

**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)."~~

<b>R#</b>	<b>Lower VSL</b>	<b>Moderate VSL</b>	<b>High VSL</b>	<b>Severe VSL</b>
<b>R3.</b>	<del>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</del>	<del>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</del>	<del>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</del>	<del>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</del>

**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><del>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)</del></p>	<p><del>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)</del></p>	<p><del>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)</del></p>	<p><del>months since the last assessment on one of its applicable BES Cyber Systems. (3.1)</del>  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)  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

---

				<div>a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR 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)</div>
--	--	--	--	--

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