunswick modifications

Change Rationale: No New Brunswick modifications

Reference to prior version: No New Brunswick modifications

Change Rationale: No New Brunswick modifications

Reference to prior version: No New Brunswick modifications

Change Rationale: No New Brunswick modifications

Rationale for R3:

No New Brunswick modifications

Rationale for R4:

No New Brunswick modifications

Rationale for R5:

No New Brunswick modifications

Version History

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	Approved Under NBEUB Matter 246

**NB Appendix
Guidelines and Technical Basis**

			2. Revised Section A 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 and to replace Regional Entity with NBEUB	
1	06/29/16	TBD	1. Revised Effective Dates in Section A to replace the contents with "CIP-007-5 shall become effective at the same time that CIP-007-6 becomes	Approved Under NBEUB Matter 322 CIP-007-5 will be retired the day prior to the effective date of CIP-007-6 as

NB Appendix
Guidelines and Technical Basis

			effective in New Brunswick	determined by implementation plan under Matter 325.
--	--	--	----------------------------	---