

NB Appendix
CIP-003-8-NB-0 - Cyber Security – Security Management Controls

This appendix establishes modifications to the FERC approved NERC standard CIP-003-8 for its specific application in New Brunswick. This appendix must be read with CIP-003-8 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-003-8 means "BPS Cyber Asset" as defined in section G.

The term "BES Cyber System" as used in this Appendix or CIP-003-8 means "BPS Cyber System" as defined in section G.

The term "Low Impact BES Cyber System Electronic Access Point" as used in this Appendix or CIP-003-8 means "Low-Impact BPS Cyber System Electronic Access Point" as defined in section G.

A. Introduction

- 1. Title:** Cyber Security – Security Management Controls
- 2. Number:** CIP-003-8
- 3. Purpose:** No New Brunswick modifications
- 4. Applicability:**
 - 4.1. Functional Entities:** No New Brunswick modifications
 - 4.1.1.** No New Brunswick modifications
 - 4.1.2.** 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
 - 4.1.2.1.3.**
 - 4.1.2.1.4.** No New Brunswick modifications

- 2

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

4.2.1.4. No New Brunswick modifications

4.2.2. No New Brunswick modifications

4.2.3. 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:

No New Brunswick modifications

6. Background:

No New Brunswick modifications

B. Requirements and Measures

R1. No New Brunswick modifications

1.1. No New Brunswick modifications

1.1.1. No New Brunswick modifications

1.1.2. No New Brunswick modifications

1.1.3. No New Brunswick modifications

1.1.4. No New Brunswick modifications

1.1.5. No New Brunswick modifications

1.1.6. No New Brunswick modifications

1.1.7. No New Brunswick modifications

1.1.8. No New Brunswick modifications

1.1.9. No New Brunswick modifications

1.2. No New Brunswick modifications

- 1.2.1.** No New Brunswick modifications
- 1.2.2.** No New Brunswick modifications
- 1.2.3.** No New Brunswick modifications
- 1.2.4.** No New Brunswick modifications
- 1.2.5.** No New Brunswick modifications
- 1.2.6.** No New Brunswick modifications

- M1.** No New Brunswick modifications
- R2.** No New Brunswick modifications
- M2.** No New Brunswick modifications
- R3.** No New Brunswick modifications
- M3.** No New Brunswick modifications
- R4.** No New Brunswick modifications
- M4.** No New Brunswick modifications

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

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-8)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	No New Brunswick modifications					
R2						
R3						
R4						

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.

Low Impact BPS Cyber System Electronic Access Point:

A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BPS Cyber Systems.

NB Appendix
CIP-003-8-NB-0 - Cyber Security – Security Management Controls

Version History (maintained by NBEUB)

Version	NBEUB Approval Date	NB Appendix Effective Date	Change Tracking	Comments
0	12/19/19	07/01/20	1. Bulk Electric System(BES)replaced with “bulk power system” throughout 2. Add New Brunswick specific definition of BPS Cyber Asset and BPS Cyber System in a new Section G of the NB Appendix. 3. Revised Section A to replace “NERC” with “New Brunswick Energy and Utilities Board approved reliability standard” 4. Revised Section C to clarify the NBEUB as the entity having the compliance enforcement authority for NB 5. Remove “NERC” from “NERC registered Entities” and from “NERC CIP Standards” in the Guidelines and Technical Basis section.	Approved by NBEUB under Matter 456

Attachment 1

**Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber
Systems**

No New Brunswick modifications

Attachment 2

**Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber
Systems**

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

Requirement R1:

No New Brunswick modifications

No New Brunswick modifications

No New Brunswick modifications

Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization’s internal culture of compliance and posture towards cyber security.

No New Brunswick modifications

1.1.1 No New Brunswick modifications

1.1.2 No New Brunswick modifications

1.1.3 No New Brunswick modifications

1.1.4 No New Brunswick modifications

1.1.5 No New Brunswick modifications

1.1.6 No New Brunswick modifications

1.1.7 No New Brunswick modifications

1.1.8 No New Brunswick modifications

1.1.9 No New Brunswick modifications

No New Brunswick modifications

1.2.1 No New Brunswick modifications

1.2.2 No New Brunswick modifications

1.2.3 No New Brunswick modifications

1.2.4 No New Brunswick modifications

1.2.5 No New Brunswick modifications

1.2.6 No New Brunswick modifications

No New Brunswick modifications

In this and all subsequent required approvals in the CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

No New Brunswick modifications

Requirement R2, Attachment 1

No New Brunswick modifications

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

No New Brunswick modifications

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

No New Brunswick modifications

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

No New Brunswick modifications

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

No New Brunswick modifications

**Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media
Malicious Code Risk Mitigation**

No New Brunswick modifications

Requirement R3:

No New Brunswick modifications

Requirement R4:

No New Brunswick modifications

Rationale:

No New Brunswick modifications

Rationale for Requirement R1:

No New Brunswick modifications

Rationale for Requirement R2:

No New Brunswick modifications

Rationale for Requirement R3:

No New Brunswick modifications

Rationale for Requirement R4:

No New Brunswick modifications