

D É C I S I O N

QUÉBEC

RÉGIE DE L'ÉNERGIE

D-2026-097	R-4335-2026	24 août 2026
------------	-------------	--------------

PRÉSENT :

Samy Gennaoui
Régisseur

Hydro-Québec
Demanderesse

Décision sur le fond

Demande d'adoption de la norme de fiabilité CIP-015-1

Demanderesse :

Hydro-Québec

représentée par M^e Pierre Chabot.

1 INTRODUCTION

[1] Le 24 avril 2026, Hydro-Québec, par sa direction principale – Contrôle des mouvements d'énergie et exploitation du réseau, désignée à titre de coordonnateur de la fiabilité au Québec (le Coordonnateur), dépose à la Régie de l'énergie (la Régie) une demande¹ visant l'adoption de la norme de fiabilité CIP-015-1 (la Norme) de la *North American Electric Reliability Corporation* (la NERC) ainsi que de son annexe Québec, dans ses versions française et anglaise².

[2] Le Coordonnateur demande également à la Régie de fixer la date d'entrée en vigueur de la Norme à adopter.

[3] Cette demande est présentée en vertu des articles 31 (5°), 85.2, 85.6 et 85.7 de la *Loi sur la Régie de l'énergie*³.

[4] Au soutien de sa demande, le Coordonnateur dépose la *Présentation de la demande*⁴, les *Informations relatives aux Normes*⁵, le *Sommaire des commentaires reçus à la suite de la consultation publique*⁶, la *Traduction française attestée des Normes*⁷, la Norme et son annexe Québec, en versions française et anglaise⁸. Le Coordonnateur dépose également, à titre informatif, le document de la NERC intitulé *Technical Rationale for Reliability Standard*, soit la *Justification technique* de la norme CIP-015-1, en versions française et anglaise⁹.

¹ Pièce [B-0002](#).

² Pièces [B-0008](#), [B-0009](#) et [B-0010](#).

³ [RLRQ, c. R-6.01](#).

⁴ Pièce [B-0004](#).

⁵ Pièce [B-0005](#).

⁶ Pièce [B-0006](#).

⁷ Pièce [B-0007](#).

⁸ Pièces [B-0008](#), [B-0009](#) et [B-0010](#).

⁹ Pièces [B-0011](#) et [B-0012](#).

[5] Le 11 mai 2026, la Régie publie sur son site internet un avis aux personnes intéressées¹⁰, dans lequel elle indique que cette demande sera traitée par voie de consultation avec des interventions formelles et invite toute personne intéressée à soumettre une demande d'intervention et un budget de participation, au plus tard le 21 mai 2026. Au terme de cette période, aucune entité visée n'a soumis de commentaire concernant la demande du Coordonnateur.

[6] Le 14 juillet 2026, la Régie transmet au Coordonnateur sa demande de renseignements n° 1 (DDR n° 1)¹¹, à laquelle ce dernier répond le 21 juillet 2026¹².

[7] Le 31 juillet 2026, la Régie transmet au Coordonnateur sa demande de renseignements n° 2 (DDR n° 2)¹³, à laquelle ce dernier répond le 7 août 2026¹⁴.

[8] Dans la présente décision, la Régie se prononce sur la demande du Coordonnateur comprenant la demande d'adoption de la Norme et de son annexe Québec ainsi que sur la date d'entrée en vigueur de la Norme et de son annexe Québec (la Demande).

2 MISE EN CONTEXTE DE LA DEMANDE

[9] La norme CIP-015-1 a été développée par la NERC afin d'assurer que les entités responsables exploitant des systèmes électriques critiques mettent en œuvre des mécanismes internes de détection, d'analyse et de neutralisation des communications réseau externes non sollicitées ou suspectes, et qu'elles développent des actions correctives afin de limiter les intrusions tout en protégeant la cybersécurité et la fiabilité du réseau en respectant les exigences spécifiées dans la Norme¹⁵. Cette norme de fiabilité porte sur la surveillance de sécurité interne du réseau pour les systèmes électroniques

¹⁰ Pièce [A-0003](#).

¹¹ Pièce [A-0005](#).

¹² Pièce [B-0015](#).

¹³ Pièce [A-0011](#).

¹⁴ Pièce [B-0023](#).

¹⁵ Pièce [B-0002](#), p. 2.

BES¹⁶ à impact élevé avec ou sans connectivité externe routable, ainsi que pour les systèmes à impact moyen disposant de connectivité externe routable¹⁷.

[10] La Demande a notamment pour objectif d'assurer une uniformité et une cohérence dans l'application de la pratique¹⁸.

[11] La Norme est issue du projet 2023-03 (*Cyber security – Internal Network Security Monitoring*) de la NERC et a été approuvée par la *Federal Energy Regulatory Commission* (FERC), le 26 juin 2025, dans sa lettre d'ordonnance RM24-7-000. La norme CIP-015-1 entrera en vigueur aux États-Unis le 1^{er} octobre 2028¹⁹.

3 CONCLUSION PRINCIPALE DE LA RÉGIE

[12] Pour les motifs énoncés ci-après, la Régie accueille la Demande du Coordonnateur.

4 DEMANDE D'ADOPTION DE LA NORME

4.1 OBJET ET APPLICABILITÉ

[13] Le Coordonnateur demande l'adoption de la Norme suivante :

- CIP-015-1 – Cybersécurité – Surveillance de sécurité de réseau interne.

¹⁶ BES : système de production-transport d'électricité.

¹⁷ Pièce [B-0005](#), p. 1.

¹⁸ Pièce [B-0004](#), p. 6 et 7.

¹⁹ Pièce [B-0004](#), p. 4.

[14] L'objet de la norme CIP-015-1 est d'améliorer la probabilité de détection d'activités réseau anormales ou non autorisées, afin de renforcer la capacité d'intervention et de rétablissement en cas d'attaque. Cette norme vise les responsables de l'équilibrage, les distributeurs, les exploitants d'installations de production, les propriétaires d'installations de production, les coordonnateurs de la fiabilité, les exploitants de réseaux de transport et les propriétaires d'installations de transport²⁰.

4.2 DISPOSITIONS PARTICULIÈRES POUR LE QUÉBEC

[15] Concernant le champ d'application, le Coordonnateur propose la disposition particulière suivante :

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 »²¹.

[16] Le Coordonnateur estime que cette disposition particulière est applicable, parce que le champ d'application équivalent au BES pour le Québec, reconnu par la Régie, est le RTP.

[17] En plus de cette disposition particulière, le Coordonnateur propose les exemptions additionnelles suivantes²² :

- 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;

²⁰ Pièce [B-0005](#), p. 1.

²¹ Pièce [B-0005](#), p. 2.

²² Pièce [B-0005](#), p. 2.

- Postes élévateurs des installations de production identifiées au point précédent.

[18] En réponse à la DDR n° 1 de la Régie, le Coordonnateur explique que cette exemption est fondée sur son évaluation selon laquelle ces installations ne présentent pas de risque significatif pour l'exploitation fiable de l'Interconnexion du Québec.

[19] Le Coordonnateur confirme que cette exemption est issue d'une décision réglementaire propre au Québec visant à soustraire explicitement certaines installations de production et leurs postes élévateurs à l'application des normes CIP²³.

[20] Il précise que la valeur de 300 MVA proposée en remplacement du seuil de 75 MVA utilisé par la NERC découle de l'évaluation réalisée par le Coordonnateur à l'égard des particularités de l'Interconnexion du Québec.

[21] De plus, il rappelle que cette évaluation a été reconnue par la Régie au paragraphe 70 de la décision D-2016-119²⁴, et qu'elle est fondée notamment sur les capacités du système de réglage fréquence-puissance (RFP), propre à l'Interconnexion du Québec.

[22] Questionné en DDR n° 2 sur le risque d'occurrence de cyberattaques simultanées visant la dégradation ou la perte de production de multiples centrales de 300 MVA ou moins, le Coordonnateur répond que ce risque est faible.

[23] Sans nier la possibilité de survenance d'un tel scénario, il soutient qu'un niveau particulièrement élevé de précision et de particularisation d'une hypothèse est généralement associé à un risque d'occurrence faible. Il explique que la mitigation de risque efficace contre les cyberattaques repose davantage sur l'analyse de scénarios englobants et représentatifs permettant de couvrir un éventail plus large de modes de défaillance plausibles, plutôt que sur l'analyse de scénarios hautement spécifiques.

²³ Pièce [B-0015](#), p. 6, R.3.1.

²⁴ Dossier R-3947-2015, décision [D-2016-119](#), p. 21, par. 70.

[24] Le Coordonnateur estime également que l'impact potentiel sur la fiabilité du RTP de ce scénario spécifique est faible. Le Coordonnateur explique que ses déductions reposent sur plusieurs facteurs cumulatifs, expliqués ci-après.

[25] Le Coordonnateur indique tout d'abord que les 34 centrales ciblées par l'élargissement de l'exemption à 300 MVA, générant une production d'environ 5149 MW de puissance installée totale, sont réparties sur plusieurs régions du Québec et sur différentes divisions du réseau de transport, exigeant ainsi une attaque compromettant simultanément des environnements technologiques hétérogènes²⁵.

[26] Ensuite, les centrales se classifient selon différents niveaux de cybersécurité, lesquels sont élaborés par des encadrements d'entreprise visant à déterminer leurs exigences distinctes. De plus, certaines centrales sont des installations mises en service avant la généralisation des architectures de cybersécurité modernes. Par conséquent, elles ne disposent pas d'accès à distance et nécessiteraient une intervention locale afin d'y déclencher une cyberattaque.

[27] Le Coordonnateur précise que les encadrements d'entreprise précédemment cités prévoient l'utilisation graduelle de systèmes de détection d'intrusion adaptés au niveau de criticité. Afin d'assurer leur diversification de cybersécurité, plusieurs de ces centrales disposent de systèmes de protection autonomes et un profil leur est attribué selon plusieurs autres variables, entre autres : leur position géographique, leur capacité de production et leur niveau de criticité.

[28] Enfin, l'impact sur la fiabilité du RTP est évalué comme faible selon les critères opérationnels de perte de production en première contingence (PPPC) et de rejet intempestif du RTPC (Rejet de la production et télédélestage de charge). À titre comparatif, aucune concentration régionale de ces installations ne permet d'atteindre un niveau de production comparable à la PPPC de 1000 MW.

[29] Le Coordonnateur soutient que des événements sévères de rejet intempestif du RTPC se rapprochant de la puissance totale de ces centrales indiquent que le réseau demeure stable dans la très grande majorité des scénarios. Les principaux enjeux de

²⁵ Pièce [B-0023](#), p. 1, R.1.1.

stabilité identifiés concernent plutôt des cas extrêmes associés à des secteurs stratégiques, dont l'importance découle du rôle de l'emplacement au sein des grands corridors de transport plutôt que de la perte de petites centrales dispersées.

4.3 DATES D'ENTRÉE EN VIGUEUR DE LA NORME

[30] Le plan de mise en œuvre du projet 2023-03 de la NERC propose une entrée en vigueur de la Norme le premier jour du premier trimestre civil à survenir 36 mois après l'approbation de la Norme.

[31] La Norme entrera en vigueur aux États-Unis le 1^{er} octobre 2028. Selon le Coordonnateur, ce délai respecte les critères établis par la Régie d'avoir une mise en vigueur le premier jour d'un trimestre civil et un délai minimal de 60 jours entre les dates d'adoption et d'entrée en vigueur d'une norme²⁶.

[32] Le Coordonnateur propose pour le Québec de reproduire le délai de mise en vigueur de la NERC, étant donné l'importance d'avoir des pratiques uniformes avec les normes obligatoires en vigueur et harmonisées avec les réseaux voisins²⁷.

[33] À cet effet, un échéancier de mise en conformité progressif s'applique. L'entité responsable qui possède des centres de contrôle et de relèvement identifiés conformément à l'exigence E1, alinéas 1.1 et 1.2 de la norme CIP-002-5.1a, doit se conformer à ce délai de 36 mois.

[34] Par ailleurs, toute entité responsable qui possède des systèmes électroniques RTP disposant de connectivité externe routable visés par la norme, à l'exception des centres de contrôle et des centres de contrôle de relèvement visés précédemment, dispose d'un délai additionnel pouvant aller jusqu'à 24 mois civils suivant la date d'entrée en vigueur de la Norme²⁸.

²⁶ Dossier R-3699-2009 Phase 2, décision [D-2016-011](#), p. 46, par. 193.

²⁷ Pièce [B-0005](#), p. 3.

²⁸ Pièce [B-0005](#), p. 3.

4.4 ÉVALUATION DE LA PERTINENCE DE LA NORME

[35] Les modifications apportées à la Norme découlent des recommandations du projet 2023-03 de la NERC. Le Coordonnateur est d'avis que la Norme repose sur l'amélioration des méthodes de détection des intrusions à l'intérieur même des réseaux opérationnels²⁹.

[36] De plus, le Coordonnateur mentionne que la Norme est pertinente car elle exige que les entités visées mettent en place un plan de surveillance de sécurité interne du réseau pour les systèmes électroniques RTP à impact élevé avec ou sans connectivité externe routable ainsi que pour les systèmes à impact moyen disposant de connectivité externe routable, afin de détecter les activités non autorisées au sein du périmètre informatique. Elle complète les contrôles périmétriques existants en permettant une meilleure visibilité des communications internes des réseaux opérationnels, là où une menace ayant franchi les défenses externes pourrait s'infiltrer³⁰.

[37] Le Coordonnateur est d'avis que la Norme soutient la fiabilité du réseau du Québec et l'harmonisation des pratiques avec celles des réseaux voisins.

4.5 ÉVALUATION DE L'IMPACT DE LA NORME

[38] De façon préliminaire, le Coordonnateur estime que l'impact pour l'implantation de la Norme est modéré, car celle-ci exige le déploiement de technologies de surveillance internes, impliquant l'ajout d'outils, de collecte et d'analyse de données, ainsi que des ajustements pouvant affecter temporairement les opérations³¹.

[39] En ce qui a trait à l'impact du maintien et du suivi de la Norme, le Coordonnateur l'estime comme étant faible, puisque l'intégration de la Norme s'inscrit dans un processus déjà établi par des mécanismes existants, notamment l'entretien des outils, la mise à jour des règles et la protection des données³².

²⁹ Pièce [B-0005](#), p. 4.

³⁰ Pièce [B-0004](#), p. 7.

³¹ Pièce [B-0004](#), p. 7.

³² Pièce [B-0004](#), p. 8.

[40] En réponse à la DDR n° 1 de la Régie, le Coordonnateur mentionne qu'il s'est basé sur la grille d'évaluation dans le sommaire qui définit un impact « modéré » comme un changement nécessitant la mobilisation de certaines ressources matérielles, humaines ou financières, sans toutefois exiger des investissements majeurs ou une transformation importante des pratiques existantes³³.

[41] De plus, le Coordonnateur est d'avis que les travaux requis pour l'implantation de la Norme concordent avec l'évaluation d'un impact modéré. La mise en œuvre nécessitera notamment le déploiement ou le renforcement de mécanismes de surveillance, l'ajout de capteurs et certaines adaptations des réseaux, afin d'assurer une surveillance adéquate des communications ainsi que la mise à jour de la documentation de conformité³⁴.

[42] Bien que ces activités représentent des efforts techniques et opérationnels non négligeables, le Coordonnateur maintient que leur ampleur est compatible avec l'estimation d'un impact modéré³⁵.

[43] En l'absence de commentaires formulés lors de la consultation publique, le Coordonnateur est d'avis que l'évaluation de l'impact présentée à l'étape préliminaire demeure inchangée³⁶.

4.6 CONSULTATION PUBLIQUE DES ENTITÉS VISÉES

[44] Le Coordonnateur soutient, en réponse à la DDR n° 1 de la Régie, que les entités visées sont informées de leur assujettissement potentiel à une nouvelle norme de fiabilité, par le biais du processus de consultation publique qu'il conduit.

[45] Il rappelle qu'un avis est publié sur son site Internet et transmis par courriel à toutes les entités inscrites au *Registre des entités visées par les normes de fiabilité* (le Registre). Les documents pertinents, incluant la norme proposée, les versions en suivi des

³³ Pièce [B-0015](#), p. 1 et 2, R. 1.1.

³⁴ Pièce [B-0015](#), p. 2 et 3, R. 1.2.

³⁵ Pièce [B-0015](#), p. 2 et 3, R. 1.2.

³⁶ Pièce [B-0005](#), p. 6.

modifications ainsi qu'un sommaire présentant notamment les fonctions visées par la norme sont mis à leur disposition. De ce fait, les entités ont l'occasion de commenter la norme proposée avant son dépôt à la Régie.

[46] Le Coordonnateur explique qu'à l'image des autres juridictions nord-américaines, où les entités enregistrées sont responsables de connaître les normes de fiabilité applicables aux fonctions pour lesquelles elles sont enregistrées, les entités inscrites au Registre au Québec doivent assurer une veille réglementaire, afin de suivre l'évolution des normes susceptibles de leur être applicables.

[47] Pour ce faire, les entités peuvent notamment s'appuyer sur les consultations publiques menées par le Coordonnateur, les avis, les dossiers et les décisions publiés par la Régie, ainsi que sur le séminaire annuel sur la fiabilité organisé par la Régie et la rencontre d'information annuelle du Coordonnateur, lesquels permettent de communiquer les développements réglementaires récents et les initiatives liées aux normes de fiabilité.

[48] Ainsi, selon le Coordonnateur, les entités disposent de plusieurs mécanismes leur permettant de prendre connaissance des nouvelles normes auxquelles elles pourraient être assujetties, ainsi que des obligations qui en découlent.

[49] Le Coordonnateur estime que les mécanismes de consultation et de communication actuellement en place offrent aux entités visées des occasions suffisantes de prendre connaissance des normes proposées et de faire valoir leurs préoccupations.

[50] En conclusion, l'absence de commentaires ne constitue pas, en soi, un indicateur que le processus de consultation doive être revu ou bonifié.

5 OPINION DE LA RÉGIE

[51] À la lumière des justifications fournies par le Coordonnateur, la Régie juge que la Norme est pertinente pour le Québec. De plus, elle note qu'aucune personne intéressée ne s'oppose à son adoption.

[52] En ce qui concerne la date de mise en vigueur de la Norme, le Coordonnateur propose d'établir une date d'entrée en vigueur de la Norme le premier jour du premier trimestre civil à survenir 36 mois suivant l'adoption de la Régie. La Régie est d'avis que cette proposition vise à fixer un délai d'implantation qui correspond à ceux accordés aux entités aux États-Unis, ce qui permet de respecter l'objectif d'harmonisation avec les réseaux voisins.

[53] En ce qui a trait au délai additionnel pouvant aller jusqu'à 24 mois civils suivant la date d'entrée en vigueur de la Norme pour toute entité responsable qui possède les systèmes électroniques RTP disposant de connectivité externe routable visés par la Norme, à l'exception des centres de contrôle et des centres de contrôle de relève, la Régie est d'avis que ce délai additionnel respecte les mêmes délais d'implantation que ceux accordés aux entités aux États-Unis.

[54] Au sujet des dispositions particulières, la Régie est satisfaite des explications additionnelles fournies en réponse à ses DDR, plus spécifiquement à l'égard de sa décision D-2016-119, dans laquelle la Régie retient une exemption pour certaines entités, au seuil précis de 300 MVA.

[55] La Régie comprend qu'une évaluation du Coordonnateur, soumise dans le cadre du dossier R-3947-2015, lui avait permis de conclure que les installations de production de 300 MVA ou moins, à l'exception de celles pouvant être synchronisées avec un réseau voisin, ne présentaient pas de risque significatif pour l'exploitation fiable de l'Interconnexion du Québec.

[56] La Régie estime cependant que, bien que certains principes généraux relatifs au régime de fiabilité soient établis au fil des décisions qu'elle rend, il revient au Coordonnateur de rendre sa preuve complète. Il doit, notamment, citer explicitement la décision ou le principe qui explique ou soutient une disposition particulière qu'il soumet,

particulièrement dans le contexte de l'adoption d'une nouvelle norme, et ce, même s'il s'appuie sur une justification « historique ».

[57] Par ailleurs, la Régie comprend que le Coordonnateur a estimé faibles le risque et l'impact de cyberattaques simultanées visant de multiples centrales de 300 MVA ou moins sur la fiabilité du RTP, en considérant un contexte de cumulation de certains facteurs précis.

[58] Il s'agit notamment de la répartition géographique des centrales ciblées, de leur classification et de leurs architectures spécifiques de cybersécurité, et des critères opérationnels de PPPC et de rejet intempestif du RPTC.

[59] La Régie rappelle que dans le contexte de transition énergétique au Québec, le réseau électrique est appelé à évoluer et à se transformer. Par exemple, cette évolution pourrait entraîner une augmentation du nombre de centrales de plus faible puissance et en impacter la répartition géographique. Cette évolution pourrait également modifier l'impact d'une perte de production sur la fiabilité du réseau, dans certaines circonstances.

[60] Dans cet environnement évolutif, la Régie juge important de s'assurer que les principes établis demeurent valables et adaptés à l'Interconnexion du Québec, alors que la configuration du réseau est modifiée, que les architectures de cybersécurité sont modernisées et que de nouvelles normes de fiabilité sont proposées pour adoption.

[61] La Régie comprend que les facteurs précis considérés par le Coordonnateur pourraient, dans ce contexte, évoluer eux aussi. **La Régie demande par conséquent que le seuil spécifique de 300 MVA soit réévalué et que sa pertinence soit démontrée ou confirmée chaque fois que l'exemption y faisant référence sera proposée, soit lors d'un dossier d'adoption d'une nouvelle norme ou d'une version subséquente d'une précédente norme en vigueur au Québec.**

[62] La Régie note par ailleurs que l'impact de la Norme est modéré en ce qui concerne son implantation, et faible en ce qui concerne son maintien et son suivi. La Régie retient que cette Norme exige le déploiement de technologies de surveillance interne, impliquant l'ajout d'outils, de collecte et d'analyse de données, ainsi que des ajustements pouvant affecter temporairement les opérations.

[63] De plus, en réponse à la DDR n° 1, le Coordonnateur mentionne que les entités ont à leur disposition suffisamment de mécanismes de consultation et de communication pour être informées de leurs obligations en vertu du régime de fiabilité, notamment par les consultations publiques menées par le Coordonnateur, les avis diffusés, les décisions publiées par la Régie, le séminaire annuel sur la fiabilité organisée par la Régie et enfin à la rencontre d'information annuelle du Coordonnateur. La Régie est satisfaite des explications du Coordonnateur quant au mécanisme de consultation et de communication utilisé auprès des entités visées dans le cadre du présent dossier.

[64] Finalement, la Régie se déclare satisfaite du niveau de concordance des textes français et anglais aux fins de la présente décision. À cet égard, elle retient que la version française de la Norme a été attestée par un traducteur agréé.

[65] **Considérant ce qui précède, la Régie :**

- **Adopte la norme CIP-015-1 ainsi que son annexe Québec, dans ses versions française et anglaise;**
- **Fixe la date d'entrée en vigueur de la norme CIP-015-1 et son annexe Québec, dans ses versions française et anglaise, au 1^{er} octobre 2029 pour les entités responsables qui possèdent des centres de contrôle et de relève identifiés conformément à l'exigence E1, alinéas 1.1 et 1.2 de la CIP-002-5.1a;**
- **Fixe la date d'entrée en vigueur de la norme CIP-015-1 et son annexe Québec, dans ses versions française et anglaise, au 1^{er} octobre 2031 pour les entités responsables qui possèdent les systèmes électroniques RTP disposant de connectivité externe routable, à l'exception des centres de contrôle et des centres de contrôle de relève visés précédemment.**

[66] **Pour ces motifs,**

La Régie de l'énergie :

ACCUEILLE la Demande du Coordonnateur;

ADOpte la norme de fiabilité CIP-015-1 et son annexe Québec, dans ses versions française et anglaise;

FIXE la date d'entrée en vigueur de la norme de fiabilité CIP-015-1 et son annexe Québec, dans ses versions française et anglaise, **au 1^{er} octobre 2029** pour les entités responsables qui possèdent des centres de contrôle et de relèvement identifiés conformément à l'exigence E1, alinéas 1.1 et 1.2 de la CIP-002-5.1a;

FIXE la date d'entrée en vigueur de la norme de fiabilité CIP-015-1 et son annexe Québec, dans ses versions française et anglaise, **au 1^{er} octobre 2031** pour les entités responsables qui possèdent les systèmes électroniques RTP disposant de connectivité externe routable, à l'exception des centres de contrôle et des centres de contrôle de relèvement visés précédemment;

FIXE au **31 août 2026** la date de dépôt de la norme de fiabilité CIP-015-1 et de son annexe Québec, dans ses versions française et anglaise, adoptées et mises en vigueur dans la présente décision et modifiées afin d'y indiquer leurs dates d'adoption et d'entrée en vigueur, selon les ordonnances contenues à la présente décision, et en y ajoutant la référence à la présente décision à la section « Historique des versions »;

ORDONNE au Coordonnateur de se conformer à tous les éléments décisionnels contenus dans la présente décision.

Samy Gennaoui

Régisseur