

**Demande visant  
l'adoption de 10 normes de fiabilité portant  
sur la protection des infrastructures critiques  
(normes CIP v5)**



## Table des matières

1	Contexte et contenu de la demande.....	5
2	Normes de fiabilité de la NERC pour adoption par la Régie .....	5
2.1	Dispositions particulières applicables au Québec.....	9
3	Processus de consultation publique .....	10
3.1	Étapes franchies .....	10
3.2	Commentaires .....	11
4	Évaluation de la pertinence et des impacts des normes déposées .....	11
4.1	Évaluation de la pertinence.....	11
4.2	Évaluation de l'impact .....	12
5	Glossaire des termes et des acronymes relatifs aux normes de fiabilité .....	13
6	Registre des entités visées par les normes de fiabilité .....	13
7	Conclusion .....	14
	Annexe A.....	15

### Liste des tableaux

Tableau 1	Évaluation de l'impact monétaire des normes (M\$).....	13
-----------	--	----



## **1 Contexte et contenu de la demande**

1 Conformément aux dispositions de la *Loi sur la Régie de l'énergie* (la « Loi »), le  
2 coordonnateur de la fiabilité au Québec (le « Coordonnateur ») soumet, pour adoption par la  
3 Régie de l'énergie (la « Régie »), dix normes de fiabilité portant sur la protection des  
4 infrastructures critiques (les « normes CIP ») de la *North American Electric Reliability*  
5 *Corporation* (la « NERC »), soit les normes CIP-002-5.1, CIP-003-5, CIP-004-5.1, CIP005-5,  
6 CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 et CIP-011-1 (les « normes CIP  
7 v5 ») et leur Annexe respective ainsi que les modifications au Glossaire des termes et des  
8 acronymes relatifs aux normes de fiabilité (le « Glossaire »)<sup>1</sup>. Le Coordonnateur soumet  
9 aussi, pour approbation par la Régie, les modifications au Registre des entités visées par  
10 les normes de fiabilité (le « Registre »)<sup>2</sup>. Par conséquent, le Coordonnateur demande  
11 également le retrait des normes CIP-002-1 à CIP-009-1 (les « normes CIP v1 ») adoptées  
12 par la Régie dans ses décisions D-2012-091, D-2013-176 et D-2014-048 dans le cadre du  
13 dossier R-3699-2009, phase I, et dont l'entrée en vigueur a été suspendue par la Régie  
14 dans sa décision D-2015-168.

15 Le Coordonnateur présente les dix normes proposées à la pièce HQCMÉ-2, Document 1  
16 (version française) et à la pièce HQCMÉ-2, Document 2 (version anglaise), ainsi que les  
17 modifications proposées au Glossaire à la pièce HQCMÉ-2, Document 3.

18 La présente demande inclut des informations connexes présentées aux sections 2 et 3. La  
19 section 2 présente les normes de fiabilité proposées. La section 3 rend compte de  
20 l'application du processus de consultation publique à leur égard. La section 4 traite de  
21 l'évaluation de la pertinence et de l'impact des normes proposées.

22 Enfin, la section 5 présente les modifications proposées au Glossaire alors que la section 6  
23 présente celles au Registre.

## **2 Normes de fiabilité de la NERC pour adoption par la Régie**

24 Les dix normes de fiabilité de la NERC que le Coordonnateur soumet pour adoption à la  
25 Régie portent sur la protection des infrastructures critiques. Elles ont été approuvées par la  
26 FERC dans l'ordonnance n° 791 le 22 novembre 2013 et deviendront obligatoires, aux  
27 États-Unis et dans d'autres provinces canadiennes, dès le 1<sup>er</sup> avril 2016. Ces normes,  
28 sommairement décrites ci-après, constituent ce que l'industrie désigne comme étant la  
29 version 5 des normes CIP.

---

<sup>1</sup> Glossaire adopté par la Régie de l'énergie (décision D-2015-098), 23 juin 2015

<sup>2</sup> Registre des entités approuvé par la Régie de l'énergie (décision D-2015-098), 23 juin 2015

- 1       • CIP-002-5.1 - Catégorisation des systèmes électroniques BES : Cette norme exige  
2 d'inventorier et de catégoriser les systèmes électroniques BES et leurs actifs  
3 électroniques BES connexes, en fonction de critères spécifiques pour l'application  
4 des exigences de cybersécurité proportionnelle à l'impact négatif que la perte, la  
5 dégradation ou la mauvaise utilisation de ces systèmes électroniques BES pourrait  
6 avoir sur l'exploitation fiable du BES. L'inventaire et la catégorisation des systèmes  
7 électroniques BES permettent d'établir une protection appropriée contre les  
8 dégradations qui pourraient entraîner un fonctionnement incorrect ou une instabilité  
9 du BES.
- 10       • CIP-003-5 - Mécanismes de gestion de la sécurité : Cette norme exige des entités  
11 responsables qu'elles définissent des mécanismes de gestion de la sécurité  
12 cohérents et viables qui établissent les responsabilités et l'imputabilité à l'égard de  
13 la protection des systèmes électroniques BES contre les compromissions qui  
14 pourraient entraîner un fonctionnement incorrect ou des instabilités dans le BES.  
15 Plusieurs politiques de cybersécurité (par exemple, personnel et formation,  
16 périmètres de sécurité électronique, plans de rétablissement des systèmes  
17 électroniques, gestion des changements de configuration et analyses de  
18 vulnérabilité) doivent être mises en œuvre et l'entité responsable doit confier à un  
19 cadre supérieur CIP la responsabilité de mener et de gérer l'implantation et le  
20 respect permanent des normes CIP.
- 21       • CIP-004-5.1 - Personnel et formation : Cette norme vise à minimiser les risques de  
22 compromissions, qui pourraient entraîner un fonctionnement incorrect ou une  
23 instabilité du BES, attribuables à des personnes qui accèdent à des systèmes  
24 électroniques BES, en exigeant la gestion des accès, une évaluation des risques  
25 liés au personnel, une formation et une sensibilisation à la sécurité qui soient  
26 adéquates pour protéger ces systèmes électroniques BES.
- 27       • CIP-005-5 - Périmètres de sécurité électroniques : Cette norme impose aux entités  
28 responsables de gérer l'accès électronique aux systèmes électroniques BES en  
29 établissant un périmètre de sécurité électronique (ESP) contrôlé afin de protéger  
30 les systèmes électroniques BES contre les compromissions qui pourraient entraîner  
31 un fonctionnement incorrect ou une instabilité dans le BES. Le contrôle des flux  
32 entrants et sortants du périmètre de sécurité électronique et la gestion des accès  
33 distants interactifs à l'aide d'authentification multifactorielle sont des exemples  
34 d'exigences que l'on trouve dans cette norme.
- 35       • CIP-006-5 - Sécurité physique des systèmes électroniques BES : Cette norme vise  
36 à gérer l'accès physique aux systèmes électroniques BES en établissant un plan de

1            sécurité physique afin de protéger les systèmes électroniques BES contre les  
2            compromissions qui pourraient entraîner un fonctionnement incorrect ou une  
3            instabilité dans le BES. Par exemple, l'utilisation de cartes d'accès, les systèmes  
4            de verrouillage, le personnel de sécurité et les dispositifs d'authentification tels que  
5            les systèmes de lecteurs de carte d'accès et de saisie de code d'accès [numéro  
6            d'identification personnel (NIP)] sont autant de méthodes utilisées pour assurer la  
7            sécurité physique des actifs électroniques. La mise en place d'un programme de  
8            contrôle d'accès des visiteurs et d'un programme de maintenance et d'essai des  
9            systèmes de contrôle d'accès physiques sont également requis.

10           • CIP-007-5 - Gestion de la sécurité des systèmes : Cette norme vise à gérer la  
11           sécurité des systèmes en établissant des exigences techniques, opérationnelles et  
12           administratives particulières afin de protéger les systèmes électroniques BES  
13           contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou  
14           une instabilité dans le BES. Par exemple, les entités responsables doivent avoir en  
15           place un processus permettant la gestion des ports et services, des rustines de  
16           sécurité et des logiciels pour la protection contre le code malveillant. De plus, des  
17           processus documentés doivent être prévus pour la surveillance des incidents de  
18           sécurité et la gestion des comptes d'accès logiques.

19           • CIP-008-5 - Déclaration des incidents et planification des mesures d'intervention :  
20           Cette norme vise à réduire les risques posés au fonctionnement fiable du BES par  
21           un incident de cybersécurité en définissant des exigences d'intervention en cas  
22           d'incident. Un plan d'intervention en cas d'incidents de cybersécurité doit être  
23           établi, et tous les incidents doivent être documentés.

24           • CIP-009-5 - Plans de rétablissement des systèmes électroniques BES : Cette  
25           norme définit les exigences relatives aux plans de rétablissement en vue du  
26           maintien de la stabilité, de l'exploitabilité et de la fiabilité du BES. Par exemple, les  
27           entités responsables doivent avoir instauré des plans de rétablissement des  
28           systèmes électroniques BES qui seront soumis à un exercice annuel.

29           • CIP-010-1 - Gestion des changements de configuration et analyses de  
30           vulnérabilité : Cette norme vise à prévenir et détecter les changements non  
31           autorisés aux systèmes électroniques BES au moyen d'exigences relatives à la  
32           gestion et à la surveillance des changements de configuration. De plus, des  
33           analyses de vulnérabilité doivent être réalisées en vue d'identifier et de corriger les  
34           lacunes ciblées.

35           • CIP-011-1 - Protection de l'information : Cette norme vise à empêcher tout accès  
36           non autorisé à l'information de système électronique BES en définissant des

1 exigences de protection de l'information visant à prévenir toute compromission  
2 pouvant entraîner un fonctionnement incorrect ou une instabilité dans le BES. De  
3 plus, un processus documenté doit être prévu pour la réutilisation et l'élimination  
4 sécuritaire d'un actif électronique BES qui contient de l'information de système  
5 électronique BES dans le but d'empêcher la diffusion non autorisée d'information.

6 Cette nouvelle version des normes CIP représente une amélioration importante par rapport  
7 à la version 1 des normes CIP adoptées par la Régie de l'énergie dans ses décisions  
8 D-2012-091, D-2013-176 et D-2014-048 dans le cadre du dossier R-3699-2009, phase I.  
9 Les normes CIP v5, bien que présentant un cadre semblable aux versions antérieures,  
10 proposent une approche plus robuste pour la catégorisation du niveau de risque que pose  
11 un actif en particulier. Notamment, cette version utilise une approche basée sur les  
12 pratiques du National Institute of Standards and Technology (NIST) consistant à catégoriser  
13 les systèmes selon leur degré d'impact (faible, moyen ou élevé) sur le système de  
14 production-transport d'électricité. De plus, la version 5 est améliorée grâce à l'expérience  
15 acquise par l'industrie dans la mise en œuvre des versions antérieures et en comble les  
16 lacunes. En effet, cette nouvelle version propose une approche plus systématique en  
17 imposant des critères précis<sup>3</sup> pour l'identification des infrastructures critiques assurant ainsi  
18 l'application d'un niveau de protection adéquat à tous les systèmes pouvant avoir un impact  
19 sur la fiabilité de l'Interconnexion. L'identification des systèmes critiques n'est donc plus  
20 fonction d'une méthodologie développée par l'entité comme c'était le cas pour les versions 1  
21 à 3 des normes CIP.

22 Le Coordonnateur propose de passer directement de la version 1 à la version 5 dans une  
23 optique d'harmonisation du régime de fiabilité québécois avec ceux des juridictions voisines.  
24 En effet, les versions 2 et 4 n'ont pas été mises en vigueur dans les autres juridictions. Par  
25 ailleurs, même si une mise à jour en fonction de la version 3 actuellement en vigueur aux  
26 États-Unis avait été possible dans le cadre du dossier R-3699-2009, le développement de la  
27 version 5 avait déjà été entamé. Dans un souci d'efficacité réglementaire, le Coordonnateur  
28 a donc jugé préférable d'attendre l'approbation de la version 5 par les instances  
29 réglementaires américaines pour passer directement à cette version.

---

<sup>3</sup> Ces critères sont définis à l'annexe 1 de la norme CIP-002-5.1



## **2.1 Dispositions particulières applicables au Québec**

1 Le Coordonnateur souligne qu'il ne dépose aucune variante ou autre norme spécifique au  
2 Québec, autre que celles présentées sous forme de disposition particulière pour le Québec  
3 dans les annexes de chacune des normes présentées à la pièce HQCMÉ-2, Document 1  
4 (version française) et à la pièce HQCMÉ-2, Document 2 (version anglaise).

5 Ces dispositions particulières, soit des aspects normatifs à caractère technique ainsi que  
6 des aspects normatifs à caractère administratif spécifiques à l'application de la norme au  
7 Québec, sont les suivantes :

- 8 • Applicabilité – installations : le champ d'application tel que défini à la section 4.2  
9 des normes CIP v5 est le réseau de transport principal (RTP) à l'instar du champ  
10 d'application approuvé par la Régie pour les normes CIP v1 par les décisions  
11 D-2012-091, D-2013-176 et D-2014-048. Toute référence aux termes « systèmes  
12 de production-transport d'électricité » ou « BES » est remplacée par les termes  
13 « réseau de transport principal » ou « RTP » respectivement.
- 14 • Applicabilité – Exemptions additionnelles : sont exemptées de l'application des  
15 normes CIP v5 les installations de production ayant une puissance nominale de  
16 300 MVA ou moins, incluant leur poste élévateur, à l'exception des installations  
17 comprenant un ou plusieurs groupes pouvant être îlotés sur un réseau voisin afin  
18 d'éviter tout impact sur ces réseaux. Cette exemption est fondée notamment sur les  
19 capacités de réponse du système de réglage fréquence-puissance (RFP) propre à  
20 l'interconnexion du Québec. Les informations relatives à cette exemption  
21 additionnelle sont présentées sous pli confidentiel à la pièce HQCMÉ-1,  
22 Document 4.

23 Le Coordonnateur propose l'introduction de cette exemption afin de permettre aux  
24 entités de concentrer leurs efforts sur la protection des systèmes électroniques qui  
25 ont un risque accru sur la fiabilité du RTP. Cela permettra également de réduire  
26 potentiellement les coûts associés à la conformité aux normes CIP en exemptant  
27 les installations dont l'impact des systèmes électroniques sur la fiabilité est  
28 négligeable. La disposition particulière aura donc pour bénéfice de mettre  
29 l'emphase sur les systèmes électroniques ayant un impact potentiel important et  
30 d'éviter des coûts notables pour des systèmes n'ayant peu ou pas d'impact.

### **3 Processus de consultation publique**

1 Le Coordonnateur a suivi le processus de consultation tel que décrit à l'annexe de la  
2 décision D-2011-139 pour les normes de fiabilité faisant l'objet de la présente demande.

#### **3.1 Étapes franchies**

3 Le 2 décembre 2014, le Coordonnateur publie sur son site Internet les documents proposés  
4 suivants :

- 5 • Les normes de fiabilité proposées CIP-002-5.1, CIP-003-5, CIP-004-5.1, CIP-005-5,  
6 CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, CIP-011-1 ;
- 7 • L'annexe afférente à chaque norme proposée contenant les aspects normatifs à  
8 caractère technique et administratif propres à l'Interconnexion du Québec ;
- 9 • Un sommaire décrivant les normes proposées, y compris une évaluation  
10 préliminaire de la pertinence et de l'impact de ces normes, et les modifications  
11 proposées au Glossaire ;
- 12 • les modifications proposées au Registre.

13 Le Coordonnateur présente ce sommaire ainsi que les dates d'entrée en vigueur proposées  
14 pour ces normes à la pièce HQCMÉ-1, Document 2.

15 De plus, le Coordonnateur diffuse un premier avis de consultation sur son site Internet et le  
16 transmet à la Régie, à la NERC, au Northeast Power Coordinating Council, Inc. (« NPCC »)  
17 et à toutes les entités inscrites au Registre. Cet avis de consultation précisait la durée de la  
18 consultation (2 décembre 2014 au 2 février 2015) et demandait des commentaires écrits sur  
19 l'ensemble des documents proposés.

20 Le 15 janvier 2015, le Coordonnateur tient une séance d'information sous forme de  
21 webinaire avec les entités visées pour présenter l'évaluation préliminaire de la pertinence et  
22 des impacts des normes proposées de même que les documents proposés.

23 Le 23 janvier 2015, le Coordonnateur publie sur son site Internet la présentation et une  
24 transcription des questions de ces entités et des réponses du Coordonnateur discutées lors  
25 de cette séance et informe également les entités visées de cette publication.

26 Par ailleurs, la période de consultation a été prolongée du 2 au 20 février 2015 à la  
27 demande d'une entité.

28 Le 17 septembre 2015, le Coordonnateur diffuse, suivant les commentaires reçus lors de la  
29 première période de consultation, un second avis de consultation sur son site Internet et le  
30 transmet à la Régie, à la NERC, au NPCC et à toutes les entités inscrites au Registre. Cet  
31 avis de consultation précisait la durée de la consultation (17 au 29 septembre 2015) et

1 demandait des commentaires écrits sur l'impact de la disposition particulière visant  
2 l'exemption de certaines installations de production et de leur poste élévateur de  
3 l'application des normes CIP v5.

### **3.2 Commentaires**

4 Au terme de la première période de consultation, quatre entités ont émis plusieurs  
5 commentaires. Le Coordonnateur publie les commentaires ainsi que ses réponses sur son  
6 site Internet le 16 avril 2015 et informe également les entités visées de cette publication.

7 Le Coordonnateur produit, conformément au processus de consultation publique, un  
8 sommaire des commentaires reçus avec les raisons données et sa conclusion, qu'il dépose  
9 à la pièce HQCMÉ-1, Document 3.

10 Essentiellement, les commentaires reçus constituent des demandes de clarification ou des  
11 questions sur les normes proposées auxquelles le Coordonnateur a répondu. De plus,  
12 certains commentaires proposent de réduire la fréquence de contrôles prévus aux  
13 exigences des normes CIP-004-5.1, CIP-008-5, CIP-009-5 et CIP-010-1. Le Coordonnateur  
14 n'a pas retenu ces commentaires puisqu'il juge qu'il n'y a aucune spécificité technique  
15 propre à l'Interconnexion du Québec justifiant la réduction de la fréquence des contrôles.  
16 Par ailleurs, à la demande d'une entité, le Coordonnateur a accepté de modifier les délais  
17 d'entrée en vigueur proposés afin de donner le temps nécessaire aux entités de mettre en  
18 œuvre les normes CIP v5 : la date proposée, auparavant fixe, a été modifiée pour une date  
19 relative à l'adoption des normes par la Régie.

20 Au terme de la seconde période de consultation, deux entités (Hydro-Québec TransÉnergie  
21 et Hydro-Québec Production) ont répondu indiquant que la disposition particulière proposée  
22 n'avait pas d'impact sur leur évaluation des coûts. Aucune autre entité n'a formulé de  
23 commentaires à cet égard.

## **4 Évaluation de la pertinence et des impacts des normes déposées**

24 Tel que prévu au paragraphe 2 de l'article 85.6 de la Loi, le Coordonnateur fournit une  
25 évaluation de la pertinence et de l'impact des normes de fiabilité déposées, intégrant les  
26 commentaires et les intrants retenus.

### **4.1 Évaluation de la pertinence**

27 Du fait que les normes ont été développées par des représentants de l'industrie électrique  
28 nord-américaine, soumises à son approbation ainsi qu'à celle de la NERC et de la FERC, le  
29 Coordonnateur évalue la pertinence de ces normes en fonction du maintien de la fiabilité de  
30 l'Interconnexion du Québec.

1 Le Coordonnateur est d'avis que les normes proposées sont pertinentes et nécessaires, et  
2 contribueront au maintien de la fiabilité de l'Interconnexion Québec et, par le fait même, des  
3 réseaux interconnectés en assurant une protection adéquate des systèmes critiques à  
4 l'exploitation fiable du réseau de transport principal. En effet, tel que mentionné  
5 précédemment, ces normes présentent une amélioration importante des versions  
6 antérieures en imposant des critères précis pour l'identification des systèmes électroniques  
7 qui ont un impact potentiel sur l'exploitation du réseau de transport principal au Québec. De  
8 plus, l'adoption de ces normes favorisera l'harmonisation des pratiques entre le Québec, les  
9 provinces voisines et les États-Unis qui rendront également ces normes de fiabilité  
10 obligatoires. Aucune entité n'a d'ailleurs formulé de commentaires sur l'évaluation  
11 préliminaire du Coordonnateur.

12 L'évaluation de la pertinence des normes CIP v5 est présentée à la section 1 de la pièce  
13 HQCMÉ-1, Document 2.

#### **4.2 Évaluation de l'impact**

14 Dans le cadre de la consultation publique, le Coordonnateur présente tout d'abord une  
15 évaluation préliminaire de l'impact monétaire des normes qualifiant l'implantation, le  
16 maintien et le suivi de la conformité d'une norme par les niveaux « Faible », « Modéré » ou  
17 « Élevé ». Cette évaluation est présentée à la section 9 de la pièce HQCMÉ-1, Document 2.

18 Par la suite, le Coordonnateur présente une évaluation globale intégrant les évaluations  
19 reçues au terme de la période de consultation à la section 10 de ce même document.  
20 Énergie La Lièvre s.e.c., Hydro-Québec TransÉnergie, Hydro-Québec Production, Le  
21 groupe Ohméga Inc.<sup>4</sup>, Northland Power Inc. et Rio Tinto Alcan sont les seules entités ayant  
22 fourni une évaluation de l'impact des normes sur leurs activités. Selon les entités visées, les  
23 coûts indiqués représentent une évaluation approximative des coûts d'implantation, et de  
24 maintien et de suivi de la conformité.

25 L'évaluation de l'impact monétaire de ces normes est présentée au tableau 1 de façon  
26 globale puisque la nature des normes CIP ne permet pas, dans la plupart des cas, de  
27 dissocier l'application des différentes normes et donc d'évaluer l'impact monétaire des  
28 normes de façon distincte. L'impact est évalué selon deux catégories, soient les coûts liés à  
29 l'implantation des normes, et les coûts récurrents associés au maintien et au suivi de la  
30 conformité.

---

<sup>4</sup> Le groupe Ohméga Inc. n'est pas une entité identifiée au Registre. Cette firme représente certains parcs éoliens inscrits au Registre. Son évaluation représente le coût moyen de la mise en conformité aux normes CIP d'un parc éolien ayant seulement des systèmes électroniques BES à impact faible.

**Tableau 1**  
**Évaluation de l'impact monétaire des normes (M\$)**

<b>Entité</b>	<b>Implantation (M\$)</b>	<b>Maintien et suivi de la conformité (M\$/an)</b>
Énergie La Lièvre	0,00	0,00
Hydro-Québec Production	6,00	1,5
Hydro-Québec TransÉnergie	40,00	2,5
Le Groupe Ohméga Inc.	0,02	0,00
Northland Power	0,00	0,00
Rio Tinto Alcan	2,50	0,20
Total	48,52	4,20

1 Tel qu'il appert du tableau 1, les coûts d'implantation s'élèvent à 48,52 M\$ alors que les  
 2 coûts relatifs au maintien et au suivi de la conformité sont estimés à 4,20 M\$ par année.

**5 Glossaire des termes et des acronymes relatifs aux normes de fiabilité**

3 Le Coordonnateur présente les modifications au Glossaire qu'il soumet pour adoption à la  
 4 pièce HQCMÉ-2, document 3. Les ajouts, modifications et retraits de termes ont été  
 5 approuvés par la FERC dans l'ordonnance n° 791 relative aux normes CIP v5, le 22  
 6 novembre 2013. La liste de ces modifications est présentée en annexe A. Tel qu'il appert de  
 7 cette dernière, les modifications comportent l'ajout de 15 nouveaux termes, la modification  
 8 de quatre termes et le retrait de deux termes, dans leurs versions française et anglaise. Le  
 9 Coordonnateur souligne que l'adoption de ces modifications est essentielle à l'interprétation  
 10 des normes proposées pour adoption.

**6 Registre des entités visées par les normes de fiabilité**

11 La norme CIP-002-5.1 stipule que les entités responsables concernées doivent catégoriser  
 12 leurs systèmes électroniques BES et les actifs électroniques BES connexes, selon les  
 13 critères de l'annexe 1 de cette norme. Les entités responsables sont tenues d'inventorier et  
 14 de catégoriser les systèmes électroniques BES dont l'impact est élevé ou moyen. De plus,  
 15 les listes exigées par l'exigence E1 de cette norme doivent être revues sur une base

1 périodique pour s'assurer que tous les systèmes électroniques BES pertinents ont été  
2 correctement identifiés et catégorisés. Ces activités ne peuvent dorénavant plus être  
3 réalisées par le Coordonnateur de la fiabilité pour l'ensemble des entités visées au Québec  
4 comme c'était le cas en vertu des dispositions particulières d'application des normes CIP v1  
5 adoptées par la Régie.

6 Par conséquent, les modifications au Registre comportent le retrait de toute information à  
7 l'égard des actifs critiques, d'une part le champ « Actifs classés critiques aux fins des  
8 normes CIP » des fiches des entités visées (annexe A du Registre) et d'autre part, la  
9 colonne « Actif critique » des installations de transport, de production, de  
10 télécommunications et les centres d'exploitation (Annexes B, C, D et F du Registre).

11 Par ailleurs, une mention sera ajoutée à la colonne « Particularités » de l'annexe C  
12 identifiant les installations de production dont certains groupes peuvent être îlotés sur des  
13 réseaux à l'extérieur de l'Interconnexion du Québec afin de départager les installations qui  
14 sont visées par l'application des normes CIP de celles qui en sont exemptées.

## **7 Conclusion**

15 Le Coordonnateur soumet à la Régie que les normes de fiabilité de la NERC et leurs  
16 annexes respectives déposées au présent dossier sont essentielles et pertinentes à  
17 l'atteinte de ses objectifs de fiabilité. En effet, les normes CIP v5 améliorent la fiabilité du  
18 réseau de transport en permettant une meilleure protection des infrastructures essentielles  
19 à l'exploitation.

20 Le Coordonnateur demande à la Régie d'adopter les normes CIP v5 et leur Annexe  
21 respective ainsi que les modifications au Glossaire, et d'approuver les modifications au  
22 Registre des entités visées par les normes de fiabilité, dans leurs versions française et  
23 anglaise.

24 Conséquemment, le Coordonnateur demande également le retrait des normes CIP v1  
25 adoptées par la Régie, soit les normes CIP-002-1 à CIP-009-1.

26

**Annexe A**

**Ajout de nouveaux termes au Glossaire**

<b>Nouveaux termes français</b>	<b>Nouveaux termes anglais</b>
Accès distant interactif	Interactive Remote Access
Actif électronique BES	BES Cyber Asset
Actifs électroniques protégés	Protected Cyber Assets (PCA)
Cadre supérieur CIP	CIP Senior Manager
Centre de contrôle <sup>5</sup>	Control Center
Circonstance CIP exceptionnelle	CIP Exceptional Circumstance
Connectivité externe routable	External Routable Connectivity
Connectivité par lien commuté	Dial-up Connectivity
Incident de cybersécurité à déclarer	Reportable Cyber Security Incident
Information de système électronique BES	BES Cyber System Information
Point d'accès électronique	Electronic Access Point (EAP)
Système électronique BES	BES Cyber System
Système intermédiaire	Intermediate System
Système de contrôle des accès physiques	Physical Access Control Systems (PACS)
Systèmes de contrôle ou de surveillance des accès électroniques	Electronic Access Control or Monitoring Systems (EACMS)

---

<sup>5</sup> Cette nouvelle définition de la NERC remplacera la définition du Coordonnateur présentement au Glossaire.

**Modification des définitions des termes au Glossaire**

<b>Définition modifiée des termes (français)</b>	<b>Définition modifiée des termes (anglais)</b>
Actifs électroniques	Cyber Assets
Incident de cybersécurité	Cyber Security Incident
Périmètre de sécurité électronique	Electronic Security Perimeter (ESP)
Périmètre de sécurité physique	Physical Security Perimeter (PSP)

**Retrait des termes au Glossaire**

<b>Termes retirés (français)</b>	<b>Termes retirés (anglais)</b>
Actifs critiques	Critical Assets
Actifs électroniques critiques	Critical Cyber Assets