This appendix establishes modifications to the FERC approved NERC standard CIP-007-6 for its specific application in New Brunswick. This appendix must be read with CIP-007-6 to determine a full understanding of the requirements of the standard for New Brunswick. Where the standard and appendix differ, the appendix shall prevail.

For the purpose of this standard the term "Bulk Electric System" and its acronym, "BES" shall mean the "bulk power system" (BPS) as defined in the New Brunswick *Reliability Standards Regulation - Electricity Act*.

The term “BES Cyber Asset” as used in this Appendix or CIP-007-6 means “BPS Cyber Asset” as defined in section G.

The term “BES Cyber System” as used in this Appendix or CIP-007-6 means “BPS Cyber System” as defined in section G.

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-6

3. **Purpose:** No New Brunswick modifications

4. **Applicability:**

   4.1. **Functional Entities:** No New Brunswick modifications

      4.1.1 **Balancing Authority**

      4.1.2 **Distribution Provider** No New Brunswick modifications

         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 (SPS) or Remedial Action Scheme (RAS) where the SPS or RAS 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 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** No New Brunswick modifications

4.2.1 **Distribution Provider**: No New Brunswick modifications

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 SPS or RAS where the SPS or RAS 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**: No New Brunswick modifications

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:

No New Brunswick modifications

6. Background:

No New Brunswick modifications

B. Requirements and Measures

R1. No New Brunswick modifications

M1. No New Brunswick modifications

CIP-007-6 Table R1– Ports and Services			
Part	Applicable Systems	Requirements	Measures
1.1	No New Brunswick modifications	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed. Where not technically feasible a Responsible Entity shall request an exception from strict compliance and comply with the New Brunswick Energy and Utilities Board procedure "Technical Feasibility Exceptions for Critical Infrastructure Protection Reliability Standards".	No New Brunswick modifications
1.2	No New Brunswick modifications		

R2. No New Brunswick modifications

M2. No New Brunswick modifications

CIP-007-6 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-007-6 Table R3 – Malicious Code Prevention			
Part	Applicable Systems	Requirements	Measures
3.1	No New Brunswick modifications		
3.2			
3.3			

R4. No New Brunswick modifications

M4. No New Brunswick modifications

CIP-007-6 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
4.1	No New Brunswick modifications		
4.2			
4.3	No New Brunswick modifications	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances. Where not technically feasible a Responsible Entity shall request an exception from strict compliance and comply with the New Brunswick Energy and Utilities Board procedure “Technical Feasibility Exceptions for Critical Infrastructure Protection Reliability Standards”.	No New Brunswick modifications

CIP-007-6 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
4.4	No New Brunswick modifications		

R5. No New Brunswick modifications

M5. No New Brunswick modifications

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	No New Brunswick modifications	Have a method(s) to enforce authentication of interactive user access, where technically feasible. Where not technically feasible a Responsible Entity shall request an exception from strict compliance and comply with the New Brunswick Energy and Utilities Board procedure “Technical Feasibility Exceptions for Critical Infrastructure Protection Reliability Standards”.	No New Brunswick modifications
5.2 5.3 5.4 5.5	No New Brunswick modifications		
5.6	No New Brunswick modifications	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months. Where not technically feasible a Responsible Entity shall request an exception from strict compliance and comply with the New Brunswick Energy and Utilities Board procedure “Technical Feasibility Exceptions for Critical Infrastructure Protection Reliability Standards”.	No New Brunswick modifications
5.7	No New Brunswick modifications	Where technically feasible, either:	No New Brunswick modifications

		• Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts. Where not technically feasible a Responsible Entity shall request an exception from strict compliance and comply with the New Brunswick Energy and Utilities Board procedure “Technical Feasibility Exceptions for Critical Infrastructure Protection Reliability Standards”.	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means the New Brunswick Energy and Utilities Board.

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

2. Table of Compliance Elements (maintained by NBEUB)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	No New Brunswick modifications					
R2						
R3						
R4						
R5						

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 nonoperation, 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.

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.

Version History (maintained by NBEUB)

Version	NBEUB Approval Date	NB Appendix Effective Date	Change Tracking	Comments
0	09/07/16	01/01/17	1. Bulk Electric System(BES)replaced with “bulk power system” throughout 2. Revised Section A to replace “NERC” with “New Brunswick Energy and	Approved Under NBEUB Matter 325

			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 5. Add a requirement to comply with the NBEUB Board approved Technical Feasibility Exception (TFE) process in R1, R4 and R5 where strict adherence to the requirement is not technically feasible.	
0	09/07/16	01/01/17	1. On 09/30/16 corrected the effective date for the NB Appendix.	Effective Dates: R1, R1.1, R2, R3, R4, R5 01/01/17 R1.2 09/01/17
0	09/07/16	01/01/17	1. On 04/11/17 corrected the effective date for the NB Appendix.	Effective Dates: R1, R1.1, R2, R3, R4, R5

				01/01/17 R1.2 10/01/17

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

Requirement R1:

No New Brunswick modifications

Requirement R2:

No New Brunswick modifications

Requirement R3:

No New Brunswick modifications

Requirement R4:

No New Brunswick modifications

Requirement R5:

No New Brunswick modifications

Rationale:

No New Brunswick modifications