Information relative à la norme

Projet QC-2026-01

Norme *CIP-015-01 – Cybersécurité – Surveillance de sécurité de réseau interne*

1.1. Applicabilité de la norme

Les fonctions visées par la norme proposée pour adoption, soit la *norme de fiabilité* CIP-015-1, sont indiquées dans le tableau ci-dessous.

Norme	Fonctions visées
CIP-015-1	*Responsable de l'équilibrage (BA)* *Distributeur (DP)* *Exploitant d'installation de production (GOP)* *Propriétaire d'installation de production (GO)* *Coordonnateur de la fiabilité (RC)* *Exploitant de réseau de transport (TOP)* *Propriétaire d'installation de transport (TO)*

1.2. Objet de la norme

La présente section a pour objectif de présenter l'objet de la norme visée par la présente demande. Plus spécifiquement, le prochain point présente le titre puis l'objet de la norme.

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

1.3. Contexte réglementaire

À la suite de l'Ordonnance 887[1] de la *Federal Energy Regulatory Commission* (ci-après, la « FERC ») dans le dossier n° RM22-3-000 émise le 19 janvier 2023, la NERC a reçu l'ordonnance de développer une norme de fiabilité portant sur la surveillance de sécurité interne du réseau pour les *systèmes électroniques BES* à impact élevé avec ou sans *connectivité externe routable* ainsi que pour les systèmes à impact moyen disposant de *connectivité externe routable*. La NERC a donc dû combler cette lacune en matière de fiabilité afin d'améliorer les capacités de détection des mouvements latéraux par des acteurs malveillants.

La *norme de fiabilité* CIP-015-1 a été adoptée par le conseil d'administration de la NERC le 9 mai 2024. La NERC a ensuite déposé une requête auprès de la FERC le 24 juin 2024 demandant l'approbation de la nouvelle *norme de fiabilité*. Elle a ensuite été approuvée par la FERC le 26 juin 2025 dans le cadre de l'Ordonnance 907[2], confirmant son intégration aux normes de fiabilité américaines.

[1] Ordonnance 887 de la FERC, consultée le 17 mars 2026 au https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20230119-3085&optimized=false (en anglais seulement).
[2] Ordonnance 907 de la FERC, consultée le 17 mars 2026 au https://elibrary.ferc.gov/eLibrary/filelist?accession_num=20250626-3039 (en anglais seulement).

La *norme de fiabilité* CIP-015-1[3], élaborée dans le cadre du projet 2023-03[4] de la NERC, s'inscrit dans l'évolution du cadre réglementaire nord-américain visant la protection du *système de production-transport d'électricité* (*BES*). L'objectif de la *norme de fiabilité* CIP-015-1 est donc d'imposer la mise en place de mécanismes de surveillance continue des flux internes, la détection et l'évaluation d'activités anormales, la conservation et la protection des données de surveillance nécessaires pour soutenir une réponse appropriée aux incidents de cybersécurité. L'implémentation du projet 2023-03 marque ainsi un changement important en complétant les contrôles périmétriques existants par une capacité structurée de détection et d'analyse à l'intérieur même des environnements critiques exploités par les transporteurs, producteurs, coordonnateurs de fiabilité et autres entités responsables du *BES*.

Le Coordonnateur de la fiabilité au Québec (ci-après, le « Coordonnateur ») dépose au présent dossier le premier dépôt réglementaire de la norme CIP-015-1 du projet 2023-03 auprès de la Régie de l'énergie (ci-après, la « Régie »). L'Ordonnance 907 de la FERC précise une deuxième version de la norme CIP-015 visant à étendre l'obligation de surveillance interne des réseaux aux *systèmes de contrôle de surveillance des accès électronique* (*EACMS*) et des *systèmes de contrôle des accès physiques* (*PACS*) situés à l'extérieur du *périmètre de sécurité électronique*, tout en précisant que seuls les flux de communication entre actifs CIP sont visés. Cette deuxième version sera traitée dans un dossier réglementaire ultérieur.

1.4. Dispositions particulières pour le Québec

La première disposition particulière ci-dessous concerne le champ d'application de la norme et se lit ainsi :

> « 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* ».

Cette disposition particulière, préalablement sous la sous-section 4.2 intitulée « Installations » des annexes, est désormais sous la section 4 intitulée « Applicabilité ». L'emplacement de cette disposition particulière a été modifiée sans toutefois y modifier son contenu afin de refléter sa portée sur l'ensemble de la norme. Les installations exemptées figurent maintenant sous le paragraphe intitulé « Exemptions additionnelles ».

Le Coordonnateur est d'avis que cette disposition particulière est applicable, puisque le champ d'application équivalent au *BES* pour le Québec et reconnu par la Régie est le *RTP*.

De plus, le Coordonnateur propose les exemptions additionnelles suivantes :

- 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.

[3] *Norme de fiabilité* CIP-015-1 par la NERC, consultée le 17 mars 2026 au 2023-03-cip-015-1-fb-clean.pdf (en anglais seulement)
[4] Projet 2023-03 de la NERC, consulté le 17 mars 2026 au 2023-03 Internal Network Security Monitoring (INSM) (en anglais seulement)

1.5. Dates d'entrée en vigueur proposées

Le plan de mise en œuvre de la norme CIP-015-1 propose une entrée en vigueur de la *norme de fiabilité* au premier jour du premier trimestre civil à survenir 36 mois après l'approbation de l'organisme réglementaire de la norme. Aux États-Unis, la norme CIP-015-1 entrera en vigueur le 1er octobre 2028[5]. À compter de cette date, un échéancier de mise en conformité progressif s'applique. L'entité responsable 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 doivent se conformer dans ce délai de 36 mois, tandis que toute entité responsable qui possède les *systèmes électroniques BES* disposant de *connectivité externe routable*, à l'exception des centres de contrôle et des centres de contrôle de relève visés précédemment, dispose d'un délai additionnel pouvant aller jusqu'à 24 mois civil suivant la date d'entrée en vigueur de la norme CIP-015-1.

Cette approche graduelle reconnaît la complexité technique et organisationnelle associée à l'implantation de solutions de surveillance interne, incluant la collecte et l'analyse structurée des données réseau, l'ajustement des architectures existantes et la formation du personnel.

Le Coordonnateur considère que les critères établis par la Régie d'avoir une mise en vigueur le premier jour d'un trimestre civil[6] et un délai minimal de soixante (60) jours[7] entre la date d'adoption et l'entrée en vigueur d'une norme sont respectés dans le cadre du plan de mise en œuvre de la NERC.

Étant donné l'importance d'avoir des pratiques uniformes avec des normes obligatoires en vigueur harmonisées avec les États-Unis, le Coordonnateur propose une entrée en vigueur le premier jour du premier trimestre civil à survenir trente-six (36) mois après l'adoption de la *norme de fiabilité* par la Régie Pour certains *systèmes électroniques BES* disposant de *connectivité externe routable* de la norme CIP-015-1, le Coordonnateur propose les mêmes délais d'implantation accordés aux entités aux États-Unis.

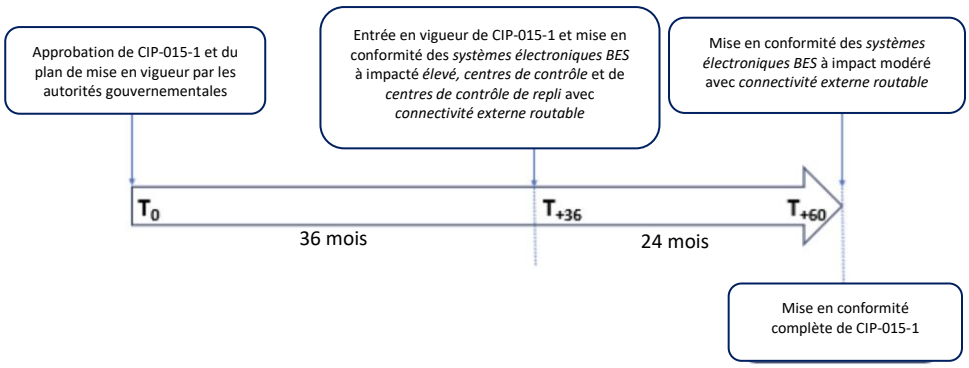

Figure 1. Schématisation chronologique du plan de mise en vigueur de la NERC pour la *norme de fiabilité* CIP-015-1.[8]

[5] Normes sujettes à une entrée en vigueur future sur le site de la NERC, consultées le 17 mars 2026 au https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx (en anglais seulement).
[6] Par sa décision D-2015-168, la Régie fixe l'entrée en vigueur des normes au 1er jour des trimestres civils suivant la date d'adoption.
[7] Par sa décision D-2016-011, la Régie fixe à soixante (60) jours le délai minimal à prévoir entre la date d'adoption et celle d'entrée en vigueur des normes à venir.
[8] Schématisation chronologique du plan de mise en vigueur de la NERC du projet 2023-03 (p.3/3), consulté le 17 mars 2026: https://www.nerc.com/globalassets/standards/projects/2023-03/2023-03-implementation-plan-fb-clean.pdf (en anglais seulement).

1.6. Norme à retirer

Aucune norme à retirer.

1.7. Modifications au Glossaire

Aucune modification au Glossaire.

2. ÉVALUATION DE LA PERTINENCE

La norme CIP-015-1 vise à inclure des politiques stipulant que les entités visées mettent en place un plan de surveillance de sécurité interne du réseau pour les *systèmes électroniques BES* 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 impose notamment la détection et l'évaluation des anomalies, la conservation des données de surveillance et la protection de l'intégrité de ces données**,** facilitant ainsi les enquêtes potentielles et la gestion des incidents. Pour ce faire, la *norme de fiabilité* CIP-015-1 contient trois exigences principales. L'exigence E1 oblige les entités responsables à mettre en œuvre des processus documentés pour surveiller, détecter et évaluer toute activité anormale ou non autorisée au sein du *périmètre de sécurité électronique* (PSE) des systèmes informatiques du *RTP*. L'exigence E2 stipule la conservation des données de surveillance pendant une durée minimale spécifiée afin de soutenir les enquêtes et la vérification de la conformité. Finalement, l'exigence E3 impose une protection des données de surveillance contre toute modification ou suppression non-autorisée. Afin de répondre aux exigences, toutes les entités responsables concernées auront potentiellement à acquérir des capteurs pour faciliter la collecte de données réseau des réseaux applicables, à apporter des modifications aux réseaux afin de mieux les aligner avec la *norme de fiabilité* CIP-015-1.

La NERC est d'avis que la norme proposée pour adoption est raisonnable, n'est pas discriminatoire, ne procure pas d'avantages indus et est dans l'intérêt du public[9]. La FERC a conclu dans l'Ordonnance 907[10] que les motivations de la NERC sont appuyées sur le fait que la nouvelle *norme de fiabilité* permet d'améliorer la cybersécurité du *BES* en exigeant que les entités visées mettent en œuvre des mécanismes de surveillance de sécurité interne des réseaux afin d'assurer la détection d'activités réseau anormales indicatives d'une attaque en cours.

De plus, la Commission de l'énergie et des services publics du Nouveau-Brunswick a approuvé la norme CIP-015-1-NB-0 le 31 octobre 2025 dans le projet n^{o} ER-004-2025[11], et prévoit une mise en vigueur le 1er janvier 2029. En Ontario, la date d'approbation du projet de la norme demeure à être déterminée par la Commission de l'énergie de l'Ontario[12].

La pertinence de la *norme de fiabilité* CIP-015-1 repose sur l'amélioration des méthodes de détection des intrusions à l'intérieur même des réseaux opérationnels. Les infrastructures de transport reposent sur de nombreux systèmes cybernétiques, notamment les systèmes SCADA, les centres de contrôle, les relais de protection numériques et les équipements de télécommunication. Bien que ces systèmes soient

[9] Avis de la NERC (p.1), consulté le 17 mars 2026 au https://www.nerc.com/globalassets/who-we-are/membership/legal--regulatory/ca/filings--orders/qb-notice-of-filing-of-cip-015-insm_packaged.pdf (en anglais seulement)
[10] Ordonnance 907 de la FERC, consultée le 17 mars 2026 au https://elibrary.ferc.gov/eLibrary/filelist?accession_num=20250626-3039 (en anglais seulement).
[11] Instance n^{o} 555 au Nouveau-Brunswick, consultée le 17 mars 2026 au https://filemaker.nbeub.ca/fmi/webd/NBEUB%20ToolKit13
[12] Processus de révision de la Commission de l'énergie de l'Ontario, consulté le 17 mars 2026 au https://www.ieso.ca/en/Sector-Participants/System-Reliability/OEB-Review-Process (en anglais seulement).

généralement protégés par des contrôles périmétriques imposés par les normes CIP existantes, une attaque réussie pourrait permettre à une entité menaçante de se déplacer à l'intérieur du réseau interne. Pour les entités visées, l'application de cette norme pourrait donc se traduire par l'implantation ou le renforcement de technologies de surveillance du trafic réseau industriel, d'analyses comportementales et de collecte de données des environnements contenant des systèmes cybernétiques critiques. Ces mesures amélioreraient la visibilité des communications internes du réseau et permettraient une détection plus rapide des incidents de cybersécurité**,** réduisant ainsi les risques sur le *réseau de transport principal* (RTP).

Considérant les éléments mentionnés ci-haut concernant la *norme de fiabilité* CIP-015-1 et en considérant que cette norme a été élaborée par des organismes reconnus en Amérique du Nord, y compris au Québec et chez les juridictions voisines, et ce, conformément à l'entente conclue en 2009 entre la Régie, la NERC et le NPCC avec l'autorisation du gouvernement du Québec[13], le Coordonnateur est d'avis que la norme CIP-015-1 contribue à la fiabilité du *réseau* du Québec et à l'harmonisation avec les *réseaux* voisins.

3. ÉVALUATION PRÉLIMINAIRE DE L'IMPACT

Cette section présente l'évaluation préliminaire de l'impact sur l'ensemble des entités du Québec selon le *coordonnateur de la fiabilité*.

L'impact préliminaire découlant de l'implantation de la norme de fiabilité CIP-015-1 au Québec peut être qualifié de modéré, compte tenu du fait que la norme exige que les entités visées déploient des technologies de surveillance de sécurité du réseau interne capable de détecter une activité anormale au sein du *périmètre de sécurité électronique* (ESP) des systèmes *RTP* à impact élevé avec ou sans *connectivité externe routable* et des systèmes à impact moyen disposant d'une connectivité externe routable. Cela nécessitera des outils de surveillance, de la collecte de données et des processus d'analyse du trafic interne, ce qui pourrait nécessiter des interruptions des installations opérationnelles et/ou de mettre en œuvre des capacités pour ingérer de grandes quantités d'informations réseau et effectuer l'analyse nécessaire.

Comme plusieurs autres mesures de cybersécurité CIP sont déjà en place et sont responsables de nombreux contrôles de cybersécurité fondamentaux, l'introduction de surveillance des réseaux internes au sein des zones de confiance nécessite des modifications supplémentaires à l'architecture, y compris des capteurs additionnels, des systèmes de conservation et des processus de détection d'anomalies. Ces déploiements peuvent nécessiter une intégration technique entre les réseaux opérationnels. En conséquence, le risque de mise en œuvre est modéré, car de nouvelles technologies doivent être intégrées dans les systèmes de contrôle existants sans perturber les opérations du réseau.

L'impact du maintien de la nouvelle infrastructure peut être considéré comme faible puisqu'une fois l'infrastructure de surveillance déployée, les entités responsables ne doivent qu'assurer le maintien des capteurs associés, la mise à jour des règles de détection, ainsi que la conservation des données de surveillance et leur protection contre toute modification non autorisée. Ces exigences supplémentaires de maintien sont en partie atténuées par la présence de mécanismes de gouvernance en cybersécurité déjà établis dans le cadre du programme de protection des infrastructures critiques. Les entités sont déjà tenues de maintenir des processus de gestion de la cybersécurité, des programmes de formation du

[13] Entente conclue conformément au décret n° 443-2009 publié le 8 avril 2009. http://www.regie-energie.qc.ca/audiences/normes_fiab_tranp_elec/Entente_Regie_NERC_NPCC_5mai09.pdf

personnel ainsi que de la documentation des systèmes, conformément à des normes telles les *normes de fiabilité* CIP-003 et CIP-004.

Finalement, l'impact associé au suivi et à la surveillance réglementaire liés à la mise en vigueur de la norme CIP-015-1 est faible. Dans ce contexte, le coordonnateur de la fiabilité au Québec assure la consultation des parties prenantes de l'industrie et soumet les normes proposées à la Régie de l'énergie pour adoption avant leur mise en application. Étant donné que ce mécanisme est déjà en place pour l'intégration réglementaire, l'introduction de la CIP-015-1, ainsi que de sa version subséquente CIP-015-2, devrait demeurer essentiellement procédurale.

Le tableau suivant présente des estimations préliminaires des impacts sur l'ensemble des entités du Québec.

	Impacts		
Norme	**Implantation**	**Maintien**	**Suivi**
CIP-015-1	Modéré	Faible	Faible

Légende :

Faible : Pratique normale de l'industrie ou norme n'entraînant que des ajustements mineurs aux processus ou aux pratiques en place.

Modéré : Changement qui nécessite de mobiliser certaines ressources matérielles, humaines ou financières pour implanter la norme proposée, la maintenir ou assurer le suivi de la conformité.

Important : Changement qui nécessite de prévoir et de mobiliser d'importantes ressources matérielles, humaines ou financières pour planifier et implanter la norme proposée, la maintenir ou assurer le suivi de la conformité.

4. ÉVALUATION FINALE DE L'IMPACT

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 inchangée.