

**Annexes Québec des normes de fiabilité en
suivi de modifications (versions française et
anglaise)**

Annexe CIP-005-7-QC-1

Dispositions particulières applicables au Québec visant la norme CIP-005-67 – Cybersécurité – Périmètres de sécurité électronique

Cette-La présente annexe établit les dispositions particulières d'application au Québec de la norme ~~au Québec qu'elle vise~~. Les dispositions de la norme visée et de ~~son~~ l'annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe a préséance.

A. Introduction

1. **Titre :** Aucune disposition particulière.
2. **Numéro :** Aucune disposition particulière.
3. **Objet :** Aucune disposition particulière.
4. **Applicabilité :**

4.1. Entités fonctionnelles

Aucune disposition particulière

4.2. Installations

La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

- Toute installation de production qui répond aux deux conditions suivantes : (1) la puissance nominale de l'installation est de 300 MVA ou moins et (2) aucun groupe de l'installation ne peut être synchronisé avec un réseau voisin.
- Postes élévateurs des installations de production identifiées au point précédent.

5. Date d'entrée en vigueur ~~au Québec~~ :

- | | |
|--|--------------|
| 5.1. Adoption de la norme par la Régie de l'énergie : | xx mois 20xx |
| 5.2. Adoption de l'annexe par la Régie de l'énergie : | xx mois 20xx |
| 5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : | xx mois 20xx |

6. Contexte : Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Annexe CIP-005-7-QC-1

Dispositions particulières applicables au Québec visant la norme CIP-005-67 – Cybersécurité – Périmètres de sécurité électronique

Au Québec, le terme *responsable des mesures pour assurer la conformité* désigne la Régie de l'énergie dans le rôle visant à surveiller la conformité avec la norme de fiabilité visée et à la présente annexe, et à assurer l'application de celles-ci.

1.2. Conservation des pièces justificatives

Aucune disposition particulière.

1.3. Programme de surveillance de la conformité et d'application des normes

La Régie de l'énergie établit les processus de surveillance qui servent à évaluer les données ou l'information afin de déterminer la conformité ou la non-conformité avec la norme de fiabilité visée et avec la présente annexe.

Niveau de gravité de la non-conformité (VSL)

Aucune disposition particulière.

D. Différences régionales

Aucune disposition particulière.

E. Documents connexes

Aucune disposition particulière.

Principes directeurs et fondements techniques

~~Aucune disposition particulière.~~

Justifications

~~Aucune disposition particulière.~~

Historique des révisions

Version	Date	Intervention	Suivi des modifications
1	xx mois 20xx	Nouvelle annexe <u>en suivi de la décision D-xxxx-yyyy.</u>	Nouvelle

Annexe CIP-010-4-QC-1

Dispositions particulières applicables au Québec visant la norme

CIP-010-34 – Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

La présente annexe établit les dispositions particulières d'application au Québec de la norme qu'elle vise. Les dispositions de la norme visée et de l'annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe a préséance.

A. Introduction

1. **Titre :** Aucune disposition particulière.
2. **Numéro :** Aucune disposition particulière.
3. **Objet :** Aucune disposition particulière.
4. **Applicabilité :**

4.1. Entités fonctionnelles

Aucune disposition particulière.

4.2. Installations

La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

- Toute installation de production qui répond aux deux conditions suivantes : (1) la puissance nominale de l'installation est de 300 MVA ou moins et (2) aucun groupe de l'installation ne peut être synchronisé avec un réseau voisin.
- Postes élévateurs des installations de production identifiées au point précédent.

5. Date d'entrée en vigueur :

- 5.1. Adoption de la norme par la Régie de l'énergie : xx mois 20xx
- 5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 20xx
- 5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : xx mois 20xx

6. Contexte : Aucune disposition particulière.

B. Exigences et mesures

Aucune disposition particulière.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Annexe CIP-010-4-QC-1

Dispositions particulières applicables au Québec visant la norme

CIP-010-34 – Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

Au Québec, le terme *responsable des mesures pour assurer la conformité* désigne la Régie de l'énergie dans le rôle visant à surveiller la conformité avec la norme de fiabilité visée et à la présente annexe, et à assurer l'application de celles-ci.

1.2. Conservation des pièces justificatives

Aucune disposition particulière.

1.3. Programme de surveillance de la conformité et d'application des normes

La Régie de l'énergie établit les processus de surveillance qui servent à évaluer les données ou l'information afin de déterminer la conformité ou la non-conformité avec la norme de fiabilité visée et avec la présente annexe.

Niveau de gravité de la non-conformité (VSL)

Aucune disposition particulière.

~~Correction de l'erratum pour le VSL modéré de l'exigence E3, ajout « et moins de 21 mois » dans la partie suivante de la phrase « a effectué une analyse de vulnérabilité dans un délai de plus de 18 mois et de moins de 21 mois suivant la dernière analyse de l'un de ses systèmes.~~

Ex.#	VSL faible	VSL modéré	VSL élevé	VSL critique
E3.	L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses systèmes électroniques BES visés, mais elle a effectué une analyse de vulnérabilité dans un délai de plus de 15 mois et de moins de 18 mois suivant la dernière analyse de l'un de ses systèmes électroniques BES visés. (3.1)	L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses systèmes électroniques BES visés, mais elle a effectué une analyse de vulnérabilité dans un délai de plus de 18 mois et de moins de 21 mois suivant la dernière analyse de l'un de ses systèmes électroniques BES visés. (3.1)	L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses systèmes électroniques BES visés, mais elle a effectué une analyse de vulnérabilité dans un délai de plus de 21 mois et de moins de 24 mois suivant la dernière analyse de l'un de ses systèmes électroniques BES visés. (3.1)	L'entité responsable n'a mis en œuvre aucun processus d'analyse de vulnérabilité pour un de ses systèmes électroniques BES visés. (E3) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses systèmes électroniques BES visés, mais elle a effectué une analyse de vulnérabilité plus de 24 mois suivant la
	OU	OU	OU	
	L'entité responsable a mis en œuvre un ou	L'entité responsable a mis en œuvre un ou	L'entité responsable a mis en œuvre un ou	

Annexe CIP-010-4-QC-1

Dispositions particulières applicables au Québec visant la norme

CIP-010-34 – Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

	<p>plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 36 mois et de moins de 39 mois suivant la dernière analyse active de l'un de ses systèmes électroniques BES visés. (3.2)</p>	<p>plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 39 mois et de moins de 42 mois suivant la dernière analyse active de l'un de ses systèmes électroniques BES visés. (3.2)</p>	<p>plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 42 mois et de moins de 45 mois suivant la dernière analyse active de l'un de ses systèmes électroniques BES visés. (3.2)</p>	<p>dernière analyse de l'un de ses systèmes électroniques BES visés. (3.1)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 45 mois suivant la dernière analyse active de l'un de ses systèmes électroniques BES visés. (3.2)</p> <p>OU</p> <p>L'entité responsable a mis en œuvre et documenté un ou plusieurs processus d'analyse de vulnérabilité pour chacun de ses systèmes électroniques BES visés, mais elle n'a pas effectué l'analyse de vulnérabilité active d'une manière qui simule une configuration de référence existante de ses systèmes électroniques BES visés. (3.3)</p>
--	---	---	---	---

Annexe CIP-010-4-QC-1

Dispositions particulières applicables au Québec visant la norme

CIP-010-34 – Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

				<p>OU</p> <p>L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses systèmes électroniques BES visés, mais elle n'a pas documenté les résultats des analyses de vulnérabilité, les plans d'action pour corriger ou atténuer les vulnérabilités constatées dans les analyses, la date planifiée d'achèvement du plan d'action et l'état d'exécution des plans d'atténuation. (3.4)</p>
--	--	--	--	---

D. Différences régionales

Aucune disposition particulière.

E. Documents connexes

Aucune disposition particulière.

CIP-010-4 – Annexe 1

Aucune disposition particulière.

CIP-010-4 – Annexe 2

Aucune disposition particulière

Principes directeurs et fondements techniques

~~Aucune disposition particulière.~~

Historique des révisions

Version	Date	Intervention	Suivi des modifications
---------	------	--------------	-------------------------

Annexe CIP-010-4-QC-1

Dispositions particulières applicables au Québec visant la norme

CIP-010-34 – Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

1	xx mois 20xx	Nouvelle annexe <u>en suivi de la décision D- xxxx-yyy.</u>	Nouvelle
---	--------------	---	----------

Annexe CIP-013-2-QC-1

Dispositions particulières applicables au Québec visant la norme

CIP-013-42 – Cybersécurité — Gestion des risques dans la chaîne d’approvisionnement

La présente annexe établit les dispositions particulières d’application au Québec de la norme qu’elle vise. Les dispositions de la norme visée et de l’annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d’interprétation. En cas de divergence entre la norme et l’annexe, l’annexe a préséance.

A. Introduction

1. **Titre :** Aucune disposition particulière.
2. **Numéro :** Aucune disposition particulière.
3. **Objet :** Aucune disposition particulière.
4. **Applicabilité :**

4.1. Entités fonctionnelles

Aucune disposition particulière.

4.2. Installations

La présente norme s’applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l’application de cette norme, toute référence aux termes « *système de production-transport d’électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

Exemptions additionnelles

Sont exemptés de l’application de la présente norme :

- Toute installation de production qui répond aux deux conditions suivantes : (1) la puissance nominale de l’installation est de 300 MVA ou moins et (2) aucun groupe de l’installation ne peut être synchronisé avec un réseau voisin.
- Postes élévateurs des installations de production identifiées au point précédent.

5. Date d’entrée en vigueur :

- | | |
|--|--------------|
| 5.1. Adoption de la norme par la Régie de l’énergie : | xx mois 20xx |
| 5.2. Adoption de l’annexe par la Régie de l’énergie : | xx mois 20xx |
| 5.3. Date d’entrée en vigueur de la norme et de l’annexe au Québec : | xx mois 20xx |

B. Exigences et mesures

Aucune disposition particulière.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Au Québec, le terme *responsable des mesures pour assurer la conformité* désigne la Régie de l’énergie dans le rôle visant à surveiller la conformité avec la norme de fiabilité visée et à la présente annexe, et à assurer l’application de celles-ci.

Annexe CIP-013-2-QC-1

Dispositions particulières applicables au Québec visant la norme

CIP-013-42 – Cybersécurité — Gestion des risques dans la chaîne d’approvisionnement

1.2. Conservation des pièces justificatives

Aucune disposition particulière.

1.3. Programme de surveillance de la conformité et d’application des normes

La Régie de l’énergie établit les processus de surveillance qui servent à évaluer les données ou l’information afin de déterminer la conformité ou la non-conformité avec la norme de fiabilité visée et avec la présente annexe.

Niveau de gravité de la non-conformité (VSL)

Aucune disposition particulière.

D. Différences régionales

Aucune disposition particulière.

E. Documents connexes

Aucune disposition particulière.

Justification

~~Aucune disposition particulière~~

Historique des révisions

Version	Date	Intervention	Suivi des modifications
1	xx mois 20xx	Nouvelle annexe en suivi de la décision-D-xxxx-yyyy.	Nouvelle

Appendix CIP-005-7-QC-1
Specific provisions applicable in Québec for standard
CIP-005-67 – Cyber Security – Electronic Security Perimeter(s)

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** No specific provisions.
2. **Number:** No specific provisions.
3. **Purpose:** No specific provisions.
4. **Applicability:**

4.1. Functional Entities

No specific provisions.

4.2. Facilities

This standard only applies to the facilities of the Main Transmission System (RTP) and to the facilities specified for the Distribution Provider. In the application of this standard, all reference to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

Additional Exemptions

The following are exempt from this standard:

- Any generating facility that meets the two following conditions: (1) the nameplate capacity of the facility is 300 MVA or less, and (2) no unit of the facility can be synchronized with a neighbouring system.
- Step-up substations of generating facilities identified in the preceding point.

5. **Effective Date:**

- | | |
|---|----------------|
| 5.1. Adoption of the standard by the Régie de l'énergie: | Month xx, 20xx |
| 5.2. Adoption of the appendix by the Régie de l'énergie: | Month xx, 20xx |
| 5.3. Effective date of the standard and its appendix in Québec: | Month xx, 20xx |

6. **Background:** No specific provisions.

B. Requirements and Measures

No specific provisions.

C. Compliance

1. **Compliance Monitoring Process**

1.1. **Compliance Enforcement Authority**

~~The Régie de l'énergie is responsible, in Québec, for compliance enforcement with respect to the reliability standard and its appendix that it adopts.~~

Appendix CIP-005-7-QC-1
Specific provisions applicable in Québec for standard
CIP-005-67 – Cyber Security – Electronic Security Perimeter(s)

In Québec, “Compliance Enforcement Authority” means the Régie de l’énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

~~No specific provisions.~~

The Régie de l’énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels (VSL)

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Guidelines and technical basis

~~No specific provisions.~~

Rationale

~~No specific provisions.~~

Version History

Version	Date	Action	Change Tracking
1	Month xx, 20xx	New appendix <u>as per decision D-xxxx-yyyy.</u>	New

Appendix CIP-010-4-QC-1
Specific provisions applicable in Québec for standard
CIP-010-34 – Cyber Security — Configuration Change Management and Vulnerability
Assessments

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** No specific provisions.
2. **Number:** No specific provisions.
3. **Purpose:** No specific provisions.
4. **Applicability:**

4.1. Functional Entities

No specific provisions.

4.2. Facilities

This standard only applies to the facilities of the Main Transmission System (RTP) and to the facilities specified for the Distribution Provider. In the application of this standard, all reference to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

Additional Exemptions

The following are exempt from this standard:

- Any generating facility that meets the two following conditions: (1) the nameplate capacity of the facility is 300 MVA or less, and (2) no unit of the facility can be synchronized with a neighbouring system.
- Step-up substations of generating facilities identified in the preceding point.

5. **Effective Date:**

- | | |
|---|----------------|
| 5.1. Adoption of the standard by the Régie de l'énergie: | Month xx, 20xx |
| 5.2. Adoption of the appendix by the Régie de l'énergie: | Month xx, 20xx |
| 5.3. Effective date of the standard and its appendix in Québec: | Month xx, 20xx |

6. **Background:** No specific provisions.

B. Requirements and Measures

No specific provisions.

C. Compliance

1. **Compliance Monitoring Process**

1.1. **Compliance Enforcement Authority**

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

Appendix CIP-010-4-QC-1
Specific provisions applicable in Québec for standard
CIP-010-34 – Cyber Security — Configuration Change Management and Vulnerability Assessments

1.2. Evidence Retention

No specific provisions.

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels (VSL)

No specific provisions.

~~Erratum correction in the Moderate VSL for Requirement R3, added "less than 21 months" in the following part of the sentence "has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its applicable BES Cyber Systems (3.1)."~~

R#	Lower-VSL	Moderate-VSL	High-VSL	Severe-VSL
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24

Appendix CIP-010-4-QC-1
Specific provisions applicable in Québec for standard
CIP-010-34 – Cyber Security — Configuration Change Management and Vulnerability
Assessments

	<p>implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)</p>	<p>documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)</p>	<p>implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)</p>	<p>months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (3.2)</p> <p>OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in</p>
--	--	--	--	---

Appendix CIP-010-4-QC-1
Specific provisions applicable in Québec for standard
CIP-010-34 – Cyber Security — Configuration Change Management and Vulnerability
Assessments

				<p>a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3)</p> <p>OR</p> <p>The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)</p>
--	--	--	--	--

D. Regional Variances

No specific provisions.

~~E. Interpretations~~

Appendix CIP-010-4-QC-1
Specific provisions applicable in Québec for standard
CIP-010-34 – Cyber Security — Configuration Change Management and Vulnerability
Assessments

~~No specific provisions.~~

E. Associated Documents

~~No specific provisions.~~

CIP-010-4 - Attachment 1

No specific provisions.

CIP-010-4 - Attachment 2

No specific provisions.

Guidelines and technical basis

~~No specific provisions.~~

Rationale

~~No specific provisions.~~

Version History

Version	Date	Action	Change Tracking
1	Month xx, 20xx	New appendix <u>as per decision D-xxxx-yyyy.</u>	New

Appendix CIP-013-2-QC-1
Specific provisions applicable in Québec for standard
CIP-013-42 – Cyber Security —Supply Chain Risk Management

This appendix establishes specific provisions for the application of the standard in Québec. Provisions of the standard and of this appendix must be read jointly for comprehension and interpretation purposes. Where the standard and appendix differ, the appendix shall prevail.

A. Introduction

1. **Title:** No specific provisions.
2. **Number:** No specific provisions.
3. **Purpose:** No specific provisions.
4. **Applicability:**

4.1. Functional Entities

No specific provision.

4.2. Facilities

This standard only applies to the facilities of the Main Transmission System (RTP) and to the facilities specified for the Distribution Provider. In the application of this standard, all reference to the terms "Bulk Electric System" or "BES" shall be replaced by the terms "Main Transmission System" or "RTP" respectively.

Additional Exemptions

The following are exempt from this standard:

- Any generating facility that meets the two following conditions: (1) the nameplate capacity of the facility is 300 MVA or less, and (2) no unit of the facility can be synchronized with a neighbouring system.
- Step-up substations of generating facilities identified in the preceding point.

5. **Effective Date:**

- | | |
|---|----------------|
| 5.1. Adoption of the standard by the Régie de l'énergie: | Month xx, 20xx |
| 5.2. Adoption of the appendix by the Régie de l'énergie: | Month xx, 20xx |
| 5.3. Effective date of the standard and its appendix in Québec: | Month xx, 20xx |

B. Requirements and Measures

No specific provisions.

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority

In Québec, "Compliance Enforcement Authority" means the Régie de l'énergie in its roles of monitoring and enforcing compliance with respect to the Reliability Standard and to this appendix.

1.2. Evidence Retention

No specific provisions.

Appendix CIP-013-2-QC-1
Specific provisions applicable in Québec for standard
CIP-013-42 – Cyber Security —Supply Chain Risk Management

1.3. Compliance Monitoring and Enforcement Program

The Régie de l'énergie establishes the monitoring processes used to evaluate data or information for the purpose of determining compliance or non-compliance with the Reliability Standard and with this appendix.

Violation Severity Levels (VSL)

No specific provisions.

D. Regional Variances

No specific provisions.

E. Associated Documents

No specific provisions.

Rationale

No specific provision

Version History

Version	Date	Action	Change Tracking
1	Month xx, 20xx	New appendix <u>as per decision D-xxxx-yyyy.</u>	New