

This appendix establishes modifications to the FERC approved NERC standard CIP-004-5.1 for its specific application in New Brunswick. This appendix must be read with CIP-004-5.1 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-004-5.1 means “BPS Cyber Asset” as defined in section G.

The term “BES Cyber System” as used in this Appendix or CIP-004-5.1 means “BPS Cyber System” as defined in section G.

The term “BES Cyber System Information” as used in this Appendix or CIP-004-5.1 means “BPS Cyber System Information” as defined in section G.

A. Introduction

- 1. Title:** **Cyber Security – Personnel & Training**
- 2. Number:** CIP-004-5.1
- 3. Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the bulk power system from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.
- 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:

1. No New Brunswick modifications
2. No New Brunswick modifications

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

NB Appendix
CIP-004-5.1-NB-0 - Cyber Security – Personnel & Training

B. Requirements and Measures

R1. No New Brunswick modifications

M1. No New Brunswick modifications

CIP-004-5.1 Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	No New Brunswick modifications		

R2. No New Brunswick modifications

M2. No New Brunswick modifications

CIP-004-5.1 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.1	No New Brunswick modifications		
2.2			
2.3			

R3. No New Brunswick modifications

M3. No New Brunswick modifications

NB Appendix
CIP-004-5.1-NB-0 - Cyber Security – Personnel & Training

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.1			
3.2			
3.3			
3.4			
3.5			

R4. No New Brunswick modifications

M4. No New Brunswick modifications

NB Appendix
CIP-004-5.1-NB-0 - Cyber Security – Personnel & Training

CIP-004-5.1 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.1	No New Brunswick modifications		
4.2			
4.3			
4.4			

R5. No New Brunswick modifications

M5. No New Brunswick modifications

NB Appendix
CIP-004-5.1-NB-0 - Cyber Security – Personnel & Training

CIP-004-5.1 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.1			
5.2			
5.3			
5.4			
5.5			
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

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			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 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.

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.

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

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the bulk power system or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity’s process during the tenure of employment, which may or may not be the same as the initial verification action.

No New Brunswick modifications

Requirement R4:

No New Brunswick modifications

Requirement R5:

NB Appendix
Guidelines and Technical Basis

No New Brunswick modifications

Scenario	Possible Process
No New Brunswick modifications	

No New Brunswick modifications

No New Brunswick modifications

No New Brunswick modifications

No New Brunswick modifications

Requirement 5.5 specified that passwords for shared account are to be changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the bulk power system. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

No New Brunswick modifications

Rationale for R1:

No New Brunswick modifications

Rationale for R2:

No New Brunswick modifications

Rationale for R3:

No New Brunswick modifications

Rationale for R4:

No New Brunswick modifications

**NB Appendix
Guidelines and Technical Basis**

Rationale for R5:

No New Brunswick modifications

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 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	Approved Under NBEUB Matter 246

NB Appendix
Guidelines and Technical Basis

			4. Revised the Guidelines to remove reference to NERC for functional entities	