

NB Appendix
CIP-008-5-NB-0 - Cyber Security – Incident Reporting and Response Planning

This appendix establishes modifications to the FERC approved NERC standard CIP-008-5 for its specific application in New Brunswick. This appendix must be read with CIP-008-5 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-008-5 means “BPS Cyber Asset” as defined in section G.

The term “BES Cyber System” as used in this Appendix or CIP-008-5 means “BPS Cyber System” as defined in section G.

A. Introduction

- 1. Title:** Cyber Security – Incident Reporting and Response Planning
- 2. Number:** CIP-008-5
- 3. Purpose:** To mitigate the risk to the reliable operation of the bulk power system as the result of a Cyber Security Incident by specifying incident response requirements.
- 4. Applicability:**
 - 4.1. Functional Entities:** No New Brunswick modifications
 - 4.1.1 Balancing Authority**
 - 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

NB Appendix
CIP-008-5-NB-0 - Cyber Security – Incident Reporting and Response Planning

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 Each UFLS or UVLS System that:

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

NB Appendix
CIP-008-5-NB-0 - Cyber Security – Incident Reporting and Response Planning

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

NB Appendix
CIP-008-5-NB-0 - Cyber Security – Incident Reporting and Response Planning

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

NB Appendix
CIP-008-5-NB-0 - Cyber Security – Incident Reporting and Response Planning

B. Requirements and Measures

R1. No New Brunswick modifications

M1. No New Brunswick modifications

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	No New Brunswick modifications		
1.2			
1.3			
1.4			

NB Appendix

CIP-008-5-NB-0 - Cyber Security – Incident Reporting and Response Planning

R2. No New Brunswick modifications

M2. No New Brunswick modifications

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.1	No New Brunswick modifications		
2.2			
2.3			

NB Appendix

CIP-008-5-NB-0 - Cyber Security – Incident Reporting and Response Planning

R3. No New Brunswick modifications

M3. No New Brunswick modifications

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	Applicable Systems	Requirements	Measures
3.1	No New Brunswick modifications		
3.2			

NB Appendix
CIP-008-5-NB-0 - Cyber Security – Incident Reporting and Response Planning

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

NB Appendix

CIP-008-5-NB-0 - Cyber Security – Incident Reporting and Response Planning

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	No New Brunswick modifications					
R2						
R3						

NB Appendix
CIP-008-5-NB-0 - Cyber Security – Incident Reporting and Response Planning

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.

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:

No New Brunswick modifications

Rationale:

No New Brunswick modifications

Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the bulk power system caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: No New Brunswick modifications

**NB Appendix
Guidelines and Technical Basis**

Reference to prior version: No New Brunswick modifications

Reference to prior version: No New Brunswick modifications

Change Description and Justification: No New Brunswick modifications

Reference to prior version: No New Brunswick modifications

Reference to prior version: No New Brunswick modifications

Change Description and Justification: No New Brunswick modifications

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the bulk power system caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

No New Brunswick modifications

Summary of Changes: No New Brunswick modifications

Reference to prior version: No New Brunswick modifications

Change Description and Justification: No New Brunswick modifications

Reference to prior version: No New Brunswick modifications

Change Description and Justification: No New Brunswick modifications

Reference to prior version: No New Brunswick modifications

Change Description and Justification: No New Brunswick modifications

Rationale for R3:

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	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	