

This appendix establishes modifications to the FERC approved NERC standard CIP-010-4 for its specific application in New Brunswick. This appendix must be read with CIP-010-4 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-010-4 means “BPS Cyber Asset” as defined in section F.

The term “BES Cyber System” as used in this Appendix or CIP-010-4 means “BPS Cyber System” as defined in section F.

The term “BES Cyber System Information” as used in this Appendix or CIP-010-4 means “BPS Cyber System Information” as defined in section F.

A. Introduction

1. **Title:** Cyber Security – Configuration Change Management and Vulnerability Assessments
2. **Number:** CIP-010-4
3. **Purpose:** No New Brunswick modifications
4. **Applicability:**
 - 4.1. **Functional Entities:** No New Brunswick modifications
 - 4.1.1 **Balancing Authority** No New Brunswick modifications
 - 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

- Page 2 of 9

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 Date: 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-010-4 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.1		No New Brunswick modifications	
1.2			
1.3			
1.4			
1.5	No New Brunswick modifications	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. No New Brunswick modifications. 1.5.2. No New Brunswick modifications 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
1.6	No New Brunswick modifications		

NB Appendix
CIP-010-4-NB-0 – Cyber Security – Configuration Change Management and Vulnerability Assessments

R2. No New Brunswick modifications

M2. No New Brunswick modifications

CIP-010-4 Table R2 – Configuration Monitoring			
Part	Applicable Systems	Requirements	Measures
2.1	No New Brunswick modifications		

R3. No New Brunswick modifications

M3. No New Brunswick modifications

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.1	No New Brunswick modifications		
3.2	No New Brunswick modifications	Where technically feasible, at least once every 36 calendar months: 3.2.1 No New Brunswick modifications 3.2.2 No New Brunswick modifications. 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
3.3	No New Brunswick modifications		
3.4			

R4. No New Brunswick modifications

M4. No New Brunswick modifications

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

No New Brunswick modifications

1.2. Evidence Retention:

No New Brunswick modifications

1.3. Compliance Monitoring and Enforcement Program:

“Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard as set out in the New Brunswick Compliance Monitoring and Enforcement Program.

Violation Severity Levels

R #	Violation Severity Levels (CIP-010-4)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	No New Brunswick modifications			
R2.				
R3.				
R4.				

D. Regional Variances

No New Brunswick modifications

E. Associated Documents

No New Brunswick modifications

F. 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.
BPS Cyber Information:	Information about the BPS Cyber System that could be used to gain unauthorized access or pose a security threat to the BPS Cyber System. BPS Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BPS Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BPS Cyber System Information may include, but are not limited to, security procedures or security information about BPS Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BPS Cyber System.

NB Appendix
CIP-010-4-NB-0 – Cyber Security – Configuration Change Management and Vulnerability Assessments

Version History (maintained by NBEUB)

Version	NBEUB Approval Date	NB Appendix Effective Date	Change Tracking	Comments
0	07/26/21	04/01/23	1. Replace the term “Bulk Electric System” and its acronym “BES” with “bulk power system” throughout. 2. Replace “NERC” with “New Brunswick Energy and Utilities Board approved Reliability Standard” to recognize that registered entities in New Brunswick are required to comply with Board approved Reliability Standards. 3. Add a requirement to comply with the NBEUB Board approved Technical Feasibility Exception (TFE) process. 4. Replace “As defined in NERC Rules of Procedure” with “as set out in the New Brunswick Compliance Monitoring and Enforcement Program”. 5. Add New Brunswick definition for BPS Cyber Asset, BPS Cyber System and BPS Cyber System Information.	Approved by NBEUB, Matter 498

CIP-010-4 – Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

No New Brunswick modifications

CIP-010-4 – Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

No New Brunswick modifications