A. Introduction

1. Titre : Cybersécurité — Catégorisation des systèmes électroniques BES

2. Numéro : CIP-002-5.1

3. Objet : Inventorier et catégoriser les *systèmes électroniques BES* et leurs *actifs électroniques BES* connexes, pour l'application des exigences de cybersécurité proportionnelle à l'impact négatif que la perte, la dégradation ou la mauvaise utilisation de ces *systèmes électroniques BES* pourrait avoir sur l'exploitation fiable du BES. L'inventaire et la catégorisation des *systèmes électroniques BES* permettent d'établir une protection appropriée contre les dégradations qui pourraient entraîner un fonctionnement incorrect ou une instabilité du BES.

4. Applicabilité :

4.1. Entités fonctionnelles : Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

4.1.1. Responsable de l'équilibrage

4.1.2. Distributeur qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du BES :

4.1.2.1. Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :

4.1.2.1.1. fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.1.2.1.2. effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.1.2.2. Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.3. Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.4. Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.1.3. Exploitant d'installation de production

4.1.4. Propriétaire d'installation de production

4.1.5. Coordonnateur des échanges ou Responsable des échanges

4.1.6. Coordonnateur de la fiabilité

4.1.7. Exploitant de réseau de transport

4.1.8. Propriétaire d'installation de transport

4.2. Installations : Dans le contexte des exigences de la présente norme, les *installations*, systèmes et équipements suivants détenus par chaque entité responsable indiquée à la section 4.1 sont ceux auxquels ces exigences sont applicables. Dans le cas des exigences de cette norme qui visent un type particulier d'*installations*, de système ou d'équipements, ou un sous-ensemble d'*installations*, de systèmes ou d'équipements, ceux-ci sont précisés explicitement.

4.2.1. Distributeur : Un ou plusieurs des *installations*, systèmes et équipements suivants détenus par le distributeur pour la protection ou la remise en charge du BES :

4.2.1.1. Chaque système de DSF ou de DST qui :

4.2.1.1.1. fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.2.1.1.2. effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.2.1.2. Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.3. Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.4. Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.2.2. Entités responsables indiquées en 4.1, sauf les distributeurs :
Toutes les *installations* du BES.

4.2.3. Exemptions : Sont exemptés de la norme CIP-002-5 :

4.2.3.1. Les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire

4.2.3.2. les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électroniques* distincts ;

4.2.3.3. les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme à la norme CFR 10, section 73.54 ;

4.2.3.4. dans le cas des *distributeurs*, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus.

5. Dates d'entrée en vigueur :

1. **24 mois minimum**– La norme CIP-002-5.1 entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.

2. Dans les juridictions où aucune approbation réglementaire n'est requise, la norme CIP-002-5.1 entrera en vigueur le premier jour du neuvième trimestre civil suivant l'approbation par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte :

La présente norme fournit des critères précis pour que les entités responsables visées catégorisent leurs *systèmes électroniques BES* en se basant sur l'impact de leurs *installations*, systèmes et équipements qui y sont associés, lesquels, s'ils étaient détruits, endommagés, mal utilisés ou autrement rendus indisponibles, affecteraient l'exploitation fiable du *système de production-transport d'électricité*. La démarche de cette norme est basée sur plusieurs concepts.

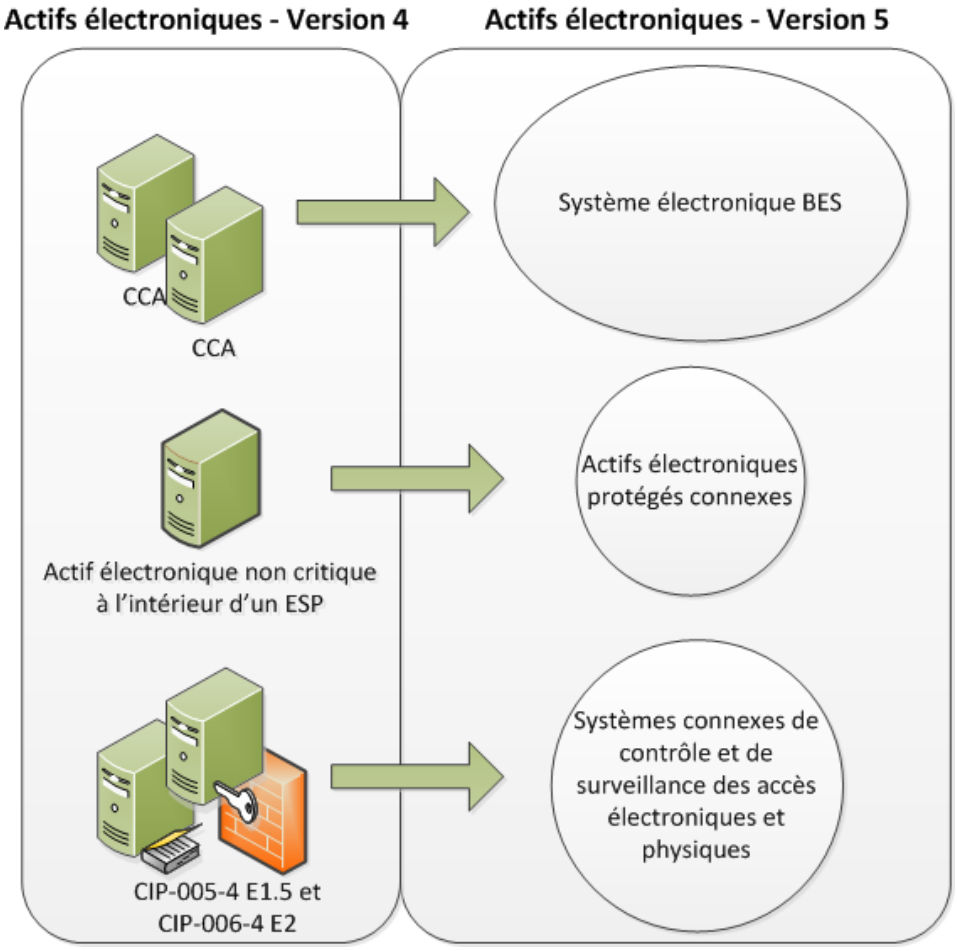
Dans l'ensemble des normes, sauf indication particulière, les éléments présentés sous forme de liste à puces dans les exigences sont des éléments liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

Plusieurs références de la section Applicabilité et les critères de l'annexe 1 de la norme CIP-002 utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST provient de la version 1 des normes CIP sur la cybersécurité. Ce seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances de systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes de DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de

seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

Systèmes électroniques BES

Une des différences fondamentales entre les versions 4 et 5 des normes CIP sur la cybersécurité est le passage de l'identification des *actifs électroniques critiques* vers l'identification des *systèmes électroniques BES*. Ce changement résulte de l'examen du cadre de gestion du risque du NIST par l'équipe de rédaction et de l'utilisation d'un terme analogue, « système d'information », comme cible pour la catégorisation et l'application des mesures de sécurité.



Dans la transition de la version 4 vers la version 5, un *système électronique BES* peut être simplement considéré comme un regroupement d'*actifs électroniques critiques* (tel que ce terme est utilisé dans la version 4). Les normes CIP sur la cybersécurité utilisent le terme « *système électronique BES* » essentiellement pour fournir un niveau plus élevé pour référer à l'objet d'une exigence. Par exemple, il devient possible d'appliquer des exigences concernant le rétablissement et la protection contre les maliciels à un regroupement plutôt qu'à des *actifs électroniques* individuels, et il

devient plus clair dans l'exigence que la protection contre les maliciels s'applique au système dans son ensemble et que la conformité individuelle de chaque dispositif peut ne pas être nécessaire.

Une autre raison d'utiliser le terme « *système électronique BES* » est de fournir un niveau pratique auquel une entité responsable peut organiser la mise en œuvre documentée des exigences et des pièces justificatives de conformité. Les entités responsables peuvent utiliser le concept bien développé de plan de sécurité pour chaque *système électronique BES* afin de documenter les programmes, processus et plans en place visant à se conformer aux exigences de sécurité.

Il est laissé à la discrétion de l'entité responsable de déterminer le niveau de granularité pour délimiter un *système électronique BES*, compte tenu des conditions de la définition de *système électronique BES*. Par exemple, l'entité responsable pourrait choisir de considérer l'ensemble d'un système de commande de centrale comme un seul *système électronique BES*, ou choisir de considérer certaines parties de ce système comme des *systèmes électroniques BES* distincts. L'entité responsable devrait prendre en considération le contexte opérationnel et le cadre de gestion lorsqu'elle définit les limites d'un *système électronique BES*, de manière à maximiser l'efficience de son fonctionnement sécurisé. Définir des limites trop étroites pourrait entraîner des redondances dans les processus administratifs et les autorisations, tandis que définir des limites trop larges pourrait rendre le fonctionnement sécurisé du *système électronique BES* difficile à surveiller et à évaluer.

Exploitation fiable du BES

La portée d'application des normes CIP sur la cybersécurité est limitée aux *systèmes électroniques BES* qui auraient un impact sur l'exploitation fiable du BES. Afin d'identifier les *systèmes électroniques BES*, les entités responsables déterminent si le *système électronique BES* effectue ou soutient une des fonctions de fiabilité du BES selon les tâches de fiabilité associées à leur fonction de fiabilité et par les responsabilités correspondantes de l'entité fonctionnelle telles que définies par ses relations avec les autres entités fonctionnelles dans le modèle fonctionnel de la NERC. Cela fait en sorte que la portée d'application initiale inclut seulement les *systèmes électroniques BES* et leurs *actifs électroniques BES* connexes qui effectuent ou soutiennent l'exploitation fiable du BES. La définition du terme « *actif électronique BES* » fournit la base de cette portée d'application.

Exploitation en temps réel

Une caractéristique de l'*actif électronique BES* est sa portée temps réel. L'horizon temporel qui est significatif pour les *systèmes électroniques BES* et les *actifs électroniques BES* visés par l'application de la version 5 des normes CIP sur la cybersécurité est défini comme étant celui qui est important pour l'exploitation fiable en temps réel du BES. Pour décrire l'horizon temporel de façon plus précise qu'au moyen de l'expression « *temps réel* », les *actifs électroniques BES* sont des *actifs électroniques* qui, s'ils étaient rendus indisponibles, endommagés ou mal utilisés,

auraient un impact négatif sur le fonctionnement fiable du BES dans les 15 minutes de l'activation ou de la mise en œuvre de la solution de rechange. Cette fenêtre de temps ne doit pas tenir compte ici de l'activation d'*actifs électroniques BES* ou de *systèmes électroniques BES* redondants : au point de vue de la cybersécurité, la redondance n'atténue pas les vulnérabilités de cybersécurité.

Critères de catégorisation

Les critères énoncés à l'annexe 1 servent à catégoriser les *systèmes électroniques BES* en catégories d'impact. L'exigence E1 demande de dresser la liste des *systèmes électroniques BES* classés dans les catégories Impact élevé et Impact moyen seulement. Tous les *systèmes électroniques BES* d'*installations* auxquelles ne s'appliquent pas les critères de catégorisation 1.1 à 1.4 et 2.1 à 2.11 de l'annexe 1 – Critères d'évaluation de l'impact tombent par défaut dans la catégorie Impact faible.

Ce processus général de catégorisation des *systèmes électroniques BES* en fonction de l'impact sur l'exploitation fiable du BES est cohérent avec l'approche de gestion du risque aux fins de l'application des exigences de cybersécurité dans le reste des normes CIP sur la cybersécurité version 5.

Systèmes de contrôle ou de surveillance des accès électroniques, systèmes de contrôle des accès physiques et actifs électroniques protégés associés aux systèmes électroniques BES

Les *systèmes électroniques BES* comportent des *actifs électroniques* associés qui, s'ils sont compromis, présentent une menace pour le *système électronique BES* en raison : a) de leur emplacement à l'intérieur du *périmètre de sécurité électronique* (*actifs électroniques protégés*), ou b) de la fonction de contrôle de sécurité qu'ils remplissent (*systèmes de contrôle ou de surveillance des accès électroniques* et *systèmes de contrôle des accès physiques*). Ces *actifs électroniques* comprennent :

Systèmes de contrôle ou de surveillance des accès électroniques (EACMS) – Exemples : *points d'accès électroniques*, *systèmes intermédiaires*, serveurs d'authentification (serveurs Radius, serveurs Active Directory, autorités de certification, etc.), systèmes de surveillance des événements de sécurité et systèmes de détection des intrusions.

Systèmes de contrôle des accès physiques (PACS) – Exemples : serveurs d'authentification et systèmes d'accès à carte ou à porte-nom.

Actifs électroniques protégés (PCA) – Exemples, dans la mesure où ils se trouvent à l'intérieur de l'ESP : serveurs de fichiers, serveurs FTP, serveurs de temps, commutateurs LAN, imprimantes réseau, enregistreurs numériques de défauts et systèmes de surveillance des émissions.

B. Exigences et mesures

E1. Chaque entité responsable doit mettre en œuvre un processus qui considère chacun des actifs suivants aux fins des alinéas 1.1 à 1.3 : *[Facteur de risque de la non-conformité : élevé] [Horizon : planification de l'exploitation]*

- **i.** *centres de contrôle* et *centres de contrôle* de repli ;
- **ii.** postes de transport ;
- **iii.** ressources de production ;
- **iv.** systèmes et installations essentiels à la remise en charge du réseau, y compris les *ressources à démarrage autonome* et les *chemins de démarrage* ainsi que les exigences relatives aux manœuvres initiales ;
- **v.** *automatismes de réseau* qui contribuent à la fiabilité du *système de production-transport d'électricité* ; et
- **vi.** pour les *distributeurs*, *systèmes de protection* indiqués à l'alinéa 4.2.1 de la section Applicabilité ci-dessus.

1.1. identifier chacun des *systèmes électroniques BES* à impact élevé, selon la section 1 de l'annexe 1, s'il y en a, pour chaque actif ;

1.2. identifier chacun des *systèmes électroniques BES* à impact moyen, selon la section 2 de l'annexe 1, s'il y en a, pour chaque actif ; et

1.3. identifier chaque actif qui comporte un *système électronique BES* à impact faible, selon la section 3 de l'annexe 1, s'il y en a (une liste des *systèmes électroniques BES* à impact faible n'est pas exigée).

M1. Les pièces justificatives acceptables comprennent, mais sans s'y limiter, les listes électroniques ou papier datées requises en vertu de l'exigence E1 et ses alinéas 1.1 et 1.2.

E2. L'entité responsable doit : *[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation]*

2.1 passer en revue les identifications de l'exigence E1 et ses alinéas (et les mettre à jour en cas de changement constaté) au moins une fois tous les 15 mois civils, même si aucun élément n'a été identifié selon l'exigence E1 ; et

2.2 faire approuver par son *cadre supérieur CIP* ou son délégué les identifications exigées par l'exigence E1 au moins une fois tous les 15 mois civils, même si aucun élément n'a été identifié selon l'exigence E1.

M2. Les pièces justificatives acceptables comprennent, mais sans s'y limiter, des documents électroniques ou papier datés pour démontrer que l'entité responsable a

passé en revue et mis à jour, lorsque nécessaire, les identifications exigées selon l'exigence E1 et ses alinéas, et qu'elle a fait approuver par son *cadre supérieur CIP* ou son délégué les identifications exigées selon l'exigence E1 et ses alinéas au moins une fois tous les 15 mois civils, même si aucun élément n'a été identifié selon l'exigence E1 et ses alinéas, conformément à l'exigence E2.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable de la surveillance de l'application des normes

L'entité régionale joue le rôle de responsable de la surveillance de l'application des normes (CEA), à moins que l'entité concernée soit détenue, exploitée ou contrôlée par l'entité régionale. Dans de tels cas, l'organisation de fiabilité électrique (ERO), une entité régionale approuvée par la FERC ou un autre organisme gouvernemental pertinent joue le rôle du CEA.

1.2. Conservation des pièces justificatives

Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces justificatives afin de démontrer sa conformité. Dans les cas où la période de conservation des pièces justificatives indiquée est plus courte que le temps écoulé depuis le dernier audit, le CEA peut demander à l'entité de fournir d'autres pièces justificatives pour montrer qu'elle était conforme pendant la période complète écoulée depuis le dernier audit.

L'entité responsable doit conserver les données ou pièces justificatives attestant de sa conformité de la façon indiquée ci-après, à moins que son CEA lui demande de conserver certains documents plus longtemps dans le cadre d'une enquête :

- Chaque entité responsable doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité responsable est jugée non conforme, elle doit conserver l'information relative à cette non-conformité jusqu'à ce que les correctifs aient été appliqués et approuvés ou pendant la période indiquée ci-dessus, selon la durée la plus longue.
- Le CEA doit conserver les derniers dossiers d'audit ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Processus de surveillance et d'évaluation de la conformité

- Audits de conformité
- Déclarations sur la conformité
- Contrôles ponctuels

- Enquêtes sur les non-conformités
- Déclarations volontaires
- Plaintes

1.4. Autres informations sur la conformité

- Aucun

CIP-002-5.1 – Annexe 1

Critères de degré d'impact

Les critères définis à la présente annexe ne sont pas des exigences de conformité autonomes, mais des éléments de caractérisation du degré d'impact auxquels renvoient les exigences.

1. Impact élevé (H)

Chaque *système électronique BES* utilisé par et situé dans une des installations suivantes :

1.1. Chaque *centre de contrôle* ou *centre de contrôle* de repli utilisé pour s'acquitter des obligations fonctionnelles du *coordonnateur de la fiabilité*.

1.2. Chaque *centre de contrôle* ou *centre de contrôle* de repli utilisé pour s'acquitter des obligations fonctionnelles du *responsable de l'équilibrage* pour : 1) une production totale de 3 000 MW ou plus dans une même *Interconnexion*, ou 2) au moins un actif qui répond au critère 2.3, 2.6 ou 2.9.

1.3. Chaque *centre de contrôle* ou *centre de contrôle* de repli utilisé pour s'acquitter des obligations fonctionnelles de l'*exploitant de réseau de transport* pour au moins un actif qui répond au critère 2.2, 2.4, 2.5, 2.7, 2.8, 2.9 ou 2.10.

1.4 Chaque *centre de contrôle* ou *centre de contrôle* de repli utilisé pour s'acquitter des obligations fonctionnelles de l'*exploitant d'installation de production* pour au moins un actif qui répond au critère 2.1, 2.3, 2.6 ou 2.9.

2. Impact moyen (M)

Chaque *système électronique BES,* non inclus dans la section 1 ci-dessus, associés à un des éléments suivants :

2.1. Production en service, pour chaque ensemble de groupes de production à une seule centrale, dont la puissance active nominale nette totale la plus élevée des 12 mois civils précédents est de 1 500 MW ou plus dans une même *Interconnexion*. Pour chaque ensemble de groupes de production, les seuls *systèmes électroniques BES* qui répondent à ce critère sont les *systèmes électroniques BES* partagés qui pourraient, dans un délai de 15 minutes, avoir un impact négatif sur l'exploitation fiable de toute combinaison de groupes de production qui, ensemble, représentent 1 500 MW ou plus dans une même *Interconnexion*.

2.2. Chaque ressource ou groupe de ressources de puissance réactive du BES à un seul emplacement (à l'exclusion des *installations* de production) dont la puissance réactive nominale maximale totale est de 1 000 Mvar ou plus (à l'exclusion de celles aux *installations* de production). Les seuls *systèmes électroniques BES* qui répondent à ce

critère sont les *systèmes électroniques BES* partagés qui pourraient, dans un délai de 15 minutes, avoir un impact négatif sur l'exploitation fiable de toute combinaison de ressources qui au total représentent 1 000 Mvar ou plus.

2.3. Chaque *installation* de production que son *coordonnateur de la planification* ou son *planificateur de réseau de transport* désigne, et en informe le *propriétaire d'installation de production* ou l'*exploitant d'installation de production,* comme étant nécessaire pour éviter un *impact négatif sur la fiabilité* dans un horizon de planification de plus d'un an.

2.4. *Installations* de *transport* exploitées à 500 kV ou plus. Aux fins de ce critère, le jeu de barres collectrices d'une centrale de production n'est pas considéré comme une *installation* de *transport*, mais comme une partie de l'*installation* de raccordement de la production.

2.5. *Installations* de *transport* exploitées entre 200 et 499 kV dans un seul poste, dans les cas où le poste est raccordé à une tension de 200 kV ou plus à au moins trois autres postes de *transport* et ayant une « valeur pondérée totale » de plus de 3 000 selon le tableau ci-dessous. La « valeur pondérée totale » pour un même poste est déterminée en faisant la somme des « valeurs pondérées par ligne » indiquées au tableau ci-dessous pour chaque *ligne de transport* BES d'arrivée et de départ qui le relie à un autre poste de *transport*. Aux fins de ce critère, le jeu de barres collectrices d'une centrale de production n'est pas considéré comme une *installation* de *transport*, mais comme une partie de l'*installation* de raccordement de la production.

Valeur de tension d'une ligne	Valeur pondérée par ligne
Moins de 200 kV (sans objet)	(sans objet)
200 à 299 kV	700
300 à 499 kV	1300
500 kV et plus	0

2.6. Production d'une seule centrale ou *installations* de *transport* d'un seul poste, qui sont désignées par leur *coordonnateur de la fiabilité*, leur *responsable de la planification* ou leur *planificateur de réseau de transport* comme essentielles au calcul des *limites d'exploitation pour la fiabilité de l'Interconnexion* (IROL) et leurs contingences associées.

2.7. *Installations* de *transport* désignées comme essentielles pour respecter les exigences relatives à l'interface de centrale nucléaire.

2.8. *Installations* de *transport*, y compris les *installations* de raccordement de la production, qui fournissent le raccordement de la production nécessaire pour raccorder la sortie du groupe de production aux *réseaux* de *transport* et qui, si elles étaient détruites, endommagées, mal utilisées ou autrement rendues indisponibles,

entraîneraient la perte d'*installations* de production identifiées par un *propriétaire d'installation de production* en vertu du critère 2.1 ou 2.3 de l'annexe 1.

2.9. Chaque *automatisme de réseau* (SPS), *plan de défense* (RAS) ou système de manoeuvre automatisé qui commande des éléments du BES qui, s'ils étaient détruits, endommagés, mal utilisés ou autrement rendus indisponibles, provoqueraient le dépassement d'une ou de plusieurs *limites d'exploitation pour la fiabilité de l'Interconnexion* (IROL) à défaut de fonctionner comme prévu ou entraîneraient la réduction d'une ou de plusieurs IROL s'ils étaient détruits, endommagés, mal utilisés ou autrement rendus indisponibles.

2.10. Chaque système ou groupe d'*éléments* qui effectue du délestage de *charge* automatique sous un système de commande commun, sans intervention humaine, de 300 MW ou plus en mettant en oeuvre du délestage de charge en sous-tension (DST) ou du délestage de charge en sous-fréquence (DSF) selon un programme de délestage de charge soumis à une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

2.11. Chaque *centre de contrôle* ou *centre de contrôle* de repli, non déjà inclus dans la catégorie Impact élevé (H) ci-dessus, utilisé pour s'acquitter des obligations fonctionnelles de l'*exploitant d'installation de production* pour une puissance active nominale nette totale maximale, pour les 12 mois civils précédents, de 1 500 MW ou plus dans une même *Interconnexion*.

2.12. Chaque *centre de contrôle* ou *centre de contrôle* de repli utilisé pour s'acquitter des obligations fonctionnelles de l'*exploitant de réseau de transport* non inclus dans la catégorie Impact élevé (H) ci-dessus.

2.13. Chaque *centre de contrôle* ou *centre de contrôle* de repli, non déjà inclus dans la catégorie Impact élevé (H) ci-dessus, utilisé pour s'acquitter des obligations fonctionnelles du *responsable de l'équilibrage* pour une production égale ou supérieure à 1 500 MW dans une même *Interconnexion*.

3. Impact faible (L)

Systèmes électroniques BES non inclus dans les sections 1 et 2 ci-dessus, qui sont associés à l'un ou l'autre des actifs suivants et qui répondent aux critères d'applicabilité de l'alinéa 4.2 (*Installations*) de la section Applicabilité de la présente norme :

3.1. *Centres de contrôle* et *centres de contrôle* de repli ;

3.2. Postes de transport ;

3.3. Ressources de production ;

3.4. Systèmes et installations essentiels à la remise en charge du réseau, y compris les *ressources à démarrage autonome* et les *chemins de démarrage* ainsi que les exigences relatives aux manœuvres initiales ;

3.5. *Automatismes de réseau* qui supportent l'exploitation fiable du *système de production-transport d'électricité* ;

3.6. Pour les *distributeurs*, *systèmes de protection* indiqués à l'alinéa 4.2.1 de la section Applicabilité ci-dessus.

Annexe QC-CIP-002-5.1
Dispositions particulières de la norme CIP-002-5.1 applicables au Québec

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son 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 aura préséance.

A. Introduction

1. **Titre :** Cybersécurité — Catégorisation des systèmes électroniques BES

2. **Numéro :** CIP-002-5.1

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

Entités fonctionnelles

Aucune disposition particulière

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 :

- Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur 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 201x

5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 201x

5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : xx mois 201x

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. **Processus de surveillance de la conformité**

1.1. Responsable de la surveillance de l'application des normes

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et d'évaluation de la conformité

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

CIP-002-5.1 — Annexe 1

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	Xx mois 201x	Nouvelle annexe	Nouvelle

A. Introduction

1. Titre : Cybersécurité – Mécanismes de gestion de la sécurité

2. Numéro : CIP-003-5

3. Objet : Définir des mécanismes de gestion de la sécurité cohérents et viables qui établissent les responsabilités et l'imputabilité à l'égard de la protection des *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou des instabilités dans le BES.

4. Applicabilité :

4.1. Entités fonctionnelles : Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

4.1.1 Responsable de l'équilibrage

4.1.2 Distributeur qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du BES :

4.1.2.1 Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :

4.1.2.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.1.2.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.1.2.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

4.2. Installations : Dans le contexte des exigences de la présente norme, les *installations*, systèmes et équipements suivants détenus par chaque entité responsable indiquée à la section 4.1 sont ceux auxquels ces exigences sont applicables. Dans le cas des exigences de cette norme qui visent un type particulier d'*installations*, de système ou d'équipements, ou un sous-ensemble d'*installations*, de systèmes ou d'équipements, ceux-ci sont précisés explicitement.

4.2.1 Distributeur : Un ou plusieurs des *installations*, systèmes et équipements suivants détenus par le distributeur pour la protection ou la remise en charge du BES :

4.2.1.1 Chaque système de DSF ou de DST qui :

4.2.1.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.2.1.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

4.2.3 Exemptions : Sont exemptés de la norme CIP-003-5 :

4.2.3.1 Les actifs électroniques aux installations réglementés par la Commission canadienne de sûreté nucléaire ;

4.2.3.2 Les actifs électroniques associés aux réseaux de communication et aux liaisons d'échange de données entre périmètres de sécurité électroniques distincts ;

4.2.3.3 Les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme à la norme CFR 10, section 73.54 ;

4.2.3.4 Dans le cas des *distributeurs*, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus.

5. Dates d'entrée en vigueur :

1. **24 mois minimum** – La norme CIP-003-5, à l'exception de l'exigence E2 de la CIP-003-5, entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long. L'exigence E2 de la CIP-003-5 entrera en vigueur soit le 1er juillet 2016, soit le premier jour civil du treizième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.
2. Dans les juridictions où une aucune approbation réglementaire n'est requise, la norme CIP-003-5, à l'exception de l'exigence E2 de la CIP-003-5, entrera en vigueur le premier jour du neuvième trimestre civil suivant l'adoption par le Conseil d'administration ; l'exigence E2 de la CIP-003-5 entrera en vigueur le premier jour du treizième trimestre civil suivant l'adoption par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte :

La norme CIP-003-5 fait partie d'une série de normes CIP sur la cybersécurité. La norme CIP-002-5 exige l'identification et la catégorisation initiales des *systèmes électroniques BES*. Les normes CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 et CIP-011-1 exigent un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*. Cette série de normes CIP est appelée « version 5 des normes CIP sur la cybersécurité ».

Le SDT a intégré à la présente norme une reconnaissance à l'effet que certaines exigences ne devraient pas mettre l'accent sur les cas individuels de défaillance comme seul motif d'infraction à la norme. En particulier, le SDT a intégré une approche visant à habiliter l'industrie à identifier, à évaluer et à corriger les lacunes dans la mise en œuvre de certaines exigences. L'intention est de changer la manière de considérer les infractions dans ces exigences, de sorte qu'il ne s'agisse plus de savoir *si* une lacune existe, mais plutôt d'identifier, d'évaluer et de corriger les

lacunes. Ceci est présenté dans ces exigences en modifiant la notion de « mise en œuvre » de la façon suivante :

> Chaque entité responsable doit mettre en œuvre**, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes…**

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité devrait inclure autant qu'elle le juge nécessaire à leurs processus documentés, pourvu que les exigences pertinentes soient couvertes. Les processus documentés eux-mêmes n'ont pas à intégrer la démarche « détecter, évaluer et corriger les lacunes » décrite au paragraphe précédent, car cette démarche est liée à la manière de mettre en œuvre les processus documentés et pourrait être réalisée par d'autres mesures de contrôle ou de gestion de la conformité.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », lorsque cela fait du sens et est communément compris. Par exemple, les processus documentés qui décrivent une réponse sont généralement appelés « plans » (plan d'action en cas d'incident, plan de rétablissement, etc.). De plus, un plan de sécurité peut décrire une approche comportant plusieurs procédures couvrant un thème étendu.

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont un exemple trouvé dans les normes. La mise en œuvre complète des normes CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

Les entités responsables peuvent mettre en œuvre des moyens communs qui répondent aux besoins de plusieurs *systèmes électroniques BES* à impact élevé et moyen. Par exemple, un même programme de formation pourrait répondre aux exigences en formation du personnel de plusieurs *systèmes électroniques BES*.

Les mesures présentent des exemples de pièces justificatives pour montrer la documentation et la mise en œuvre de l'exigence. Ces mesures servent à fournir des conseils aux entités sur ce qui peut constituer des dossiers de conformité acceptables et ne devraient pas être considérées comme une liste exhaustive.

Dans l'ensemble des normes, sauf indication particulière, les éléments présentés à la section Exigences et mesures sous forme de liste à puces sont liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST

provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances de systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes de DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

B. Exigences et mesures

E1. Chaque entité responsable, pour ses *systèmes électroniques BES* à impact élevé ou moyen, doit revoir et faire approuver par un *cadre supérieur CIP*, au moins une fois tous les 15 mois civils, une ou plusieurs politiques de cybersécurité documentées qui, collectivement, couvrent les thèmes suivants : *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]*

- **1.1** personnel et formation (CIP-004) ;
- **1.2** *périmètres de sécurité électronique* (CIP-005), y compris l'*accès distant interactif* ;
- **1.3** sécurité physique des *systèmes électroniques BES* (CIP-006) ;
- **1.4** gestion de la sécurité des systèmes (CIP-007) ;
- **1.5** déclaration des incidents et planification des mesures d'intervention (CIP-008) ;
- **1.6** plans de rétablissement des *systèmes électroniques BES* (CIP-009) ;
- **1.7** gestion des changements de configuration et analyses de vulnérabilité (CIP-010) ;
- **1.8** protection de l'information (CIP-011) ; et
- **1.9** déclaration et réponse aux *circonstances CIP exceptionnelles*.

M1. Des exemples de pièces justificatives peuvent comprendre, mais ne sont pas limités à, des documents de politique ; un historique de révisions, des dossiers d'examen ou des preuves de flux de travail provenant d'un système de gestion documentaire qui indiquent l'examen de chaque politique de cybersécurité au moins une fois tous les 15 mois civils ; et l'approbation documentée de chaque politique de cybersécurité par le *cadre supérieur CIP*.

E2. Chaque entité responsable doit, pour ses actifs identifiés à la norme CIP-002-5, exigence E1, alinéa E1.3, mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, une ou plusieurs politiques de cybersécurité documentées qui, collectivement, couvrent les thèmes suivants, et doit revoir et faire approuver ces politiques par un *cadre supérieur CIP* au moins une fois tous les 15 mois civils : *[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation]*

- **2.1** sensibilisation à la cybersécurité ;
- **2.2** contrôles de sécurité physique ;
- **2.3** contrôle des accès électroniques pour les connexions externes à protocole routable et la *connectivité par lien commuté* ; et
- **2.4** intervention en cas d'incident de cybersécurité.

Un inventaire, une liste ou une identification distincte des *systèmes électroniques BES* à impact faible ou de leurs *actifs électroniques BES* n'est pas exigé.

M2. Des exemples de pièces justificatives peuvent comprendre, mais ne sont pas limités à, une ou plusieurs politiques de cybersécurité documentées et des preuves de processus, de procédures ou de plans qui démontrent la mise en oeuvre des thèmes exigés ; historique de révisions, dossiers d'examen ou preuves de flux de travail provenant d'un système de gestion documentaire qui indique l'examen de chaque politique de cybersécurité au moins une fois tous les 15 mois civils ; et approbation documentée de chaque politique de cybersécurité par un *cadre supérieur CIP*.

E3. Chaque entité responsable doit désigner un *cadre supérieur CIP* par nom et documenter tout changement dans un délai de 30 jours civils suivant le changement. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]*

M3. Un exemple de pièce justificative peut comprendre, mais n'est pas limité à, un document daté et approuvé par un haut dirigeant indiquant le nom de la personne désignée comme *cadre supérieur CIP*.

E4. L'entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un processus documenté de délégation de pouvoirs, sauf en l'absence de toute délégation. Dans les cas permis par les normes CIP, le *cadre supérieur CIP* peut déléguer ses pouvoirs relatifs à certains actes à un ou plusieurs délégués. Ces délégations doivent être documentées, et comprendre notamment le nom ou le titre du délégué, les actes délégués et la date de la délégation ; approuvées par le *cadre supérieur CIP* ; et mises à jour dans un délai de 30 jours suivant tout changement à la délégation. Il n'est pas nécessaire de réaffirmer les changements de délégation en cas de changement de délégant. *[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation]*

M4. Un exemple de pièce justificative peut comprendre, mais n'est pas limité à, un document daté et approuvé par le *cadre supérieur CIP* indiquant la ou les personnes (nom ou titre) auxquelles est délégué le pouvoir d'approuver ou d'autoriser des actions décrites explicitement.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable de la surveillance de l'application des normes

L'entité régionale joue le rôle de responsable de la surveillance de l'application des normes (CEA), à moins que l'entité concernée soit détenue, exploitée ou contrôlée par l'entité régionale. Dans de tels cas, le rôle de CEA est confié à l'ERO, à une entité régionale approuvée par la FERC ou à un autre organisme gouvernemental pertinent.

1.2. Conservation des pièces justificatives

Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces justificatives afin de démontrer sa conformité. Dans les cas où la période de conservation des pièces justificatives indiquée est plus courte que le temps écoulé depuis le dernier audit, le CEA peut demander à l'entité de fournir d'autres pièces justificatives pour montrer qu'elle était conforme pendant la période complète écoulée depuis le dernier audit.

L'entité responsable doit conserver les données ou pièces justificatives attestant de sa conformité de la façon indiquée ci-après, à moins que son CEA lui demande de conserver certains documents plus longtemps dans le cadre d'une enquête :

- Chaque entité responsable doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité responsable est jugée non conforme, elle doit conserver l'information relative à cette non-conformité jusqu'à ce que les correctifs aient été appliqués et approuvés ou pendant la période indiquée ci-dessus, selon la durée la plus longue.
- Le CEA doit conserver les derniers dossiers d'audit ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Processus de surveillance et d'évaluation de la conformité

- Audits de conformité
- Déclarations sur la conformité
- Contrôles ponctuels
- Enquêtes sur les non-conformités
- Déclarations volontaires
- Plaintes

1.4. Autres informations sur la conformité

- Aucune

Annexe QC-CIP-003-5
Dispositions particulières de la norme CIP-003-5 applicables au Québec

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son 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 aura préséance.

A. Introduction

1. **Titre :** Cybersécurité — Mécanismes de gestion de la sécurité
2. **Numéro :** CIP-003-5
3. **Objet :** Aucune disposition particulière
4. **Applicabilité :**

Entités fonctionnelles

Aucune disposition particulière

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 :

- Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur 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 201x

5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 201x

5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : xx mois 201x

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. **Processus de surveillance de la conformité**

1.1. Responsable de la surveillance de l'application des normes

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et d'évaluation de la conformité

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	Xx mois 201x	Nouvelle annexe	Nouvelle

A. Introduction

1. **Titre :** Cybersécurité — Personnel et formation

2. **Numéro :** CIP-004-5.1

3. **Objet :** Minimiser les risques de compromissions, qui pourraient entraîner un fonctionnement incorrect ou une instabilité du BES, attribuables à des personnes qui accèdent à des *systèmes électroniques BES,* en exigeant une évaluation des risques liés au personnel, une formation et une sensibilisation à la sécurité qui soient adéquates pour protéger ces *systèmes électroniques BES*.

4. **Applicabilité :**

   4.1. Entités fonctionnelles : Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

   4.1.1. Responsable de l'équilibrage

   4.1.2. Distributeur qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du BES :

   4.1.2.1. Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :

   4.1.2.1.1. fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

   4.1.2.1.2. effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

   4.1.2.2. Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

   4.1.2.3. Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

   4.1.2.4. Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

   4.1.3. Exploitant d'installation de production

   4.1.4. Propriétaire d'installation de production

4.1.5. Coordonnateur des échanges ou Responsable des échanges

4.1.6. Coordonnateur de la fiabilité

4.1.7. Exploitant de réseau de transport

4.1.8. Propriétaire d'installation de transport

4.2. Installations : Dans le contexte des exigences de la présente norme, les *installations*, systèmes et équipements suivants détenus par chaque entité responsable indiquée à la section 4.1 sont ceux auxquels ces exigences sont applicables. Dans le cas des exigences de cette norme qui visent un type particulier d'*installations*, de système ou d'équipements, ou un sous-ensemble d'*installations*, de systèmes ou d'équipements, ceux-ci sont précisés explicitement.

4.2.1. Distributeur : Un ou plusieurs des *installations*, systèmes et équipements suivants détenus par le distributeur pour la protection ou la remise en charge du BES :

4.2.1.1. Chaque système de DSF ou de DST qui :

4.2.1.1.1. fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.2.1.1.2. effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.2.1.2. Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.3. Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.4. Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.2.2. Entités responsables indiquées en 4.1, sauf les distributeurs :
Toutes les *installations* du BES.

4.2.3. Exemptions : Sont exemptés de la norme CIP-002-5 :

4.2.3.1. Les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire

4.2.3.2. les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électroniques* distincts ;

4.2.3.3. les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme à la norme CFR 10, section 73.54 ;

4.2.3.4. dans le cas des distributeurs, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus.

4.2.3.5. les entités responsables qui déterminent qu'elles n'ont pas de systèmes électroniques BES catégorisés comme impact élevé ou impact moyen en conformité avec le processus d'identification et de catégorisation de la CIP-002-5.

5. Dates d'entrée en vigueur :

1. **24 mois minimum**– La norme CIP-004-5.1 entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.
2. Dans les juridictions où aucune approbation réglementaire n'est requise, la norme CIP-004-5.1 entrera en vigueur le premier jour du neuvième trimestre civil suivant l'approbation par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte :

La norme CIP-004-5.1 fait partie d'une série de normes CIP sur la cybersécurité. La norme CIP-002-5 exige l'identification et la catégorisation initiales des *systèmes électroniques BES*. Les normes CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 et CIP-011-1 exigent un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*. Cette série de normes CIP est appelée « version 5 des normes CIP sur la cybersécurité ».

Le SDT a intégré à la présente norme une reconnaissance à l'effet que certaines exigences ne devraient pas mettre l'accent sur les cas individuels de défaillance comme seul motif d'infraction à la norme. En particulier, le SDT a intégré une approche visant à habiliter l'industrie à identifier, à évaluer et à corriger les lacunes dans la mise en œuvre de certaines exigences. L'intention est de changer la manière de considérer les infractions dans ces exigences, de sorte qu'il ne s'agisse plus de savoir *si* une lacune existe, mais plutôt d'identifier, d'évaluer et de corriger les lacunes. Ceci est présenté dans ces exigences en modifiant la notion de « mise en œuvre » de la façon suivante :

> Chaque entité responsable doit mettre en œuvre**, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes…**

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique

pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité devrait inclure autant qu'elle le juge nécessaire à leurs processus documentés, pourvu que les exigences pertinentes soient couvertes. Les processus documentés eux-mêmes n'ont pas à intégrer la démarche « détecter, évaluer et corriger les lacunes » décrite au paragraphe précédent, car cette démarche est liée à la manière de mettre en œuvre les processus documentés et pourrait être réalisée par d'autres mesures de contrôle ou de gestion de la conformité.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », lorsque cela a du sens et est communément compris. Par exemple, les processus documentés qui décrivent une réponse sont généralement appelés « plans » (plan d'action en cas d'incident, plan de rétablissement, etc.). De plus, un plan de sécurité peut décrire une approche comportant plusieurs procédures couvrant un thème étendu.

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont un exemple trouvé dans les normes. La mise en œuvre complète des normes CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

Les entités responsables peuvent mettre en œuvre des moyens communs qui répondent aux besoins de plusieurs *systèmes électroniques BES* à impact élevé et moyen. Par exemple, un même programme de formation pourrait répondre aux exigences en formation du personnel de plusieurs *systèmes électroniques BES*.

Les mesures présentent des exemples de pièces justificatives pour montrer la documentation et la mise en œuvre de l'exigence. Ces mesures servent à fournir des conseils aux entités sur ce qui peut constituer des dossiers de conformité acceptables et ne devraient pas être considérées comme une liste exhaustive.

Dans l'ensemble des normes, sauf indication particulière, les éléments présentés à la section Exigences et mesures sous forme de liste à puces sont liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances de systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes de DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

Colonne « Systèmes visés » des tableaux

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. Le SDT CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- **Systèmes électroniques BES à impact élevé –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.

- **Systèmes électroniques BES à impact moyen –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.

- **Systèmes électroniques BES à impact moyen à connectivité externe routable** – Désigne uniquement les *systèmes électroniques BES* à impact moyen à *connectivité externe routable*. Exclut les *actifs électroniques* des *systèmes électroniques BES* auxquels on ne peut avoir accès directement par *connectivité externe routable*.

- **Systèmes de contrôle ou de surveillance des accès électroniques (EACMS)** – Désigne tout *système de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d'authentification, et systèmes de surveillance de registre d'événement et d'alerte.

- **Systèmes de contrôle des accès physiques (PACS)** – Désigne tout *système de contrôle des accès physique*s associé à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.

B. Exigences et mesures

E1. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-004-5.1) – Programme de sensibilisation à la sécurité. *[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation]*

M1. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-004-5.1) – Programme de sensibilisation à la sécurité, ainsi que des pièces justificatives additionnelles pour démontrer la mise en œuvre tel que décrit dans la colonne Mesures du tableau.

Tableau E1 (CIP-004-5.1) – Programme de sensibilisation à la sécurité

Partie	Systèmes visés	Exigences	Mesures
1.1	*Systèmes électroniques BES* à impact élevé. *Systèmes électroniques BES* à impact moyen.	Une sensibilisation à la sécurité qui, au moins une fois par trimestre civil, rappelle les pratiques de cybersécurité (pouvant inclure les pratiques de sécurité physique associées) au personnel de l'entité responsable qui a un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *systèmes électroniques BES*.	Exemple non limitatif de pièce justificative : des documents attestant que le rappel trimestriel a été fait. Exemples non limitatifs de pièces justificatives du rappel : des copies datées de l'information utilisée pour rappeler les pratiques de sécurité et preuves de sa distribution, tel que : • communications ciblées (p. ex., courriels, notes de service, formation en ligne, etc.) ; • communications générales (p. ex., affiches, intranet, brochures, etc.) ; ou • soutien et rappels de la direction (p. ex., présentations, réunions, etc.).

E2. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou des programmes de formation sur la cybersécurité axée sur les rôles, les fonctions ou les responsabilités de chacun, qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-004-5.1) – Programme de formation sur la cybersécurité. *[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation]*

M2. Les pièces justificatives doivent inclure les programmes de formation qui comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-004-5.1) – Programme de formation sur la cybersécurité, ainsi que des pièces justificatives additionnelles pour démontrer la mise en œuvre des programmes.

Tableau E2 (CIP-004-5.1) – Programme de formation sur la cybersécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à connectivité externe routable et leurs : 1. EACMS associés ; et 2. PACS associés.	Formation portant sur : 2.1.1. les politiques de cybersécurité ; 2.1.2. le contrôle des accès physiques ; 2.1.3. le contrôle des accès électroniques ; 2.1.4. le programme de contrôle des visiteurs ; 2.1.5. la gestion et le stockage de l'information des *systèmes électroniques BES* ; 2.1.6. la détection des *incidents de cybersécurité* et l'envoi des avis initiaux conformément au plan d'intervention en cas d'incident de l'entité ; 2.1.7. les plans de rétablissement des *systèmes électroniques BES* ; 2.1.8. l'intervention en cas d'*incident de cybersécurité* ; et 2.1.9. les risques pour la cybersécurité associés à l'interconnectabilité et à l'interopérabilité des *systèmes électroniques BES* avec d'autres *actifs électroniques*.	Exemples non limitatifs de pièces justificatives : matériel de formation, tel que présentations PowerPoint, notes à l'intention des instructeurs ou des étudiants, ou documents de cours.

Tableau E2 (CIP-004-5.1) – Programme de formation sur la cybersécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Exige d'avoir terminé la formation énoncée à la partie 2.1 avant de se voir accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *actifs électroniques* visés, sauf dans des *circonstances CIP exceptionnelles*.	Exemples non limitatifs de pièces justificatives : registres de formation et documents attestant l'invocation de *circonstances CIP exceptionnelles*.
2.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS ; et 2. PACS.	Exige d'avoir terminé la formation énoncée à la partie 2.1 au moins une fois tous les 15 mois civils.	Exemple non limitatif de pièce justificative : registres de formation individuels datés.

E3. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs programmes documentés d'évaluation des risques liés au personnel avant d'accorder ou de maintenir un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *systèmes électroniques BES* et qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E3 (CIP-004-5.1) – Programme d'évaluation des risques liés au personnel. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]*

M3. Les pièces justificatives doivent comprendre le ou les programmes documentés d'évaluation des risques liés au personnel qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E3 (CIP-004-5.1) – Programme d'évaluation des risques liés au personnel, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre du ou des programmes.

Tableau E3 (CIP-004-5.1) – Programme d'évaluation des risques liés au personnel			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Processus pour confirmer l'identité.	Exemple non limitatif de pièce justificative : documents démontrant le processus suivi par l'entité responsable pour confirmer l'identité.

Tableau E3 (CIP-004-5.1) – Programme d'évaluation des risques liés au personnel			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Processus de vérification des antécédents judiciaires sur les sept années précédentes dans le cadre de chaque évaluation des risques liés au personnel qui comprend : 3.2.1. le lieu où réside actuellement la personne, peu importe depuis combien de temps ; et 3.2.2. les autres endroits où, au cours des sept années précédant immédiatement la date de vérification des antécédents judiciaires, la personne a résidé pendant au moins six mois consécutifs. S'il est impossible de mener une vérification complète des antécédents judiciaires sur les sept années précédentes, pousser la vérification le plus loin possible et consigner les motifs pour lesquels la vérification complète sur cette période n'a pu se faire.	Exemple non limitatif de pièce justificative : documents démontrant le processus suivi par l'entité responsable pour vérifier les antécédents criminels sur les sept dernières années.

Tableau E3 (CIP-004-5.1) – Programme d'évaluation des risques liés au personnel			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Critères ou processus pour évaluer les résultats de la vérification des antécédents judiciaires en vue d'autoriser un accès.	Exemple non limitatif de pièce justificative : documents démontrant le processus de l'entité responsable pour évaluer les résultats des vérifications des antécédents judiciaires.
3.4	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Critères ou processus pour vérifier que les évaluations des risques liés au personnel dont les entrepreneurs et les fournisseurs de services doivent faire l'objet sont menées conformément aux parties 3.1 à 3.3.	Exemples non limitatifs de pièces justificatives : documents démontrant les critères ou le processus de l'entité responsable pour vérifier les évaluations des risques liés au personnel pour les entrepreneurs et les fournisseurs de services.

Tableau E3 (CIP-004-5.1) – Programme d'évaluation des risques liés au personnel			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.5	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Processus permettant de s'assurer que les personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement ont fait l'objet d'une évaluation des risques liés au personnel conformément aux parties 3.1 à 3.4 au cours des sept dernières années.	Exemples non limitatifs de pièces justificatives : documents démontrant le processus suivi par l'entité responsable pour s'assurer que les personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement ont fait l'objet d'une évaluation des risques liés au personnel au cours des sept dernières années.

E4. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs programmes documentés de gestion des accès qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E4 (CIP-004-5.1) – Programme de gestion des accès. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation et exploitation du jour même]*

M4. Les pièces justificatives doivent comprendre les processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E4 (CIP-004-5.1) – Programme de gestion des accès, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre des mesures du programme de gestion des accès selon la colonne Mesures du tableau.

Tableau E4 (CIP-004-5.1) – Programme de gestion des accès			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
4.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Processus d'autorisation selon les besoins, tel que déterminé par l'entité responsable, sauf dans des *circonstances CIP exceptionnelles*, de : 4.1.1. l'accès électronique ; 4.1.2. l'accès physique sans accompagnement dans un *périmètre de sécurité physique* ; et 4.1.3. l'accès à des emplacements de stockage (physiques ou électroniques) désignés pour l'information de *système électronique BES*.	Exemples non limitatifs de pièces justificatives : documents datés démontrant le processus suivi pour autoriser un accès électronique, un accès physique sans accompagnement à un *périmètre de sécurité physique* et un accès à des emplacements de stockage (physiques ou électroniques) désignés pour l'information de *système électronique BES*.

Tableau E4 (CIP-004-5.1) – Programme de gestion des accès			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
4.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Vérifier, au moins une fois par trimestre civil, que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des registres d'accès autorisé.	Exemples non limitatifs de pièces justificatives : • documents datés attestant l'établissement d'une comparaison entre la liste, générée par le système, des personnes pour lesquelles on a autorisé l'accès (c.-à-d., base de données des activités de fourniture) et la liste, générée par le système, des personnes ayant un accès (c.-à-d., liste des comptes utilisateurs) ; ou • documents datés attestant l'établissement d'une comparaison entre la liste des personnes pour lesquelles on a autorisé l'accès (c.-à-d., formulaires d'autorisation) et la liste des personnes auxquelles on a fourni un accès (c.-à-d., formulaires de fourniture d'accès ou liste des comptes partagés).

Tableau E4 (CIP-004-5.1) – Programme de gestion des accès			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
4.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Dans le cas d'un accès électronique, vérifier, au moins une fois tous les 15 mois civils, que tous les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont correctement attribués et qu'ils sont ceux jugés nécessaires par l'entité responsable.	Exemples non limitatifs de pièces justificatives : documentation de l'examen, y compris tous les éléments suivants : 1. liste datée de tous les comptes ou groupes de comptes ou rôles au sein du système ; 2. description sommaire des droits d'accès associés à chaque groupe ou rôle ; 3. comptes attribués au groupe ou au rôle ; et 4. preuve datée démontrant que l'on a vérifié que les droits d'accès du groupe sont autorisés et qu'ils sont appropriés selon les fonctions de toute personne à qui ils sont attribués.

Tableau E4 (CIP-004-5.1) – Programme de gestion des accès			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
4.4	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Vérifier, au moins une fois tous les 15 mois civils, que l'accès aux emplacements de stockage (physiques ou électroniques) désignés pour l'information de *système électronique BES* est correctement attribué et qu'il correspond à ce que l'entité responsable juge nécessaire pour les tâches à accomplir.	Exemples non limitatifs de pièces justificatives : documentation de l'examen, y compris tous les éléments suivants : 1. liste datée des autorisations d'accès à l'information de *système électronique BES* ; 2. droits d'accès associés aux autorisations ; et 3. preuve datée démontrant que l'on s'est assuré que les autorisations et les droits d'accès sont correctement attribués et qu'ils correspondent au minimum nécessaire pour les tâches à accomplir.

E5. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs programmes documentés de révocation d'accès qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E5 (CIP-004-5.1) – Révocation d'accès. *[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation du jour même et planification de l'exploitation]*

M5. Les pièces justificatives doivent comprendre chacun des programmes documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables figurant dans le tableau E5 (CIP-004-5.1) – Révocation d'accès, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre selon la colonne Mesures du tableau.

Tableau E5 (CIP-004-5.1) – Révocation d'accès			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
5.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Un processus déclenchant le retrait à une personne de la possibilité d'accès physique sans accompagnement et d'*accès distant interactif* lors de son départ et menant à bien ce processus dans un délai de 24 heures suivant le départ. (Le retrait de la possibilité d'accès peut différer de la suppression, de la désactivation, de la révocation ou du retrait de tous les droits d'accès.)	Exemples non limitatifs de pièces justificatives : 1. formulaire d'activité ou d'approbation daté qui confirme le retrait de l'accès associé au départ ; et 2. journaux ou autres preuves attestant que la personne ne dispose plus d'un accès.

Tableau E5 (CIP-004-5.1) – Révocation d'accès			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
5.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 3. EACMS associés ; et 4. PACS associés.	Dans le cas d'une réaffectation ou d'une mutation, révoquer l'accès électronique autorisé aux comptes individuels et l'accès physique sans accompagnement autorisé que l'entité responsable juge non nécessaires avant la fin du jour civil suivant la date que l'entité responsable détermine comme étant celle où la personne n'a plus besoin de cet accès.	Exemples non limitatifs de pièces justificatives : 1. formulaire d'activité ou d'approbation daté attestant l'examen de l'accès logique et physique ; et 2. journaux ou autres preuves attestant que ces personnes ne disposent plus de l'accès que l'entité responsable détermine comme n'étant plus nécessaire.
5.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PACS associés.	Dans le cas d'un départ, révoquer l'accès de la personne aux emplacements de stockage désignés pour l'information de *système électronique BES*, qu'ils soient physiques ou électroniques (à moins que l'accès ait déjà été révoqué selon l'exigence E5.1), avant la fin du jour civil suivant la date à laquelle prend effet le départ.	Exemple non limitatif de pièce justificative : formulaire d'activité ou d'approbation attestant le retrait de l'accès aux emplacements physiques ou aux systèmes électroniques désignés pour l'information de *système électronique BES* daté du jour civil suivant le départ, au plus tard.

Tableau E5 (CIP-004-5.1) – Révocation d'accès			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
5.4	*Systèmes électroniques BES* à impact élevé et leurs : • EACMS associés.	Dans le cas d'un départ, révoquer l'accès aux comptes utilisateurs non partagés de la personne (à moins que l'accès ait déjà été révoqué selon l'exigence E5.1 ou E5.3) dans les 30 jours civils suivant la date à laquelle prend effet le départ.	Exemple non limitatif de pièce justificative : formulaire d'activité ou d'approbation attestant le retrait de l'accès à un *actif électronique BES* ou à une application logicielle selon ce qui est jugé nécessaire pour mener à bien la révocation d'accès et daté dans les 30 jours civils suivant le départ.
5.5	*Systèmes électroniques BES* à impact élevé et leurs : • EACMS associés.	Dans le cas d'un départ, changer les mots de passe des comptes partagés connus de l'utilisateur dans les 30 jours civils suivant le départ. Dans le cas d'une réaffectation ou d'une mutation, changer les mots de passe des comptes partagés connus de l'utilisateur dans les 30 jours civils suivant la date que l'entité responsable détermine comme étant celle où la personne n'a plus besoin de cet accès. Si l'entité responsable détermine et documente que cela prendra plus de temps en raison de circonstances opérationnelles atténuantes, changer les mots de passe dans les 10 jours civils suivant la fin de ces circonstances.	Exemples non limitatifs de pièces justificatives : • formulaire d'activité ou d'approbation attestant que le mot de passe a été réinitialisé dans les 30 jours civils suivant le départ ; • formulaire d'activité ou d'approbation attestant que le mot de passe a été réinitialisé dans les 30 jours civils suivant la réaffectation ou la mutation ; ou • documentation des circonstances opérationnelles atténuantes et formulaire d'activité ou d'approbation attestant que le mot de passe a été réinitialisé dans les 10 jours civils suivant la fin de ces circonstances.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable de la surveillance de l'application des normes

L'entité régionale joue le rôle de responsable de la surveillance de l'application des normes (CEA), à moins que l'entité concernée soit détenue, exploitée ou contrôlée par l'entité régionale. Dans de tels cas, le rôle de CEA est confié à l'ERO, à une entité régionale approuvée par la FERC ou à un autre organisme gouvernemental pertinent.

1.2. Conservation des pièces justificatives

Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces justificatives afin de démontrer sa conformité. Dans les cas où la période de conservation des pièces justificatives indiquée est plus courte que le temps écoulé depuis le dernier audit, le CEA peut demander à l'entité de fournir d'autres pièces justificatives pour montrer qu'elle était conforme pendant la période complète écoulée depuis le dernier audit.

L'entité responsable doit conserver les données ou pièces justificatives attestant de sa conformité de la façon indiquée ci-après, à moins que son CEA lui demande de conserver certains documents plus longtemps dans le cadre d'une enquête :

- Chaque entité responsable doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité responsable est jugée non conforme, elle doit conserver l'information relative à cette non-conformité jusqu'à ce que les correctifs aient été appliqués et approuvés ou pendant la période indiquée ci-dessus, selon la durée la plus longue.
- Le CEA doit conserver les derniers dossiers d'audit ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Processus de surveillance et d'évaluation de la conformité

- Audits de conformité
- Déclarations sur la conformité
- Contrôles ponctuels
- Enquêtes sur les non-conformités
- Déclarations volontaires
- Plaintes

1.4. Autres informations sur la conformité

- Aucune

Annexe QC-CIP-004-5.1
Dispositions particulières de la norme CIP-004-5.1 applicables au Québec

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son 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 aura préséance.

A. Introduction

1. **Titre :** Cybersécurité — Personnel et formation

2. **Numéro :** CIP-004-5.1

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

Entités fonctionnelles

Aucune disposition particulière

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 :

- Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur 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 201x

5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 201x

5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : xx mois 201x

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. **Processus de surveillance de la conformité**

1.1. Responsable de la surveillance de l'application des normes

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et d'évaluation de la conformité

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	Xx mois 201x	Nouvelle annexe	Nouvelle

A. Introduction

1. Titre : Cybersécurité – Périmètres de sécurité électronique

2. Numéro : CIP-005-5

3. Objet : Gérer l'accès électronique aux *systèmes électroniques BES* en établissant un *périmètre de sécurité électronique* (ESP) contrôlé afin de protéger les *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou une instabilité dans le BES.

4. Applicabilité :

4.1. Entités fonctionnelles : Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

4.1.1 Responsable de l'équilibrage

4.1.2 Distributeur qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du BES :

4.1.2.1 Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :

4.1.2.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.1.2.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.1.2.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

4.2. Installations : Dans le contexte des exigences de la présente norme, les *installations*, systèmes et équipements suivants détenus par chaque entité responsable indiquée à la section 4.1 sont ceux auxquels ces exigences sont applicables. Dans le cas des exigences de cette norme qui visent un type particulier d'*installations*, de système ou d'équipements, ou un sous-ensemble d'*installations*, de systèmes ou d'équipements, ceux-ci sont précisés explicitement.

4.2.1 Distributeur : Un ou plusieurs des *installations*, systèmes et équipements suivants détenus par le distributeur pour la protection ou la remise en charge du BES :

4.2.1.1 Chaque système de DSF ou de DST qui :

4.2.1.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.2.1.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

4.2.3 Exemptions : Sont exemptés de la norme CIP-005-5 :

4.2.3.1 Les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire ;

4.2.3.2 les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électroniques* distincts ;

4.2.3.3 les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme à la norme CFR 10, section 73.54 ;

4.2.3.4 dans le cas des distributeurs, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus ;

4.2.3.5 les entités responsables qui déterminent qu'elles n'ont pas de systèmes électroniques BES catégorisés comme impact élevé ou impact moyen en conformité avec le processus d'identification et de catégorisation de la CIP-002-5.

5. Dates d'entrée en vigueur :

1. **24 mois minimum** – La norme CIP-005-5 entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.
2. Dans les juridictions où aucune approbation réglementaire n'est requise, la norme CIP-005-5 entrera en vigueur le premier jour du neuvième trimestre civil suivant l'approbation par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte :

La norme CIP-005-5 fait partie d'une série de normes CIP sur la cybersécurité. La norme CIP-002-5 exige l'identification et la catégorisation initiales des *systèmes électroniques BES*. Les normes CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 et CIP-011-1 exigent un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*. Cette série de normes CIP est appelée « version 5 des normes CIP sur la cybersécurité ».

La plupart des exigences commencent ainsi : « Chaque entité responsable doit mettre en œuvre un ou plusieurs [processus, plans, etc.] documentés qui correspondent à toutes les parties d'exigence applicables du tableau [référence au tableau]. » Le tableau en référence précise les éléments qui doivent être inclus dans les procédures pour le thème commun de l'exigence.

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité devrait inclure autant qu'elle le juge nécessaire à leurs processus documentés, pourvu que les exigences pertinentes soient couvertes.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », lorsque cela a du sens et est communément compris. Par exemple, les processus documentés qui décrivent une réponse sont généralement appelés

« plans » (plan d'action en cas d'incident, plan de rétablissement, etc.). De plus, un plan de sécurité peut décrire une approche comportant plusieurs procédures couvrant un thème étendu.

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont un exemple trouvé dans les normes. La mise en œuvre complète des normes CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

Les entités responsables peuvent mettre en œuvre des moyens communs qui répondent aux besoins de plusieurs *systèmes électroniques BES* à impact élevé et moyen. Par exemple, un même programme de formation pourrait répondre aux exigences en formation du personnel de plusieurs *systèmes électroniques BES*.

Les mesures présentent des exemples de pièces justificatives pour montrer la documentation et la mise en œuvre de l'exigence. Ces mesures servent à fournir des conseils aux entités sur ce qui peut constituer des dossiers de conformité acceptables et ne devraient pas être considérées comme une liste exhaustive.

Dans l'ensemble des normes, sauf indication particulière, les éléments présentés à la section Exigences et mesures sous forme de liste à puces sont liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances de systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes de DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

Colonnes « Systèmes visés » des tableaux :

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. Le SDT CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- **Systèmes électroniques BES à impact élevé** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes électroniques BES à impact élevé à connectivité par lien commuté** – Désigne uniquement les *systèmes électroniques BES* à impact élevé à connectivité par lien commuté.
- **Systèmes électroniques BES à impact élevé à connectivité externe routable** – Désigne uniquement les *systèmes électroniques BES* à impact élevé à connectivité externe routable. Exclut les *actifs électroniques* des *systèmes électroniques BES* auxquels on ne peut avoir accès directement par connectivité externe routable.
- **Systèmes électroniques BES à impact moyen** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes électroniques BES à impact moyen situés aux centres de contrôle** – Désigne uniquement les *systèmes électroniques BES* à impact moyen situés dans un centre de contrôle.
- **Systèmes électroniques BES à impact moyen à connectivité par lien commuté** – Désigne uniquement les *systèmes électroniques BES* à impact moyen à connectivité par lien commuté.
- **Systèmes électroniques BES à impact moyen à connectivité externe routable** – Désigne uniquement les *systèmes électroniques BES* à impact moyen à connectivité externe routable. Exclut les *actifs électroniques* des *systèmes électroniques BES* auxquels on ne peut avoir accès directement par connectivité externe routable.
- **Actifs électroniques protégés (PCA)** – Désigne tout *actif électronique protégé* associé à un *système électronique BES* à impact élevé ou moyen visé.
- **Points d'accès électronique (EAP)** – Désigne les *points d'accès électronique* associés à un *système électronique BES* à impact élevé ou moyen visé.

B. Exigences et mesures

E1. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du *tableau* E1 (CIP-005-5) – *Périmètre de sécurité électronique*. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation et exploitation du jour même]*

M1. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-005-5) – *Périmètre de sécurité électronique*, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-005-5) – Périmètre de sécurité électronique			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.1	*Systèmes électroniques BES* à impact élevé et leurs : • PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : • PCA associés.	Tous les *actifs électroniques* applicables qui sont reliés à un réseau au moyen d'un protocole routable doivent être situés à l'intérieur d'un ESP défini.	Exemple non limitatif de pièce justificative : liste de tous les ESP avec tous les *actifs électroniques* applicables à identifiant unique qui sont reliés au moyen d'un protocole routable dans chaque ESP.

Tableau E1 (CIP-005-5) – Périmètre de sécurité électronique			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.2	*Systèmes électroniques BES* à impact élevé à *connectivité externe routable* et leurs : • PCA associés. *Systèmes électroniques BES* à impact moyen à connectivité externe routable et leurs : • PCA associés.	Toute *connectivité externe routable* doit s'effectuer par l'intermédiaire d'un *point d'accès électronique* (EAP) identifié.	Exemples non limitatifs de pièces justificatives : schémas de réseau montrant tous les chemins de communication routables externes et les EAP identifiés.
1.3	*Points d'accès électronique* associés à des *systèmes électroniques BES* à impact élevé. *Points d'accès électronique* associés à des *systèmes électroniques BES* à impact moyen.	Exiger des autorisations pour les accès entrants et sortants, incluant la raison pour donner l'accès, et refuser tout autre accès par défaut.	Exemple non limitatif de pièce justificative : liste de règles (coupe-feu, liste des droits d'accès, etc.) démontrant que seuls les accès autorisés sont permis et que chaque règle d'accès est justifiée, documentation à l'appui.

Tableau E1 (CIP-005-5) – Périmètre de sécurité électronique			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.4	*Systèmes électroniques BES* à impact élevé à *connectivité par lien commuté* et leurs : • PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité par lien commuté* et leurs : • PCA associés.	Lorsque techniquement faisable, effectuer l'authentification lors de l'établissement de la *connectivité par lien commuté* avec les *actifs électroniques* applicables.	Exemple non limitatif de pièce justificative : processus documenté décrivant la méthode utilisée par l'entité responsable pour assurer l'authentification des accès effectués via chaque connexion par lien commuté.
1.5	*Points d'accès électronique* associés à des *systèmes électroniques BES* à impact élevé. *Points d'accès électronique* associés à des *systèmes électroniques BES* à impact moyen situés dans des *centres de contrôle*.	Avoir un ou plusieurs moyens de détection des communications entrantes et sortantes malveillantes avérées ou présumées.	Exemple non limitatif de pièce justificative : documentation attestant la mise en œuvre de moyens de détection des communications malveillantes (système de détection des intrusions, pare-feu au niveau de la couche application, etc.).

E2. Chaque entité responsable qui autorise un *accès distant interactif* à des *systèmes électroniques BES* doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, lorsque techniquement faisable, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-005-5) – Gestion des *accès distants interactifs*. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation et exploitation du jour même]*

M2. Les pièces justificatives doivent comprendre les processus documentés qui, collectivement, traitent de chacune des parties d'exigence applicables du tableau E2 (CIP-005-5) – Gestion des *accès distants interactifs*, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-005-5) – Gestion des accès distants interactifs			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et leurs : • PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : • PCA associés.	Utiliser un *système intermédiaire* de façon à ce que l'*actif électronique* à initiant l'*accès distant interactif* n'ait pas directement accès à l'*actif électronique* visé.	Exemples non limitatifs de pièces justificatives : schémas de réseau ou documents sur l'architecture.
2.2	*Systèmes électroniques BES* à impact élevé et leurs : • PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : • PCA associés.	Pour toutes les sessions d'*accès distant interactif*, utiliser un cryptage se terminant à un *système intermédiaire*.	Exemple non limitatif de pièce justificative : documents sur l'architecture qui indiquent les points où commence et où se termine le cryptage.

Tableau E2 (CIP-005-5) – Gestion des accès distants interactifs			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.3	*Systèmes électroniques BES* à impact élevé et leurs : • PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : • PCA associés.	Exiger l'authentification multifactorielle pour toutes les sessions d'*accès distant interactif*.	Exemple non limitatif de pièce justificative : documents sur l'architecture décrivant les facteurs d'authentification utilisés. Exemples non limitatifs de facteurs d'authentification : • ce que l'utilisateur sait, comme un mot de passe ou un NIP. Ceci n'inclut pas les identifiants d'utilisateur ; • ce que l'utilisateur possède, comme un jeton, un certificat numérique ou une carte intelligente ; ou • une caractéristique biométrique de l'utilisateur, comme ses empreintes digitales ou le motif de son iris.

C. Conformité

1. Processus de surveillance de la conformité :

1.1. Responsable de la surveillance de l'application des normes :

L'entité régionale joue le rôle de responsable de la surveillance de l'application des normes (CEA), à moins que l'entité concernée soit détenue, exploitée ou contrôlée par l'entité régionale. Dans de tels cas, le rôle de CEA est confié à l'ERO, à une entité régionale approuvée par la FERC ou à un autre organisme gouvernemental pertinent.

1.2. Conservation des pièces justificatives :

Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces justificatives afin de démontrer sa conformité. Dans les cas où la période de conservation des pièces justificatives indiquée est plus courte que le temps écoulé depuis le dernier audit, le CEA peut demander à l'entité de fournir d'autres pièces justificatives pour montrer qu'elle était conforme pendant la période complète écoulée depuis le dernier audit.

L'entité responsable doit conserver les données ou pièces justificatives attestant de sa conformité de la façon indiquée ci-après, à moins que son CEA lui demande de conserver certains documents plus longtemps dans le cadre d'une enquête :

- Chaque entité responsable doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité responsable est jugée non conforme, elle doit conserver l'information relative à cette non-conformité jusqu'à ce que les correctifs aient été appliqués et approuvés ou pendant la période indiquée ci-dessus, selon la durée la plus longue.
- Le CEA doit conserver les derniers dossiers d'audit ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Processus de surveillance et d'évaluation de la conformité :

- Audits de conformité
- Déclarations sur la conformité
- Contrôles ponctuels
- Enquêtes sur les non-conformités
- Déclarations volontaires
- Plaintes

1.4. Autres informations sur la conformité :

- Aucune

Annexe QC-CIP-005
Dispositions particulières de la norme CIP-005-5 applicables au Québec

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son 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 aura préséance.

A. Introduction

1. **Titre :** Cybersécurité — Périmètres de sécurité électronique

2. **Numéro :** CIP-005-5

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

   Entités fonctionnelles

   Aucune disposition particulière

   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 :

   - Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur 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 201x

   5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 201x

   5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : xx mois 201x

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. **Processus de surveillance de la conformité**

   1.1. Responsable de la surveillance de l'application des normes

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et d'évaluation de la conformité

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	Xx mois 201x	Nouvelle annexe	Nouvelle

A. Introduction

1. Titre : Cybersécurité – Sécurité physique des systèmes électroniques BES

2. Numéro : CIP-006-5

3. Objet : Gérer l'accès physique aux *systèmes électroniques BES* en établissant un plan de sécurité physique afin de protéger les *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou une instabilité dans le BES.

4. Applicabilité :

4.1. Entités fonctionnelles : Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

4.1.1 Responsable de l'équilibrage

4.1.2 Distributeur qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du BES :

4.1.2.1 Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :

4.1.2.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.1.2.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.1.2.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

4.2. Installations : Dans le contexte des exigences de la présente norme, les *installations*, systèmes et équipements suivants détenus par chaque entité responsable indiquée à la section 4.1 sont ceux auxquels ces exigences sont applicables. Dans le cas des exigences de cette norme qui visent un type particulier d'*installations*, de système ou d'équipements, ou un sous-ensemble d'*installations*, de systèmes ou d'équipements, ceux-ci sont précisés explicitement.

4.2.1 Distributeur : Un ou plusieurs des *installations*, systèmes et équipements suivants détenus par le distributeur pour la protection ou la remise en charge du BES :

4.2.1.1 Chaque système de DSF ou de DST qui :

4.2.1.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.2.1.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.4 Chaque chemin de démarrage et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

4.2.3 Exemptions : Sont exemptés de la norme CIP-006-5 :

4.2.3.1 Les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire ;

4.2.3.2 les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électroniques* distincts ;

4.2.3.3 les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme à la norme CFR 10, section 73.54 ;

4.2.3.4 dans le cas des distributeurs, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus ;

4.2.3.5 les entités responsables qui déterminent qu'elles n'ont pas de systèmes électroniques BES catégorisés comme impact élevé ou impact moyen en conformité avec le processus d'identification et de catégorisation de la CIP-002-5.

5. Dates d'entrée en vigueur

1. **24 mois minimum –** La norme CIP-006-5 entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.
2. Dans les juridictions où aucune approbation réglementaire n'est requise, la norme CIP-006-5 entrera en vigueur le premier jour du neuvième trimestre civil suivant l'approbation par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte

La norme CIP-006-5 fait partie d'une série de normes CIP sur la cybersécurité. La norme CIP-002-5 exige l'identification et la catégorisation initiales des *systèmes électroniques BES*. Les normes CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 et CIP-011-1 exigent un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*. Cette série de normes CIP est appelée « version 5 des normes CIP sur la cybersécurité ».

La plupart des exigences commencent ainsi : « *Chaque entité responsable doit mettre en œuvre un ou plusieurs [processus, plans, etc.] documentés qui correspondent à toutes les parties d'exigence applicables du tableau [référence au tableau].* » Le tableau en référence précise les éléments qui doivent être inclus dans les procédures pour le thème commun de l'exigence.

Le SDT a intégré à la présente norme une reconnaissance à l'effet que certaines exigences ne devraient pas mettre l'accent sur les cas individuels de défaillance comme seul motif d'infraction à la norme. En particulier, le SDT a intégré une approche visant à habiliter l'industrie à identifier, à évaluer et à corriger les lacunes dans la mise en œuvre de certaines exigences. L'intention est de changer la manière de considérer les infractions dans ces exigences, de sorte qu'il ne s'agisse plus de

savoir *si* une lacune existe, mais plutôt d'identifier, d'évaluer et de corriger les lacunes. Ceci est présenté dans ces exigences en modifiant la notion de « mise en œuvre » de la façon suivante :

> Chaque entité responsable doit mettre en œuvre**, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes…**

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité devrait inclure autant qu'elle le juge nécessaire à leurs processus documentés, pourvu que les exigences pertinentes soient couvertes. Les processus documentés eux-mêmes n'ont pas à intégrer la démarche « détecter, évaluer et corriger les lacunes » décrite au paragraphe précédent, car cette démarche est liée à la manière de mettre en œuvre les processus documentés et pourrait être réalisée par d'autres mesures de contrôle ou de gestion de la conformité.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », lorsque cela a du sens et est communément compris. Par exemple, les processus documentés qui décrivent une réponse sont généralement appelés « plans » (plan d'action en cas d'incident, plan de rétablissement, etc.). De plus, un plan de sécurité peut décrire une approche comportant plusieurs procédures couvrant un thème étendu.

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont un exemple trouvé dans les normes. La mise en œuvre complète des normes CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

Les entités responsables peuvent mettre en œuvre des moyens communs qui répondent aux besoins de plusieurs *systèmes électroniques BES* à impact élevé et moyen. Par exemple, un même programme de formation pourrait répondre aux exigences en formation du personnel de plusieurs *systèmes électroniques BES*.

Les mesures présentent des exemples de pièces justificatives pour montrer la documentation et la mise en œuvre de l'exigence. Ces mesures servent à fournir des conseils aux entités sur ce qui peut constituer des dossiers de conformité acceptables et ne devraient pas être considérées comme une liste exhaustive.

Dans l'ensemble des normes, sauf indication particulière, les éléments présentés à la section Exigences et mesures sous forme de liste à puces sont liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à

300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances de systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes de DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

Colonnes « Systèmes visés » des tableaux

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. Le SDT CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- **Systèmes électroniques BES à impact élevé** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes électroniques BES à impact moyen** – Désigne les s*ystèmes électroniques BES* classés dans la catégorie « impact moyen », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes électroniques BES à impact moyen sans connectivité externe routable** – Désigne uniquement les *systèmes électroniques BES* à impact moyen sans *connectivité externe routable*.
- **Systèmes électroniques BES à impact moyen à connectivité externe routable** – Désigne uniquement les *systèmes électroniques BES* à impact moyen à *connectivité externe routable*. Exclut les *actifs électroniques* des *systèmes électroniques BES* auxquels on ne peut avoir accès directement par *connectivité externe routable*.
- **Systèmes de contrôle ou de surveillance des accès électroniques (EACMS)** – Désigne tout *système de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d'authentification, et systèmes de surveillance de registre d'événement et d'alerte.
- **Systèmes de contrôle des accès physiques (PACS)** – Désigne tout *système de contrôle des accès physique*s associé à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.
- **Actifs électroniques protégés (PCA)** – Désigne tout *actif électronique protégé* associé à un *système électronique BES* à impact élevé ou moyen visé.

- **Matériel et dispositifs installés localement au périmètre de sécurité physique** – Désigne le matériel et les dispositifs (p. ex. détecteurs de mouvement, mécanismes de verrouillage électroniques ou lecteurs de carte d'accès) installés localement au *périmètre de sécurité physique* associé à un *système électronique BES* à impact élevé ou moyen à *connectivité externe routable* visé, mais qui ne contiennent pas et n'enregistrent pas d'information servant au contrôle des accès, et qui n'assurent pas de façon autonome l'authentification des accès. Ce matériel et ces dispositifs sont par définition exclus des *systèmes de contrôle des accès physiques*.

B. Exigences et mesures

E1. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs plans de sécurité physique documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP 006 5) – Plan de sécurité physique. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification à long terme et exploitation du jour même]*

M1. Les pièces justificatives doivent comprendre chacun des plans de sécurité physique documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP 006 5) – Plan de sécurité physique, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre selon la colonne Mesures du tableau.

Tableau E1 (CIP-006-5) – Plan de sécurité physique			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.1	*Systèmes électroniques BES* à impact moyen sans *connectivité externe routable*. *Systèmes de contrôle des accès physiques* (PACS) associés à : • des *systèmes électroniques BES* à impact élevé, ou • des *systèmes électroniques BES* à impact moyen à *connectivité externe routable*.	Définir des mesures opérationnelles ou administratives permettant de restreindre l'accès physique.	Exemple non limitatif de pièce justificative : documentation attestant que des mesures opérationnelles ou administratives sont en place.

Tableau E1 (CIP-006-5) – Plan de sécurité physique			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.2	*Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés, et 2. PCA associés.	Utiliser au moins un mécanisme de contrôle des accès physiques permettant l'accès physique sans accompagnement à chaque *périmètre de sécurité physique* visé aux seules personnes ayant un accès physique autorisé sans accompagnement.	Exemple non limitatif de pièce justificative : des énoncés dans le plan de sécurité physique qui décrivent chaque *périmètre de sécurité physique* et comment les accès physiques sans accompagnement y sont contrôlés par au moins un mécanisme ainsi que des preuves qui attestent que seules les personnes autorisées y ont un accès physique sans accompagnement, telles que des listes de personnes autorisées et les registres d'accès correspondants.
1.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PCA associés.	Lorsque techniquement faisable, utiliser au moins deux mécanismes de contrôle des accès physiques différents (ce qui n'exige pas nécessairement deux systèmes de contrôle complètement indépendants) qui, ensemble, permettent l'accès physique sans accompagnement aux *périmètres de sécurité physique* aux seules personnes ayant un accès physique autorisé sans accompagnement.	Exemple non limitatif de pièce justificative : des énoncés dans le plan de sécurité physique qui décrivent les *périmètres de sécurité physique* et comment les accès physiques sans accompagnement sont contrôlés par au moins deux mécanismes différents ainsi que des preuves qui attestent que seules les personnes autorisées y ont un accès physique sans accompagnement, telles que des listes de personnes autorisées et les registres d'accès correspondants.

Tableau E1 (CIP-006-5) – Plan de sécurité physique			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.4	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PCA associés.	Surveiller les accès non autorisés au point d'accès physique d'un *périmètre de sécurité physique*.	Exemple non limitatif de pièce justificative : documentation des mécanismes de surveillance des accès non autorisé à un point d'accès physique d'un *périmètre de sécurité physique*.

Tableau E1 (CIP-006-5) – Plan de sécurité physique			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.5	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PCA associés.	Émettre une alarme ou une alerte en réponse à la détection d'un accès non autorisé au point d'accès physique d'un *périmètre de sécurité physique* au personnel désigné dans le plan d'intervention en cas d'*incident de cybersécurité* lié au BES, dans les 15 minutes suivant la détection.	Exemple non limitatif de pièce justificative : des énoncés dans le plan de sécurité physique décrivant le processus d'émission d'une alarme ou d'une alerte en réponse à un accès non autorisé au point d'accès physique d'un *périmètre de sécurité physique* et des pièces justificatives additionnelles qui attestent que l'alarme ou l'alerte a été émise et communiquée conformément au plan d'intervention en cas d'*incident de cybersécurité* lié au BES, telles que des journaux d'alarmes ou d'alertes électroniques ou manuelles ou des registres de communications par cellulaire ou téléavertisseur, ou d'autres pièces justificatives qui documentent que l'alarme ou l'alerte a été généré et communiquée.
1.6	*Systèmes de contrôle des accès physiques* (PACS) associés à : • des *systèmes électroniques BES* à impact élevé, ou • des *systèmes électroniques BES* à impact moyen à *connectivité externe routable*.	Surveiller chaque *système de contrôle des accès physiques* pour les accès physiques non autorisés à un *système de contrôle des accès physiques*.	Exemple non limitatif de pièce justificative : documentation des mécanismes de surveillance pour les accès physiques non autorisés à un PACS.

Tableau E1 (CIP-006-5) – Plan de sécurité physique			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.7	*Systèmes de contrôle des accès physiques* (PACS) associés à : • des *systèmes électroniques BES* à impact élevé, ou • des *systèmes électroniques BES* à impact moyen à *connectivité externe routable*.	Émettre une alarme ou une alerte en réponse à la détection d'un accès physique non autorisé à un *système de contrôle des accès physiques* au personnel désigné dans le plan d'intervention en cas d'*incident de cybersécurité* lié au BES dans les 15 minutes suivant la détection.	Exemple non limitatif de pièce justificative : des énoncés dans le plan de sécurité physique précisant qu'une alarme ou une alerte est émise en réponse à la détection d'un accès physique non autorisé à un *système de contrôle des accès physiques* et des pièces justificatives additionnelles qui attestent que l'alarme ou l'alerte a été émise et communiquée conformément au plan d'intervention en cas d'*incident de cybersécurité* lié au BES, telles que des journaux d'alarmes ou d'alertes ou des registres de communications par cellulaire ou téléavertisseur, ou d'autres pièces justificatives qui attestent que l'alarme ou l'alerte a été généré et communiquée.

Tableau E1 (CIP-006-5) – Plan de sécurité physique			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.8	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 3. EACMS associés ; et 4. PCA associés.	Consigner (par des moyens automatisés ou par du personnel qui contrôle l'entrée) l'accès de chaque personne ayant un accès physique autorisé sans accompagnement dans chaque *périmètre de sécurité physique* avec l'information permettant d'identifier la personne, ainsi que la date et l'heure de l'accès.	Exemple non limitatif de pièce justificative : des énoncés dans le plan de sécurité physique décrivant la consignation et l'enregistrement des accès physiques à chaque *périmètre de sécurité physique* et des pièces justificatives additionnelles pour démontrer que cette consignation a été mise en œuvre, telles que des registres d'accès physique aux *périmètres de sécurité physique* qui montrent la personne ainsi que la date et l'heure de l'accès au *périmètre de sécurité physique*.
1.9	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PCA associés.	Conserver les registres d'accès physique des personnes ayant un accès physique autorisé sans accompagnement à un *périmètre de sécurité physique* pendant au moins 90 jours civils.	Exemple non limitatif de pièce justificative : documents datés, comme des registres des accès physiques aux *périmètres de sécurité physique* qui montrent la date et l'heure de l'accès au *périmètre de sécurité physique*.

E2. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs programmes de contrôle des visiteurs documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP 006 5) – Programme de contrôle des visiteurs. *[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation du jour même]*

M2. Les pièces justificatives doivent comprendre un ou plusieurs programmes de contrôle des visiteurs documentés qui, collectivement, comprennent toutes les parties d'exigences applicables du tableau E2 (CIP 006 5) – Programme de contrôle des visiteurs, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre selon la colonne Mesures du tableau.

Tableau E2 (CIP-006-5) – Programme de contrôle des visiteurs			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PCA associés.	Exiger un accompagnement continu des visiteurs (personnes à qui l'accès est accordé, mais n'ayant pas un accès physique autorisé sans accompagnement) à l'intérieur de chaque *périmètre de sécurité physique*, sauf dans des *circonstances CIP exceptionnelles*.	Exemple non limitatif de pièce justificative : des énoncés dans un programme de contrôle des visiteurs exigeant un accompagnement continu des visiteurs à l'intérieur des *périmètres de sécurité physique* ainsi que des pièces justificatives additionnelles attestant que cette mesure a été mise en oeuvre, telles que des registres de visiteurs.
2.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PCA associés.	Exiger la consignation manuelle ou automatique de l'entrée de tout visiteur dans un *périmètre de sécurité physique*, et sa sortie, y compris la date et l'heure de sa première entrée et de sa dernière sortie, le nom du visiteur et le nom de son répondant, sauf dans des *circonstances CIP exceptionnelles*.	Exemple non limitatif de pièce justificative : des énoncés dans un programme de contrôle des visiteurs qui exige un accompagnement continu des visiteurs à l'intérieur des *périmètres de sécurité physique* et des pièces justificatives additionnelles pour démontrer que cette mesure a été mise en oeuvre, telles que des registres de visiteurs datés renfermant les données pertinentes.

Tableau E2 (CIP-006-5) – Programme de contrôle des visiteurs			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.3	*Systèmes électroniques BES* à impact élevé et leurs : 3. EACMS associés ; et 4. PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; et 2. PCA associés.	Conserver les registres des visiteurs durant au moins 90 jours civils.	Exemple non limitatif de pièce justificative : documentation attestant que les registres des visiteurs ont été conservés durant au moins 90 jours civils.

E3. Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés de maintenance et d'essai des *systèmes de contrôle des accès physiques* qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E3 (CIP 006 5) – Programme de maintenance et d'essais. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification à long terme]*

M3. Les pièces justificatives doivent comprendre tous les programmes documentés de maintenance et d'essai des *systèmes de contrôle des accès physiques* qui, collectivement, comprennent toutes les exigences pertinentes du tableau E3 (CIP 006 5) – Programme de maintenance et d'essais, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre selon la colonne Mesures du tableau.

Tableau E3 (CIP-006-5) – Programme de maintenance et d'essais des systèmes de contrôle des accès physiques			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes de contrôle des accès physiques* (PACS) associés à : • des *systèmes électroniques BES* à impact élevé, ou • des *systèmes électroniques BES* à impact moyen à *connectivité externe routable*. Matériel et dispositifs installés localement aux *périmètres de sécurité physique* associés à : • des *systèmes électroniques BES* à impact élevé, ou • des *systèmes électroniques BES* à impact moyen à *connectivité externe routable*.	La maintenance et l'essai de chaque *système de contrôle des accès physiques* et de chaque composant matériel ou dispositif installé localement au *périmètre de sécurité physique* au moins une fois tous les 24 mois civils pour s'assurer qu'ils fonctionnent correctement.	Exemple non limitatif de pièce justificative : un programme de maintenance et d'essai exigeant l'essai, au moins une fois tous les 24 mois civils, de chaque *système de contrôle des accès physiques* et du matériel ou des dispositifs installés localement à un *périmètre de sécurité physique* visé, et des pièces justificatives additionnelles pour démontrer que l'essai a été effectué, telles que des registres de maintenance datés, ou tout autre document montrant que la maintenance et l'essai ont été effectués pour chaque système et dispositif visés au moins une fois tous les 24 mois civils.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable de la surveillance de l'application des normes

L'entité régionale joue le rôle de responsable de la surveillance de l'application des normes (CEA), à moins que l'entité concernée soit détenue, exploitée ou contrôlée par l'entité régionale. Dans de tels cas, le rôle de CEA est confié à l'ERO, à une entité régionale approuvée par la FERC ou à un autre organisme gouvernemental pertinent.

1.2. Conservation des pièces justificatives

Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces justificatives afin de démontrer sa conformité. Dans les cas où la période de conservation des pièces justificatives indiquée est plus courte que le temps écoulé depuis le dernier audit, le CEA peut demander à l'entité de fournir d'autres pièces justificatives pour montrer qu'elle était conforme pendant la période complète écoulée depuis le dernier audit.

L'entité responsable doit conserver les données ou pièces justificatives attestant de sa conformité de la façon indiquée ci-après, à moins que son CEA lui demande de conserver certains documents plus longtemps dans le cadre d'une enquête :

- Chaque entité responsable doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité responsable est jugée non conforme, elle doit conserver l'information relative à cette non-conformité jusqu'à ce que les correctifs aient été appliqués et approuvés ou pendant la période indiquée ci-dessus, selon la durée la plus longue.
- Le CEA doit conserver les derniers dossiers d'audit ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Processus de surveillance et d'évaluation de la conformité

- Audits de conformité
- Déclarations sur la conformité
- Contrôles ponctuels
- Enquêtes sur les non-conformités
- Déclarations volontaires
- Plaintes

1.4. Autres informations sur la conformité

- Aucune

Annexe QC-CIP-006-5
Dispositions particulières de la norme CIP-006-5 applicables au Québec

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son 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 aura préséance.

A. Introduction

1. **Titre :** Cybersécurité — Sécurité physique des systèmes électroniques BES

2. **Numéro :** CIP-006-5

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

Entités fonctionnelles

Aucune disposition particulière

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 :

- Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur 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 201x

5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 201x

5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : xx mois 201x

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. **Processus de surveillance de la conformité**

1.1. Responsable de la surveillance de l'application des normes

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et d'évaluation de la conformité

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	Xx mois 201x	Nouvelle annexe	Nouvelle

A. Introduction

1. Titre : Cybersécurité — Gestion de la sécurité des systèmes

2. Numéro : CIP-007-5

3. Objet : Gérer la sécurité des systèmes en établissant des exigences techniques, opérationnelles et administratives particulières afin de protéger les *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou une instabilité dans le BES.

4. Applicabilité :

4.1. Entités fonctionnelles : Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

4.1.1 Responsable de l'équilibrage

4.1.2 Distributeur qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du BES :

4.1.2.1 Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :

4.1.2.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.1.2.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.1.2.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

4.2. **Installations :** Dans le contexte des exigences de la présente norme, les *installations*, systèmes et équipements suivants détenus par chaque entité responsable indiquée à la section 4.1 sont ceux auxquels ces exigences sont applicables. Dans le cas des exigences de cette norme qui visent un type particulier d'*installations*, de système ou d'équipements, ou un sous-ensemble d'*installations*, de systèmes ou d'équipements, ceux-ci sont précisés explicitement.

4.2.1 Distributeur : Un ou plusieurs des *installations*, systèmes et équipements suivants détenus par le distributeur pour la protection ou la remise en charge du BES :

4.2.1.1 Chaque système de DSF ou de DST qui :

4.2.1.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.2.1.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

4.2.3 Exemptions : Sont exemptés de la norme CIP-007-5 :

4.2.3.1 Les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire ;

4.2.3.2 les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électroniques* distincts ;

4.2.3.3 les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme à la norme CFR 10, section 73.54 ;

4.2.3.4 dans le cas des distributeurs, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus ;

4.2.3.5 les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* catégorisés comme impact élevé ou impact moyen en conformité avec le processus d'identification et de catégorisation de la CIP-002-5.

5. Dates d'entrée en vigueur

1. **24 mois minimum –** La norme CIP-007-5 entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.
2. Dans les juridictions où aucune approbation réglementaire n'est requise, la norme CIP-007-5 entrera en vigueur le premier jour du neuvième trimestre civil suivant l'approbation par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte :

La norme CIP-007-5 fait partie d'une série de normes CIP sur la cybersécurité. La norme CIP-002-5 exige l'identification et la catégorisation initiales des *systèmes électroniques BES*. Les normes CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 et CIP-011-1 exigent un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*. Cette série de normes CIP est appelée « version 5 des normes CIP sur la cybersécurité ».

La plupart des exigences commencent ainsi : « Chaque entité responsable doit mettre en œuvre un ou plusieurs [processus, plans, etc.] documentés qui correspondent à toutes les parties d'exigence applicables du tableau [référence au tableau]. » Le tableau en référence précise les éléments qui doivent être inclus dans les procédures pour le thème commun de l'exigence.

Le SDT a intégré à la présente norme une reconnaissance à l'effet que certaines exigences ne devraient pas mettre l'accent sur les cas individuels de défaillance comme seul motif d'infraction à la norme. En particulier, le SDT a intégré une approche visant à habiliter l'industrie à identifier, à évaluer et à corriger les lacunes dans la mise en œuvre de certaines exigences. L'intention est de changer la manière

de considérer les infractions dans ces exigences, de sorte qu'il ne s'agisse plus de savoir *si* une lacune existe, mais plutôt d'identifier, d'évaluer et de corriger les lacunes. Ceci est présenté dans ces exigences en modifiant la notion de « mise en œuvre » de la façon suivante :

> Chaque entité responsable doit mettre en œuvre**, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes…**

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité devrait inclure autant qu'elle le juge nécessaire à leurs processus documentés, pourvu que les exigences pertinentes soient couvertes. Les processus documentés eux-mêmes n'ont pas à intégrer la démarche « détecter, évaluer et corriger les lacunes » décrite au paragraphe précédent, car cette démarche est liée à la manière de mettre en œuvre les processus documentés et pourrait être réalisée par d'autres mesures de contrôle ou de gestion de la conformité.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », lorsque cela a du sens et est communément compris. Par exemple, les processus documentés qui décrivent une réponse sont généralement appelés « plans » (plan d'action en cas d'incident, plan de rétablissement, etc.). De plus, un plan de sécurité peut décrire une approche comportant plusieurs procédures couvrant un thème étendu.

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont un exemple trouvé dans les normes. La mise en œuvre complète des normes CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

Les entités responsables peuvent mettre en œuvre des moyens communs qui répondent aux besoins de plusieurs *systèmes électroniques BES* à impact élevé et moyen. Par exemple, un même programme de formation pourrait répondre aux exigences en formation du personnel de plusieurs *systèmes électroniques BES*.

Les mesures présentent des exemples de pièces justificatives pour montrer la documentation et la mise en œuvre de l'exigence. Ces mesures servent à fournir des conseils aux entités sur ce qui peut constituer des dossiers de conformité acceptables et ne devraient pas être considérées comme une liste exhaustive.

Dans l'ensemble des normes, sauf indication particulière, les éléments présentés à la section Exigences et mesures sous forme de liste à puces sont liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances de systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes de DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

Colonnes « Systèmes visés » des tableaux

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. Le SDT CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- **Systèmes électroniques BES à impact élevé** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes électroniques BES à impact moyen** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes électroniques BES à impact moyen situés aux centres de contrôle –** Désigne uniquement les *systèmes électroniques BES* à impact moyen situés aux *centres de contrôle*.
- **Systèmes électroniques BES à impact moyen à connectivité externe routable** – Désigne uniquement les *systèmes électroniques BES* à impact moyen à *connectivité externe routable*. Exclut les *actifs électroniques* des *systèmes électroniques BES* auxquels on ne peut avoir accès directement par *connectivité externe routable*.
- **Systèmes de contrôle ou de surveillance des accès électroniques (EACMS)** – Désigne tout *système de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d'authentification, et systèmes de surveillance de registre d'événement et d'alerte.
- **Systèmes de contrôle des accès physiques (PACS)** – Désigne tout *système de contrôle des accès physique*s associé à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.
- **Actifs électroniques protégés (PCA)** – Désigne tout *actif électronique protégé* associé à un *système électronique BES* à impact élevé ou moyen visé.

B. Exigences et mesures

E1. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-007-5) – Ports et services. *[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation du jour même]*

M1. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-007-5) – Ports et services, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-007-5) – Ports et services			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Lorsque techniquement faisable, activer uniquement les ports logiques accessibles par le réseau qui sont jugés nécessaires par l'entité responsable, y compris les plages de ports ou de services qui sont nécessaires pour la prise en charge de ports dynamiques. Si un dispositif ne permet pas la désactivation ou la restriction de ses ports logiques, tous les ports ouverts sont considérés comme nécessaires.	Exemples non limitatifs de pièces justificatives : • documentation établissant la nécessité de tous les ports activés de tous les *actifs électroniques* et *points d'accès électronique* visés, pris individuellement ou collectivement ; • listes des ports à l'écoute des *actifs électroniques*, pris individuellement ou collectivement, provenant des fichiers de configuration des dispositifs, du résultat de commandes telles que netstat ou de balayages réseau des ports ouverts ; ou • fichiers de configuration des pare-feu de type hôte ou de tout autre mécanisme intégré au matériel qui n'autorisent l'accès qu'aux ports nécessaires et qui le refusent à tous les autres.

Tableau E1 (CIP-007-5) – Ports et services			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.2	*Systèmes électroniques BES* à impact élevé *Systèmes électroniques BES* à impact moyen de *centres de contrôle*	Empêcher l'utilisation de ports d'entrée-sortie physiques non nécessaires utilisés pour la connectivité de réseau, les commandes pupitre ou les supports d'information amovibles.	Exemple non limitatif de pièce justificative : documentation indiquant le type de protection assurée pour les ports d'entrée-sortie physiques – soit logique (configuration du système), soit physique (verrouillage ou signalisation).

E2. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-007-5) – Gestion des rustines de sécurité. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]*

M2. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-007-5) – Gestion des rustines de sécurité, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-007-5) – Gestion des rustines de sécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et : 1. EACMS associés ; 2. PACS associés; et 3. PCA associés.	Un processus de gestion des rustines portant sur le suivi, l'évaluation et l'installation des rustines de cybersécurité pour les *actifs électroniques* visés. Le suivi comprend la désignation de la ou des sources que l'entité responsable utilise pour faire le suivi de la publication de rustines de cybersécurité destinées aux *actifs électroniques* visés qui sont actualisables et pour lesquels il existe une source de rustines.	Exemples non limitatifs de pièces justificatives : documentation d'un processus de gestion des rustines et documentation ou listes de sources qui sont utilisées pour le suivi visant chacun des *systèmes électroniques BES* ou des *actifs électroniques BES*.

Tableau E2 (CIP-007-5) – Gestion des rustines de sécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Au moins une fois tous les 35 jours civils, évaluer l'applicabilité des rustines de sécurité publiées par la ou les sources indiquées à la partie 2.1 depuis l'évaluation précédente.	Exemple non limitatif de pièce justificative : une évaluation effectuée ou citée par une entité responsable ou réalisée en son nom et portant sur les rustines de sécurité publiées par les sources documentées, et ce, au moins tous les 35 jours civils.

Tableau E2 (CIP-007-5) – Gestion des rustines de sécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Pour les rustines jugées applicables selon la partie 2.2, prendre une des mesures suivantes dans les 35 jours civils après que l'évaluation soit terminée : • appliquer les rustines applicables, • créer un plan de mitigation daté ou • réviser un plan de mitigation existant. Les plans de mitigation doivent comprendre les mesures que l'entité responsable compte prendre pour mitiger les vulnérabilités visées par chaque rustine de sécurité, ainsi qu'un délai de mise en œuvre des mesures.	Exemples non limitatifs de pièces justificatives : • Enregistrements d'installation des rustines (p. ex. rapport exporté d'un outil automatisé de gestion des rustines fournissant la date d'installation, validation de la version du logiciel des composants du *système électronique BES* ou exportation d'un registre indiquant que le logiciel a été installé) ; ou • plan daté indiquant à quel moment et de quelle façon la vulnérabilité sera corrigée, qui documente les mesures que l'entité responsable compte prendre pour mitiger les vulnérabilités visées par la rustine de sécurité et qui précise un délai d'exécution des mesures de mitigation.

Tableau E2 (CIP-007-5) – Gestion des rustines de sécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.4	*Systèmes électroniques BES* à impact élevé et : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et : 1. EACMS associés ; 2. PACS associés ; 3. PCA associés.	Pour chaque plan de mitigation créé ou mis à jour à la partie 2.3, mettre le plan en œuvre dans le délai précisé, à moins qu'une révision du plan ou un prolongement du délai indiqué à la partie 2.3 ne soit approuvé par le *cadre supérieur CIP* ou son délégué.	Exemple non limitatif de pièce justificative : dossiers de mise en œuvre des plans de mitigation.

E3. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E3 (CIP-007-5) – Protection contre les programmes malveillants. *[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation du jour même]*

M3. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E3(CIP-007-5) – Protection contre les programmes malveillants ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E3 (CIP-007-5) – Protection contre les programmes malveillants			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Utiliser une ou des méthodes pour bloquer, détecter ou prévenir les programmes malveillants.	Exemple non limitatif de pièce justificative : suivis de la mise en œuvre de ces méthodes par l'entité responsable (au moyen des logiciels antivirus habituels, du renforcement des systèmes, de politiques, etc.).

Tableau E3 (CIP-007-5) – Protection contre les programmes malveillants			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Mitiger la menace des programmes malveillants détectés.	Exemples non limitatifs de pièces justificatives : • registres des processus d'intervention en cas de détection de programmes malveillants ; • suivis de la mise en œuvre de ces processus lorsque des programmes malveillants sont détectés.
3.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Pour les méthodes indiquées à la partie 3.1 qui utilisent des signatures ou des séquences de code, avoir un processus de mise à jour des signatures et des séquences de code. Le processus doit traiter de l'essai et de l'installation des signatures et des séquences de code.	Exemple non limitatif de pièce justificative : documentation décrivant le processus de mise à jour des signatures et des séquences de code.

E4. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E4 (CIP-007-5) – Surveillance des événements de sécurité. *[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation du jour même et évaluation de l'exploitation]*

M4. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E4 (CIP-007-5) – Surveillance des événements de sécurité ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E4 (CIP-007-5) – Surveillance des événements de sécurité

Partie	Systèmes visés	Exigences	Mesures
4.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; 3. PCA associés.	Journaliser les événements au niveau du *système électronique BES* (selon les capacités du *système électronique BES*) ou au niveau de l'*actif électronique* (selon les capacités de l'*actif électronique*) permettant la détection des *incidents de cybersécurité* – et les enquêtes subséquentes à leur sujet – qui comprennent au minimum chacun des types d'événements suivants : 4.1.1. toute tentative détectée d'ouverture de session ayant réussi ; 4.1.2. toute tentative détectée d'accès ou d'ouverture de session ayant échoué ; 4.1.3. tout programme malveillant détecté.	Exemples non limitatifs de pièces justificatives : liste des types d'événements que le *système électronique BES* est en mesure de détecter, générée manuellement ou par le système lui-même, et, le cas échéant, qu'il est configuré pour journaliser. Cette liste doit comprendre les types d'événements obligatoires.

Tableau E4 (CIP-007-5) – Surveillance des événements de sécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
4.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; 3. PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; 2. PACS associés ; 3. PCA associés.	Générer des alertes pour les événements de sécurité qui, selon l'entité responsable, nécessitent une alerte, y compris au minimum chacun des types d'événements suivants (selon les capacités de l'*actif électronique* ou du *système électronique BES*) : 4.2.1. programmes malveillants détectés conformément à la partie 4.1 ; 4.2.2. échec détecté de la journalisation des événements définis à la partie 4.1.	Exemples non limitatifs de pièces justificatives : liste, générée manuellement ou par le système, des événements de sécurité qui, selon l'entité responsable, nécessitent des alertes, y compris une liste, générée manuellement ou par le système, indiquant la configuration des alertes.

Tableau E4 (CIP-007-5) – Surveillance des événements de sécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
4.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen de centres de contrôle et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Lorsque techniquement faisable, conserver les journaux des événements exigés à la partie 4.1 pendant au moins 90 jours civils consécutifs, sauf dans des *circonstances CIP exceptionnelles*.	Exemples non limitatifs de pièces justificatives : documentation du processus de conservation des journaux des événements et rapports générés manuellement ou par le système qui indiquent que la configuration de conservation des journaux est réglée à 90 jours ou plus.
4.4	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PCA associés.	Passer en revue un résumé ou un échantillon des événements journalisés, tels que définis par l'entité responsable, à des intervalles d'un maximum de 15 jours civils, afin de repérer les *incidents de cybersécurité* non détectés.	Exemples non limitatifs de pièces justificatives : document décrivant l'examen et ses constatations éventuelles, et document daté démontrant que l'examen a eu lieu.

E5. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E5 (CIP-007-5) – Contrôle des accès aux systèmes. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]*

M5. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E5 (CIP-007-5) – Contrôle des accès aux systèmes, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E5 (CIP-007-5) – Contrôle des accès aux systèmes			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
5.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen de *centres de contrôle* et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Avoir une ou plusieurs méthodes pour imposer l'authentification de tout accès utilisateur interactif, lorsque techniquement faisable.	Exemple non limitatif de pièce justificative : documentation décrivant le mode d'authentification des accès.

Tableau E5 (CIP-007-5) – Contrôle des accès aux systèmes			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
5.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Identifier et répertorier par système, par groupe de systèmes, par emplacement ou par type de système tous les comptes par défaut ou autres comptes génériques qui sont connus et activés.	Exemple non limitatif de pièce justificative : liste de comptes indiquant les types de comptes activés ou génériques utilisés pour le *système électronique BES*.
5.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Identifier toutes les personnes ayant un accès autorisé à des comptes partagés.	Exemple non limitatif de pièce justificative : liste des comptes partagés et des personnes qui y ont un accès autorisé.

Tableau E5 (CIP-007-5) – Contrôle des accès aux systèmes			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
5.4	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Changer les mots de passe par défaut connus, selon les capacités de l'*actif électronique*.	Exemples non limitatifs de pièces justificatives : • documentation de l'exécution d'une procédure selon laquelle les mots de passe sont changés lorsque de nouveaux dispositifs sont en service ; ou • mention dans les manuels des systèmes ou dans d'autres documents de leurs fournisseurs selon laquelle les mots de passe par défaut ont été générés de façon pseudo-aléatoire et sont donc exclusifs à chaque dispositif.

Tableau E5 (CIP-007-5) – Contrôle des accès aux systèmes			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
5.5	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	En ce qui concerne l'authentification par mot de passe uniquement de l'accès utilisateur interactif, imposer les paramètres suivants par des moyens techniques ou procéduraux : 5.5.1. une longueur de mot de passe d'au moins huit caractères ou de la longueur maximale permise par l'*actif électronique*, selon la moindre des deux ; 5.5.2. une complexité minimale du mot de passe d'au moins trois types différents de caractères (lettres majuscules, lettres minuscules, chiffres, caractères non alphanumériques) ou du maximum permis par l'*actif électronique*, selon la moindre des deux.	Exemples non limitatifs de pièces justificatives : • rapports générés par le système ou captures d'écran montrant les paramètres de mot de passe appliqués par le système, y compris la longueur et la complexité ; ou • attestations comportant un renvoi aux procédures documentées ayant été suivies.

Tableau E5 (CIP-007-5) – Contrôle des accès aux systèmes			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
5.6	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Lorsque techniquement faisable, en ce qui concerne l'authentification par mot de passe uniquement de l'accès utilisateur interactif, imposer par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe au moins une fois tous les 15 mois civils.	Exemples non limitatifs de pièces justificatives : • rapports générés par le système ou captures d'écran montrant la fréquence de changement du mot de passe appliquée par le système ; ou • attestations comportant un renvoi aux procédures documentées ayant été suivies.
5.7	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen de *centres de contrôle* et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Lorsque techniquement faisable, soit : • limiter le nombre de tentatives d'authentification échouées ou • générer des alertes après un certain nombre de tentatives d'authentification échouées.	Exemples non limitatifs de pièces justificatives : • documentation des paramètres de verrouillage de compte ; ou • règles de configuration des alertes indiquant comment le système avise des personnes après un nombre défini de tentatives d'ouverture de session.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable de la surveillance de l’application des normes

L’entité régionale joue le rôle de responsable de la surveillance de l’application des normes (CEA), à moins que l’entité concernée soit détenue, exploitée ou contrôlée par l’entité régionale. Dans de tels cas, le rôle de CEA est confié à l’ERO, à une entité régionale approuvée par la FERC ou à un autre organisme gouvernemental pertinent.

1.2. Conservation des pièces justificatives

Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces justificatives afin de démontrer sa conformité. Dans les cas où la période de conservation des pièces justificatives indiquée est plus courte que le temps écoulé depuis le dernier audit, le CEA peut demander à l’entité de fournir d’autres pièces justificatives pour montrer qu’elle était conforme pendant la période complète écoulée depuis le dernier audit.

L’entité responsable doit conserver les données ou pièces justificatives attestant de sa conformité de la façon indiquée ci-après, à moins que son CEA lui demande de conserver certains documents plus longtemps dans le cadre d’une enquête :

- Chaque entité responsable doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité responsable est jugée non conforme, elle doit conserver l’information relative à cette non-conformité jusqu’à ce que les correctifs aient été appliqués et approuvés ou pendant la période indiquée ci-dessus, selon la durée la plus longue.
- Le CEA doit conserver les derniers dossiers d’audit ainsi que tous les dossiers d’audit demandés et soumis par la suite.

1.3. Processus de surveillance et d’évaluation de la conformité

- Audits de conformité
- Déclarations sur la conformité
- Contrôles ponctuels
- Enquêtes sur les non-conformités
- Déclarations volontaires
- Plaintes

1.4. Autres informations sur la conformité

- Aucune.

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Annexe QC-CIP-007-5
Dispositions particulières de la norme CIP-007-5 applicables au Québec

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son 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 aura préséance.

A. Introduction

1. **Titre :** Cybersécurité — Gestion de la sécurité des systèmes
2. **Numéro :** CIP-007-5
3. **Objet :** Aucune disposition particulière
4. **Applicabilité :**

   Entités fonctionnelles

   Aucune disposition particulière

   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 :

   - Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur 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 201x

   5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 201x

   5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : xx mois 201x

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. **Processus de surveillance de la conformité**

   1.1. Responsable de la surveillance de l'application des normes

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et d'évaluation de la conformité

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	Xx mois 201x	Nouvelle annexe	Nouvelle

A. Introduction

1. Titre : Cybersécurité — Déclaration des incidents et planification des mesures d'intervention

2. Numéro : CIP-008-5

3. Objet : Réduire les risques posés au fonctionnement fiable du BES par un *incident de cybersécurité* en définissant des exigences d'intervention en cas d'incident.

4. Applicabilité :

4.1. Entités fonctionnelles : Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

4.1.1 Responsable de l'équilibrage

4.1.2 Distributeur qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du BES :

4.1.2.1 Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :

4.1.2.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.1.2.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.1.2.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

4.2. Installations : Dans le contexte des exigences de la présente norme, les *installations*, systèmes et équipements suivants détenus par chaque entité responsable indiquée à la section 4.1 sont ceux auxquels ces exigences sont applicables. Dans le cas des exigences de cette norme qui visent un type particulier d'*installations*, de système ou d'équipements, ou un sous-ensemble d'*installations*, de systèmes ou d'équipements, ceux-ci sont précisés explicitement.

4.2.1 Distributeur : Un ou plusieurs des *installations*, systèmes et équipements suivants détenus par le distributeur pour la protection ou la remise en charge du BES :

4.2.1.1 Chaque système de DSF ou de DST qui :

4.2.1.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.2.1.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

4.2.3 Exemptions : Sont exemptés de la norme CIP-008-5 :

4.2.3.1 Les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire ;

4.2.3.2 les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électroniques* distincts ;

4.2.3.3 les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme à la norme CFR 10, section 73.54 ;

4.2.3.4 dans le cas des distributeurs, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus ;

4.2.3.5 les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* catégorisés comme impact élevé ou impact moyen en conformité avec le processus d'identification et de catégorisation de la CIP-002-5.

5. Dates d'entrée en vigueur

1. **24 mois minimum** – La norme CIP-008-5 entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.
2. Dans les juridictions où aucune approbation réglementaire n'est requise, la norme CIP-008-5 entrera en vigueur le premier jour du neuvième trimestre civil suivant l'approbation par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte :

La norme CIP-008-5 fait partie d'une série de normes CIP sur la cybersécurité. La norme CIP-002-5 exige l'identification et la catégorisation initiales des *systèmes électroniques BES*. Les normes CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 et CIP-011-1 exigent un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*. Cette série de normes CIP est appelée « version 5 des normes CIP sur la cybersécurité ».

La plupart des exigences commencent ainsi : « Chaque entité responsable doit mettre en œuvre un ou plusieurs [processus, plans, etc.] documentés qui correspondent à toutes les parties d'exigence applicables du tableau [référence au tableau]. » Le tableau en référence précise les éléments qui doivent être inclus dans les procédures pour le thème commun de l'exigence.

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation

des exigences. Une entité devrait inclure autant qu'elle le juge nécessaire à leurs processus documentés, pourvu que les exigences pertinentes soient couvertes.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », lorsque cela a du sens et est communément compris. Par exemple, les processus documentés qui décrivent une réponse sont généralement appelés « plans » (plan d'action en cas d'incident, plan de rétablissement, etc.). De plus, un plan de sécurité peut décrire une approche comportant plusieurs procédures couvrant un thème étendu.

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont un exemple trouvé dans les normes. La mise en œuvre complète des normes CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

Les entités responsables peuvent mettre en œuvre des moyens communs qui répondent aux besoins de plusieurs *systèmes électroniques BES* à impact élevé et moyen. Par exemple, un même programme de formation pourrait répondre aux exigences en formation du personnel de plusieurs *systèmes électroniques BES*.

Les mesures présentent des exemples de pièces justificatives pour montrer la documentation et la mise en œuvre de l'exigence. Ces mesures servent à fournir des conseils aux entités sur ce qui peut constituer des dossiers de conformité acceptables et ne devraient pas être considérées comme une liste exhaustive.

Dans l'ensemble des normes, sauf indication particulière, les éléments présentés à la section Exigences et mesures sous forme de liste à puces sont liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances de systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes de DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

Colonnes « Systèmes visés » des tableaux

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. Le SDT CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards

and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- **Systèmes électroniques BES à impact élevé** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes électroniques BES à impact moyen** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.

B. Exigences et mesures

E1. Chaque entité responsable doit mettre en œuvre un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-008-5) – Caractéristiques du plan d'intervention en cas d'*incident de cybersécurité*. *[Facteur de risque de la non-conformité : faible] [Horizon : planification à long terme]*

M1. Les pièces justificatives doivent comprendre chacun des plans documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-008-5) – Caractéristiques du plan d'intervention en cas d'*incident de cybersécurité*.

Tableau E1 (CIP-008-5) – Caractéristiques du plan d'intervention en cas d'incident de cybersécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.1	*Systèmes électroniques BES* à impact élevé. *Systèmes électroniques BES* à impact moyen.	Un ou plusieurs processus visant à identifier les *incidents de cybersécurité*, à les classer et à y répondre.	Exemple non limitatif de pièce justificative : plan ou plans d'intervention en cas d'*incident de cybersécurité* documentés et datés qui prévoient un processus pour détecter les *incidents de cybersécurité*, les classer et y répondre.

Tableau E1 (CIP-008-5) – Caractéristiques du plan d'intervention en cas d'incident de cybersécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.2	*Systèmes électroniques BES* à impact élevé. *Systèmes électroniques BES* à impact moyen.	Un ou plusieurs processus visant à déterminer si un *incident de cybersécurité* identifié est un *incident de cybersécurité à déclarer* et à aviser l'Electricity Sector Information Sharing and Analysis Center (ES-ISAC), à moins que la loi ne l'interdise. L'ES-ISAC doit recevoir le premier avis (qui peut n'être que préliminaire) concernant un *incident de cybersécurité à déclarer* dans un délai d'au plus une heure.	Exemples non limitatifs de pièces justificatives : plan ou plans d'intervention en cas d'*incident de cybersécurité* documentés et datés qui fournissent des indications ou des seuils pour déterminer quels *incidents de cybersécurité* sont à déclarer ; preuve que des avis préliminaires ont été transmis à l'ES-ISAC.
1.3	*Systèmes électroniques BES* à impact élevé. *Systèmes électroniques BES* à impact moyen.	Rôles et responsabilités des groupes ou des personnes chargés de l'intervention en cas d'*incident de cybersécurité*.	Exemple non limitatif de pièce justificative : processus ou procédures d'intervention en cas d'*incident de cybersécurité* datés qui définissent les rôles et les responsabilités (p. ex., surveillance, déclaration, déclenchement, documentation, etc.) des groupes ou des personnes chargés de l'intervention en cas d'*incident de cybersécurité*.

Tableau E1 (CIP-008-5) – Caractéristiques du plan d'intervention en cas d'incident de cybersécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.4	*Systèmes électroniques BES* à impact élevé. *Systèmes électroniques BES* à impact moyen.	Procédures de gestion des *incidents de cybersécurité*.	Exemples non limitatifs de pièces justificatives : processus ou procédures d'intervention en cas d'*incident de cybersécurité* datés qui traitent de la gestion des incidents (p. ex., confinement, élimination, reprise après incident ou résolution de l'incident).

E2. Chaque entité responsable doit mettre en œuvre chacun de ses plans d'intervention en cas d'*incident de cybersécurité* documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-008-5) – Mise en œuvre et vérification du plan d'intervention en cas d'*incident de cybersécurité*. *[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation et exploitation en temps réel].*

M2. Les pièces justificatives doivent comprendre, sans toutefois s'y limiter, des documents qui, collectivement, démontrent la mise en œuvre de toutes les parties d'exigence applicables du tableau E2 (CIP-008-5) – Mise en œuvre et vérification du plan d'intervention en cas d'*incident de cybersécurité*.

Tableau E2 (CIP-008-5) – Mise en œuvre et vérification du plan d'intervention en cas d'incident de cybersécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé. *Systèmes électroniques BES* à impact moyen.	Tester chaque plan d'intervention en cas d'*incident de cybersécurité* au moins une fois tous les 15 mois civils : • en répondant à un *incident de cybersécurité à déclarer* réel ; • en effectuant un exercice sur papier ou sur table de réponse à un *incident de cybersécurité à déclarer* ; ou • en effectuant un exercice opérationnel de réponse à un *incident de cybersécurité à déclarer*.	Exemple non limitatif de pièce justificative : preuve datée de l'existence d'un rapport sur les leçons apprises qui contient un résumé de l'épreuve ou une compilation des notes, des journaux et des communications qui résultent du test. Les types d'exercices peuvent inclure des exercices axés sur les discussions ou sur les opérations.
2.2	*Systèmes électroniques BES* à impact élevé. *Systèmes électroniques BES* à impact moyen.	Utiliser le ou les plans d'intervention en cas d'*incident de cybersécurité* cités à l'exigence E1 au moment de répondre à un *incident de cybersécurité à déclarer* ou d'effectuer un exercice de réponse à un *incident de cybersécurité à déclarer*. Documenter les écarts entre le ou les plans et les mesures prises pendant l'intervention en cas d'incident ou l'exercice.	Exemples non limitatifs de pièces justificatives : rapports d'incident, journaux et notes prises durant l'intervention en cas d'incident, et documents de suivi décrivant les écarts entre le ou les plans et les mesures prises durant l'intervention en cas d'incident ou l'exercice.

Tableau E2 (CIP-008-5) – Mise en œuvre et vérification du plan d'intervention en cas d'incident de cybersécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.3	*Systèmes électroniques BES* à impact élevé. *Systèmes électroniques BES* à impact moyen.	Conserver les dossiers relatifs aux *incidents de cybersécurité à déclarer*.	Exemples non limitatifs de pièces justificatives : documents datés, tels que journaux de sécurité, rapports de police, courriels, formulaires d'intervention ou listes de contrôle, résultats d'analyses judiciaires, dossiers de remise en charge et notes d'analyse après incident relativement à des *incidents de cybersécurité à déclarer*.

E3. Chaque entité responsable doit tenir à jour chacun de ses plans d'intervention en cas d'*incident de cybersécurité* conformément à chacune des parties d'exigence applicables du tableau E3 (CIP-008-5) – Examen, mise à jour et communication du plan d'intervention en cas d'*incident de cybersécurité*. *[Facteur de risque de la non-conformité : faible] [Horizon : évaluation de l'exploitation]*

M3. Les pièces justificatives doivent comprendre, sans toutefois s'y limiter, des documents qui, collectivement, démontrent que tous les plans d'intervention en cas d'*incident de cybersécurité* sont tenus à jour conformément aux parties d'exigence applicables du tableau E3 (CIP-008-5) – Examen, mise à jour et communication du plan d'intervention en cas d'*incident de cybersécurité*.

Tableau E3 (CIP-008-5) – Examen, mise à jour et communication du plan d'intervention en cas d'incident de cybersécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes électroniques BES* à impact élevé. *Systèmes électroniques BES* à impact moyen.	Au plus tard 90 jours civils après la réalisation d'un test des plans d'intervention en cas d'*incident de cybersécurité* ou après une intervention en cas d'*incident de cybersécurité à déclarer* réel : 3.1.1. documenter les leçons apprises, ou encore l'absence de leçons apprises ; 3.1.2. mettre à jour le plan d'intervention en cas d'*incident de cybersécurité* en tenant compte des leçons apprises documentées qui se rapportent à ce plan ; et 3.1.3. aviser chaque personne ou groupe qui joue un rôle défini dans le plan d'intervention en cas d'*incident de cybersécurité* des mises à jour à ce plan qui tiennent compte des leçons apprises documentées.	Exemples non limitatifs de pièces justificatives : 1. documents datés, tels que notes de réunion après incident ou rapports de suivi indiquant les leçons apprises associées à la mise à l'épreuve du ou des plans d'intervention en cas d'*incident de cybersécurité* ou à une intervention en cas d'*incident de cybersécurité à déclarer* réelle, ou encore documents datés confirmant l'absence de leçons apprises ; 2. plan d'intervention en cas d'*incident de cybersécurité* daté et révisé indiquant toutes les modifications apportées en tenant compte des leçons apprises ; et 3. preuve de distribution du plan révisé, par exemple : • courriels ; • « US Postal Service » ou autre service postal ; • système de distribution électronique ; ou • feuilles de présence aux formations.

Tableau E3 (CIP-008-5) – Examen, mise à jour et communication du plan d'intervention en cas d'incident de cybersécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*Systèmes électroniques BES* à impact élevé. *Systèmes électroniques BES* à impact moyen.	Au plus tard 60 jours civils après qu'un changement jugé par l'entité responsable comme ayant un impact sur la capacité d'exécuter le plan a été apporté aux rôles ou responsabilités, aux groupes ou personnes chargés de l'intervention en cas d'*incident de cybersécurité* ou à une technologie : 3.2.1. mettre à jour le ou les plans d'intervention en cas d'*incident de cybersécurité* ; et 3.2.2. aviser des mises à jour chaque personne ou groupe jouant un rôle défini dans le plan d'intervention en cas d'*incident de cybersécurité*.	Exemples non limitatifs de pièces justificatives : 1. plan d'intervention en cas d'*incident de cybersécurité* révisé et daté incluant les changements apportés aux rôles ou responsabilités, aux intervenants ou à une technologie ; et 2. preuve de distribution du plan révisé, par exemple : • courriels ; • « US Postal Service » ou autre service postal ; • système de distribution électronique ; ou • feuilles de présence aux formations.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable de la surveillance de l'application des normes

L'entité régionale joue le rôle de responsable de la surveillance de l'application des normes (CEA), à moins que l'entité concernée soit détenue, exploitée ou contrôlée par l'entité régionale. Dans de tels cas, le rôle de CEA est confié à l'ERO, à une entité régionale approuvée par la FERC ou à un autre organisme gouvernemental pertinent.

1.2. Conservation des pièces justificatives

Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces justificatives afin de démontrer sa conformité. Dans les cas où la période de conservation des pièces justificatives indiquée est plus courte que le temps écoulé depuis le dernier audit, le CEA peut demander à l'entité de fournir d'autres pièces justificatives pour montrer qu'elle était conforme pendant la période complète écoulée depuis le dernier audit.

L'entité responsable doit conserver les données ou pièces justificatives attestant de sa conformité de la façon indiquée ci-après, à moins que son CEA lui demande de conserver certains documents plus longtemps dans le cadre d'une enquête :

- Chaque entité responsable doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité responsable est jugée non conforme, elle doit conserver l'information relative à cette non-conformité jusqu'à ce que les correctifs aient été appliqués et approuvés ou pendant la période indiquée ci-dessus, selon la durée la plus longue.
- Le CEA doit conserver les derniers dossiers d'audit ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Processus de surveillance et d'évaluation de la conformité

- Audits de conformité
- Déclarations sur la conformité
- Contrôles ponctuels
- Enquêtes sur les non-conformités
- Déclarations volontaires
- Plaintes

1.4. Autres informations sur la conformité

- Aucune

2. Tableau des éléments de conformité

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-008-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	**Planification à long terme**	**Faible**	Sans objet	Sans objet	L'entité responsable a élaboré les plans d'intervention en cas d'*incident de cybersécurité*, mais le plan ne comprend pas les rôles et responsabilités des groupes ou des personnes chargés de l'intervention en cas d'*incident de cybersécurité*. (1.3) OU L'entité responsable a élaboré les plans d'intervention en cas d'*incident de cybersécurité*, mais le plan ne comprend pas les procédures de gestion des incidents pour les *incidents de cybersécurité*. (1.4)	L'entité responsable n'a pas élaboré un plan d'intervention en cas d'*incident de cybersécurité* comprenant un ou plusieurs processus pour identifier, classifier et répondre aux *incidents de cybersécurité*. (1.1) OU L'entité responsable a élaboré un plan d'intervention en cas d'*incident de cybersécurité,* mais le plan ne comprend pas un ou plusieurs processus pour identifier les *incidents de cybersécurité à déclarer*. (1.2) OU L'entité responsable a

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-008-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						élaboré un plan d'intervention en cas d'*incident de cybersécurité*, mais n'a pas fourni au moins un avis préliminaire au ES-ISAC dans l'heure suivant l'identification d'un *incident de cybersécurité à déclarer*. (1.2)
E2	**Planification de l'exploitation** **Exploitation en temps réel**	**Faible**	L'entité responsable n'a pas testé le ou les plans d'intervention en cas d'*incident de cybersécurité* à l'intérieur de 15 mois civils, sans excéder 16 mois civils entre les tests du plan. (2.1)	L'entité responsable n'a pas testé le ou les plans d'intervention en cas d'*incident de cybersécurité* à l'intérieur de 16 mois civils, sans excéder 17 mois civils entre les tests du plan. (2.1)	L'entité responsable n'a pas testé le ou les plans d'intervention en cas d'*incident de cybersécurité* à l'intérieur de 17 mois civils, sans excéder 18 mois civils entre les tests du plan. (2.1) OU L'entité responsable n'a pas documenté les écarts, s'il y en a, par rapport au plan pendant un test ou	L'entité responsable n'a pas testé le ou les plans d'intervention en cas d'*incident de cybersécurité* à l'intérieur de 18 mois civils entre les tests du plan. (2.1) OU L'entité responsable n'a pas conservé les dossiers pertinents relatifs aux *incidents de cybersécurité à déclarer*. (2.3)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-008-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					lorsqu'un *incident de cybersécurité à déclarer* se produit. (2.2)	
E3	**Évaluation de l'exploitation**	**Faible**	L'entité responsable n'a pas avisé chaque personne ou groupe qui joue un rôle défini dans le plan d'intervention en cas d'*incident de cybersécurité* des mises à jour au plan d'intervention en cas d'*incident de cybersécurité* à l'intérieur de plus de 90, mais en moins de 120 jours civils suivant un test ou une intervention réelle à un *incident de cybersécurité à déclarer*. (3.1.3)	L'entité responsable n'a pas mis à jour le plan d'intervention en cas d'incident de cybersécurité en tenant compte des leçons apprises documentées à l'intérieur de 90 à moins de 120 jours civils suivant un test ou une intervention réelle à un *incident de cybersécurité à déclarer*. (3.1.2) OU L'entité responsable n'a pas avisé chaque personne ou groupe qui joue un rôle défini dans le plan d'intervention en cas	L'entité responsable n'a ni documenté les leçons apprises ni documenté l'absence de leçons apprises à l'intérieur de 90, et en moins de 120 jours civils suivant un test ou une intervention réelle à un *incident de cybersécurité à déclarer*. (3.1.1) OU L'entité responsable n'a pas mis à jour le plan d'intervention en cas d'incident de cybersécurité en tenant compte des leçons apprises documentées à l'intérieur de 120 jours	L'entité responsable n'a ni documenté les leçons apprises ni documenté l'absence de leçons apprises à l'intérieur de 120 jours civils suivant un test ou une intervention réelle à un *incident de cybersécurité à déclarer*. (3.1.1)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-008-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				d'*incident de cybersécurité* des mises à jour au plan d'intervention en cas d'*incident de cybersécurité* à l'intérieur de 120 jours civils suivant un test ou une intervention réelle à un *incident de cybersécurité à déclarer*. (3.1.3) OU L'entité responsable n'a pas mis à jour le ou les plans d'intervention en cas d'*incident de cybersécurité* ou avisé chaque personne ou groupe qui joue un rôle défini à l'intérieur de 60, et en moins de 90 jours civils suivant un des changements suivants que l'entité responsable juge comme pouvant	civils suivant un test ou une intervention réelle à un *incident de cybersécurité à déclarer*. (3.1.2) OU L'entité responsable n'a pas mis à jour le ou les plans d'intervention en cas d'*incident de cybersécurité* ou avisé chaque personne ou groupe qui joue un rôle défini à l'intérieur de 90 jours civils suivant un des changements suivants que l'entité responsable juge comme pouvant affecter la capacité à exécuter le plan: (3.2) • Rôles et responsabilités, ou • Personnes ou groupes d'intervention en	

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-008-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				affecter la capacité à exécuter le plan: (3.2) • Rôles et responsabilités, ou • Personnes ou groupes d'intervention en cas d'*incident de cybersécurité*, ou • Changements technologiques.	cas d'*incident de cybersécurité*, ou Changements technologiques.	

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Annexe QC-CIP-008-5
Dispositions particulières de la norme CIP-008-5 applicables au Québec

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son 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 aura préséance.

A. Introduction

1. **Titre :** Cybersécurité — Déclaration des incidents et planification des mesures d'intervention

2. **Numéro :** CIP-008-5

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

   Entités fonctionnelles

   Aucune disposition particulière

   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 :

   - Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur 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 201x

   5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 201x

   5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : xx mois 201x

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable de la surveillance de l'application des normes

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et d'évaluation de la conformité

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	Xx mois 201x	Nouvelle annexe	Nouvelle

A. Introduction

1. Titre : Cybersécurité — Plans de rétablissement des systèmes électroniques BES

2. Numéro : CIP-009-5

3. Objet : Rétablir les fonctions de fiabilité exercées par les *systèmes électroniques BES* en définissant les exigences relatives aux plans de rétablissement en vue du maintien de la stabilité, de l'exploitabilité et de la fiabilité du BES.

4. Applicabilité :

4.1. Entités fonctionnelles : Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

4.1.1 Responsable de l'équilibrage

4.1.2 Distributeur qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du BES :

4.1.2.1 Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :

4.1.2.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.1.2.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.1.2.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

4.2. Installations : Dans le contexte des exigences de la présente norme, les *installations*, systèmes et équipements suivants détenus par chaque entité responsable indiquée à la section 4.1 sont ceux auxquels ces exigences sont applicables. Dans le cas des exigences de cette norme qui visent un type particulier d'*installations*, de système ou d'équipements, ou un sous-ensemble d'*installations*, de systèmes ou d'équipements, ceux-ci sont précisés explicitement.

4.2.1 Distributeur : Un ou plusieurs des *installations*, systèmes et équipements suivants détenus par le distributeur pour la protection ou la remise en charge du BES :

4.2.1.1 Chaque système de DSF ou de DST qui :

4.2.1.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.2.1.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

4.2.3 Exemptions : Sont exemptés de la norme CIP-009-5 :

4.2.3.1 Les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire ;

4.2.3.2 les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électroniques* distincts ;

4.2.3.3 les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme à la norme CFR 10, section 73.54 ;

4.2.3.4 dans le cas des distributeurs, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus ;

4.2.3.5 les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* catégorisés comme impact élevé ou impact moyen en conformité avec le processus d'identification et de catégorisation de la CIP-002-5.

5. Dates d'entrée en vigueur

1. **24 mois minimum** – La norme CIP-009-5 entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.
2. Dans les juridictions où aucune approbation réglementaire n'est requise, la norme CIP-009-5 entrera en vigueur le premier jour du neuvième trimestre civil suivant l'approbation par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte :

La norme CIP-009-5 fait partie d'une série de normes CIP sur la cybersécurité. La norme CIP-002-5 exige l'identification et la catégorisation initiales des *systèmes électroniques BES*. Les normes CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 et CIP-011-1 exigent un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*. Cette série de normes CIP est appelée « version 5 des normes CIP sur la cybersécurité ».

La plupart des exigences commencent ainsi : « Chaque entité responsable doit mettre en œuvre un ou plusieurs [processus, plans, etc.] documentés qui correspondent à toutes les parties d'exigence applicables du tableau [référence au tableau]. » Le tableau en référence précise les éléments qui doivent être inclus dans les procédures pour le thème commun de l'exigence.

Le SDT a intégré à la présente norme une reconnaissance à l'effet que certaines exigences ne devraient pas mettre l'accent sur les cas individuels de défaillance comme seul motif d'infraction à la norme. En particulier, le SDT a intégré une approche visant à habiliter l'industrie à identifier, à évaluer et à corriger les lacunes dans la mise en œuvre de certaines exigences. L'intention est de changer la manière

de considérer les infractions dans ces exigences, de sorte qu'il ne s'agisse plus de savoir *si* une lacune existe, mais plutôt d'identifier, d'évaluer et de corriger les lacunes. Ceci est présenté dans ces exigences en modifiant la notion de « mise en œuvre » de la façon suivante :

> Chaque entité responsable doit mettre en œuvre**, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes…**

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité devrait inclure autant qu'elle le juge nécessaire à leurs processus documentés, pourvu que les exigences pertinentes soient couvertes. Les processus documentés eux-mêmes n'ont pas à intégrer la démarche « détecter, évaluer et corriger les lacunes » décrite au paragraphe précédent, car cette démarche est liée à la manière de mettre en œuvre les processus documentés et pourrait être réalisée par d'autres mesures de contrôle ou de gestion de la conformité.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », lorsque cela a du sens et est communément compris. Par exemple, les processus documentés qui décrivent une réponse sont généralement appelés « plans » (plan d'action en cas d'incident, plan de rétablissement, etc.). De plus, un plan de sécurité peut décrire une approche comportant plusieurs procédures couvrant un thème étendu.

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont un exemple trouvé dans les normes. La mise en œuvre complète des normes CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

Les entités responsables peuvent mettre en œuvre des moyens communs qui répondent aux besoins de plusieurs *systèmes électroniques BES* à impact élevé et moyen. Par exemple, un même programme de formation pourrait répondre aux exigences en formation du personnel de plusieurs *systèmes électroniques BES*.

Les mesures présentent des exemples de pièces justificatives pour montrer la documentation et la mise en œuvre de l'exigence. Ces mesures servent à fournir des conseils aux entités sur ce qui peut constituer des dossiers de conformité acceptables et ne devraient pas être considérées comme une liste exhaustive.

Dans l'ensemble des normes, sauf indication particulière, les éléments présentés à la section Exigences et mesures sous forme de liste à puces sont liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances de systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes de DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

Colonnes « Systèmes visés » des tableaux

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. Le SDT CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- **Systèmes électroniques BES à impact élevé** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes électroniques BES à impact moyen** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes électroniques BES à impact moyen situés aux centres de contrôle –** Désigne uniquement les *systèmes électroniques BES* situés aux *centres de contrôle* et classés dans la catégori*e* impact moyen , conformément aux processus d'inventaire et de catégorisation de la norme CIP-002-5.
- **Systèmes de contrôle ou de surveillance des accès électroniques (EACMS)** – Désigne tout *système de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d'authentification, et systèmes de surveillance de registre d'événement et d'alerte.
- **Systèmes de contrôle des accès physiques (PACS)** – Désigne tout *système de contrôle des accès physique*s associé à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.

B. Exigences et mesures

E1. Chaque entité responsable doit disposer d'un ou de plusieurs plans de rétablissement documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-009-5) – Caractéristiques d'un plan de rétablissement. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification à long terme]*

M1. Les pièces justificatives doivent inclure le ou les plans de rétablissement documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-009-5) – Caractéristiques d'un plan de rétablissement.

Tableau E1 (CIP-009-5) – Caractéristiques d'un plan de rétablissement			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; et 2. PACS associés.	Conditions de déclenchement du ou des plans de rétablissement.	Exemples non limitatifs de pièces justificatives : un ou plusieurs plans de rétablissement où sont énoncées les conditions de déclenchement du ou des plans.
1.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; et 2. PACS associés.	Rôles et responsabilités des intervenants.	Exemples non limitatifs de pièces justificatives : un ou plusieurs plans de rétablissement où sont énoncés les rôles et responsabilités des intervenants.

Tableau E1 (CIP-009-5) – Caractéristiques d'un plan de rétablissement			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; et 2. PACS associés.	Un ou plusieurs processus pour la sauvegarde et le stockage de l'information nécessaire au rétablissement des *systèmes électroniques BES*.	Exemples non limitatifs de pièces justificatives : processus documentés pour la sauvegarde et le stockage de l'information nécessaire au rétablissement des *systèmes électroniques BES*.
1.4	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et leurs : 1. EACMS associés ; et 2. PACS associés.	Un ou plusieurs processus de vérification du bon déroulement des processus de sauvegarde énoncés à la partie 1.3 et de prise en compte des échecs de sauvegarde.	Exemples non limitatifs de pièces justificatives : journaux, preuves d'activité ou autres documents attestant le bon déroulement du processus de sauvegarde et la prise en compte des échecs de sauvegarde, le cas échéant.
1.5	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; et 2. PACS associés.	Un ou plusieurs processus de conservation des données, selon les capacités des *actifs électroniques*, permettant de déterminer la cause d'un *incident de cybersécurité* qui déclenche le ou les plans de rétablissement. La conservation des données ne doit pas nuire au rétablissement ni le limiter.	Exemples non limitatifs de pièces justificatives : procédures de conservation des données, comme la conservation d'un périphérique de stockage victime de corruption de données, ou la copie miroir des données du système avant d'entreprendre le rétablissement.

E2. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, son ou ses plans de rétablissement documentés, qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-009-5) – Mise en œuvre et essais du plan de rétablissement. *[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation et exploitation en temps réel]*

M2. Les pièces justificatives doivent comprendre, sans toutefois s'y limiter, des documents qui, collectivement, démontrent la mise en œuvre de toutes les parties d'exigence applicables du tableau E2 (CIP-009-5) – Mise en œuvre et essais du plan de rétablissement.

Tableau E2 (CIP-009-5) – Mise en œuvre et essais du plan de rétablissement			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et leurs : 1. EACMS associés ; et 2. PACS associés.	Tester chacun des plans de rétablissement visés par l'exigence E1 au moins une fois tous les 15 mois civils : • En se rétablissant après un incident réel ; • Avec un exercice sur papier ou sur table ; ou • Avec un exercice opérationnel.	Exemples non limitatifs de pièces justificatives : preuve datée de l'existence d'un essai du plan de rétablissement (rétablissement des systèmes après un incident réel, exercice sur papier ou sur table, ou exercice opérationnel) au moins une fois tous les 15 mois civils. Dans le cas de l'exercice sur papier ou de l'exercice opérationnel complet, des avis de réunion, des procès-verbaux ou autres documents consignant les résultats des exercices peuvent constituer des pièces justificatives.

Tableau E2 (CIP-009-5) – Mise en œuvre et essais du plan de rétablissement			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et leurs : 1. EACMS associés ; et 2. PACS associés.	Tester un échantillon représentatif de l'information nécessaire pour rétablir la fonctionnalité du *système électronique BES* au moins une fois tous les 15 mois civils afin de s'assurer que l'information est utilisable et compatible avec les configurations courantes. Ce test peut être remplacé par un rétablissement suivant un incident réel utilisant l'information nécessaire pour rétablir la fonctionnalité du *système électronique BES*.	Exemples non limitatifs de pièces justificatives : journaux d'exploitation ou résultats de l'essai ainsi que les critères de vérification que l'information est utilisable (p. ex., échantillonner les données sur une bande, parcourir le contenu d'une bande) et de sa compatibilité avec les configurations courantes des systèmes (p. ex., points de comparaison manuels ou automatisés entre le contenu des supports de sauvegarde et la configuration courante).
2.3	*Systèmes électroniques BES* à impact élevé	Tester chacun des plans de rétablissement visés par l'exigence E1 au moins une fois tous les 36 mois civils, en effectuant un exercice opérationnel des plans de rétablissement dans un environnement représentatif de l'environnement de production. Les mesures de rétablissement prises après un incident réel peuvent remplacer l'exercice opérationnel.	Exemples non limitatifs de pièces justificatives : • preuve documentée et datée d'un exercice opérationnel effectué au moins une fois tous les 36 mois civils, qui démontre le rétablissement dans un environnement représentatif ; ou • preuve documentée et datée de mesures de rétablissement prises, dans la fenêtre de 36 mois civils, après un incident réel ayant déclenché les plans de rétablissement.

E3. Chaque entité responsable doit tenir à jour chacun de ses plans de rétablissement conformément à chacune des parties d'exigence applicables du tableau E3 (CIP-009-5) – Examen, mise à jour et communication d'un plan de rétablissement. *[Facteur de risque de la non-conformité : faible] [Horizon : évaluation de l'exploitation]*

M3. Les pièces justificatives acceptables comprennent, sans toutefois s'y limiter, chacune des parties d'exigence applicables du tableau E3 (CIP-009-5) – Examen, mise à jour et communication d'un plan de rétablissement.

Tableau E3 (CIP-009-5) – Examen, mise à jour et communication d'un plan de rétablissement			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et leurs : 1. EACMS associés ; et 2. PACS associés.	Au plus tard 90 jours civils après la réalisation d'un test de plan de rétablissement ou un rétablissement réel : 3.1.1. documenter toutes les leçons apprises se rapportant au test de plan de rétablissement ou au rétablissement réel, ou documenter l'absence de leçons apprises ; 3.1.2. mettre à jour le plan de rétablissement en tenant compte des leçons apprises documentées associées au plan ; et 3.1.3. aviser chaque personne ou groupe qui joue un rôle défini dans le plan de rétablissement des mises à jour qui ont été apportées au plan de rétablissement en tenant compte des leçons apprises documentées.	Exemples non limitatifs de pièces justificatives : 1. documents datés consignant les lacunes relevées ou les leçons apprises pour chaque test du plan de rétablissement ou chaque rétablissement suivant un incident réel, ou documents datés attestant l'absence de leçons apprises ; 2. plan de rétablissement daté et révisé indiquant toutes les modifications apportées en tenant compte des leçons apprises ; et 3. preuve de distribution du plan révisé, par exemple : • courriels ; • « US Postal Service » ou autre service postal ; • système de distribution électronique ; ou • feuilles de présence aux formations.

Tableau E3 (CIP-009-5) – Examen, mise à jour et communication d'un plan de rétablissement			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et leurs : 1. EACMS associés ; et 2. PACS associés.	Au plus tard 60 jours civils après un changement aux rôles ou responsabilités, aux intervenants ou à une technologie que l'entité responsable juge qu'il pourrait avoir un impact sur la capacité d'exécuter le plan de rétablissement : 3.2.1. mettre à jour le plan de rétablissement ; et 3.2.2. aviser des mises à jour chaque personne ou groupe jouant un rôle défini dans le plan de rétablissement.	Exemples non limitatifs de pièces justificatives : 1. plan de rétablissement, révisé et daté, comprenant les changements apportés aux rôles ou responsabilités, aux intervenants ou à une technologie ; et 2. preuve de distribution du plan révisé, par exemple : • courriels ; • « US Postal Service » ou autre service postal ; • système de distribution électronique ; ou • feuilles de présence aux formations.

C. Conformité

1. Processus de surveillance de la conformité :

1.1. Responsable de la surveillance de l'application des normes :

L'entité régionale joue le rôle de responsable de la surveillance de l'application des normes (CEA), à moins que l'entité concernée soit détenue, exploitée ou contrôlée par l'entité régionale. Dans de tels cas, le rôle de CEA est confié à l'ERO, à une entité régionale approuvée par la FERC ou à un autre organisme gouvernemental pertinent.

1.2. Conservation des pièces justificatives :

Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces justificatives afin de démontrer sa conformité. Dans les cas où la période de conservation des pièces justificatives indiquée est plus courte que le temps écoulé depuis le dernier audit, le CEA peut demander à l'entité de fournir d'autres pièces justificatives pour montrer qu'elle était conforme pendant la période complète écoulée depuis le dernier audit.

L'entité responsable doit conserver les données ou pièces justificatives attestant de sa conformité de la façon indiquée ci-après, à moins que son CEA lui demande de conserver certains documents plus longtemps dans le cadre d'une enquête :

- Chaque entité responsable doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité responsable est jugée non conforme, elle doit conserver l'information relative à cette non-conformité jusqu'à ce que les correctifs aient été appliqués et approuvés ou pendant la période indiquée ci-dessus, selon la durée la plus longue.
- Le CEA doit conserver les derniers dossiers d'audit ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Processus de surveillance et d'évaluation de la conformité :

- Audits de conformité
- Déclarations sur la conformité
- Contrôles ponctuels
- Enquêtes sur les non-conformités
- Déclarations volontaires
- Plaintes

1.4. Autres informations sur la conformité :

- Aucune

2. Tableau des éléments de conformité

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	**Planification à long terme**	**Moyen**	Sans objet	L'entité responsable a élaboré un ou des plans de rétablissement, mais n'a pas traité de l'une des exigences comprises aux parties 1.2 à 1.5.	L'entité responsable a élaboré un ou des plans de rétablissement, mais n'a pas traité de deux des exigences comprises aux parties 1.2 à 1.5.	L'entité responsable n'a pas créé un ou des plans de rétablissement pour les *systèmes électroniques BES*. OU L'entité responsable a créé un ou des plans de rétablissement pour les *systèmes électroniques BES*, mais le ou les plans ne traitent pas des conditions de déclenchement de la partie 1.1. OU L'entité responsable a créé un ou des plans de rétablissement pour les *systèmes électroniques BES*, mais le ou les plans ne

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						traitent pas de trois des exigences des parties 1.2 à 1.5 ou plus.
E2	**Planification de l'exploitation** **Exploitation en temps réel**	**Faible**	L'entité responsable n'a pas testé le ou les plans de rétablissement conformément à la partie 2.1 (E2) à l'intérieur de 15 mois civils, sans dépasser 16 mois civils entre les tests du plan, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.1) OU L'entité responsable n'a pas testé un échantillon représentatif de l'information utilisée pour le rétablissement de la fonctionnalité du	L'entité responsable n'a pas testé le ou les plans de rétablissement conformément à la partie 2.1 (E2) à l'intérieur de 16 mois civils, sans dépasser 17 mois civils entre les tests du plan, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.1) OU L'entité responsable n'a pas testé un échantillon représentatif de l'information utilisée pour le rétablissement de la fonctionnalité du	L'entité responsable n'a pas testé le ou les plans de rétablissement conformément à la partie 2.1 (E2) à l'intérieur de 17 mois civils, sans dépasser 18 mois civils entre les tests du plan, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.1) OU L'entité responsable n'a pas testé un échantillon représentatif de l'information utilisée pour le rétablissement de la fonctionnalité du	L'entité responsable n'a pas testé le ou les plans de rétablissement conformément à la partie 2.1 (E2) à l'intérieur de 18 mois civils entre les tests du plan. (2.1) OU L'entité responsable a testé le ou les plans de rétablissement conformément à la partie 2.1 (E2) et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes. (2.1) OU L'entité responsable a

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			système électronique BES conformément à la partie 2.2 (E2) à l'intérieur de 15 mois civils, sans dépasser 16 mois civils entre les tests, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.2) OU L'entité responsable n'a pas testé le plan de rétablissement conformément à la partie 2.3 (E2) à l'intérieur de 36 mois civils, sans dépasser 37 mois civils entre les tests, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.3)	*système électronique BES* conformément à la partie 2.2 (E2) à l'intérieur de 16 mois civils, sans dépasser 17 mois civils entre les tests, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.2) OU L'entité responsable n'a pas testé le plan de rétablissement conformément à la partie 2.3 (E2) à l'intérieur de 37 mois civils, sans dépasser 38 mois civils entre les tests, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.3)	*système électronique BES* conformément à la partie 2.2 (E2) à l'intérieur de 17 mois civils, sans dépasser 18 mois civils entre les tests, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.2) OU L'entité responsable n'a pas testé le plan de rétablissement conformément à la partie 2.3 (E2) à l'intérieur de 38 mois civils, sans dépasser 39 mois civils entre les tests, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.3)	testé le ou les plans de rétablissement conformément à la partie 2.1 (E2), mais elle n'a pas identifié, évalué ou corrigé les lacunes. (2.1) OU L'entité responsable n'a pas testé un échantillon représentatif de l'information utilisée pour le rétablissement de la fonctionnalité du *système électronique BES* conformément à la partie 2.2 (E2) à l'intérieur de 18 mois civils entre les tests. (2.2) OU L'entité responsable a testé un échantillon représentatif de l'information utilisée

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						pour le rétablissement de la fonctionnalité du *système électronique BES* conformément à la partie 2.2 (E2) et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes. (2.2) OU L'entité responsable a testé un échantillon représentatif de l'information utilisée pour le rétablissement de la fonctionnalité du *système électronique BES* conformément à la partie 2.2 (E2), mais elle n'a pas identifié, évalué ou corrigé les lacunes. (2.2) OU L'entité responsable n'a pas testé le ou les plans de

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						rétablissement conformément à la partie 2.3 (E2) à l'intérieur de 39 mois civils entre les tests du plan. (2.3) OU L'entité responsable a testé le ou les plans de rétablissement conformément à la partie 2.3 (E2) et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (2.3) OU L'entité responsable a testé le ou les plans de rétablissement conformément à la partie 2.3 (E2), mais elle n'a pas identifié, évalué ou corrigé les lacunes. (2.3)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E3	**Évaluation de l'exploitation**	**Faible**	L'entité responsable n'a pas avisé chaque personne ou groupe jouant un rôle défini dans le ou les plans de rétablissement des mises à jour à l'intérieur de 90 et en moins de 120 jours civils suivant la réalisation complète de la mise à jour. (3.1.3)	L'entité responsable n'a pas mis à jour le ou les plans de rétablissement en tenant compte de toutes leçons apprises documentées à l'intérieur de 90 et en moins de 120 jours civils suivant chaque test de plan de rétablissement ou rétablissement réel. (3.1.2) OU L'entité responsable n'a pas avisé chaque personne ou groupe jouant un rôle défini dans le ou les plans de rétablissement des mises à jour à l'intérieur 120 jours civils suivant la réalisation complète de la mise à jour. (3.1.3)	L'entité responsable n'a ni leçons apprises documentées, ni n'a documenté l'absence de leçons apprises à l'intérieur de 90 et en moins de 120 jours civils suivant chaque test de plan de rétablissement ou rétablissement réel. (3.1.1) OU L'entité responsable n'a pas mis à jour le ou les plans de rétablissement en tenant compte de toutes leçons apprises documentées à l'intérieur de 120 jours civils suivant chaque test de plan de rétablissement ou rétablissement réel. (3.1.2)	L'entité responsable n'a ni leçons apprises documentées, ni n'a documenté l'absence de leçons apprises à l'intérieur de 120 jours civils suivant chaque test de plan de rétablissement ou rétablissement réel. (3.1.1)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				OU L'entité responsable n'a pas mis à jour le ou les plans de rétablissement ou avisé chaque personne ou groupe jouant un rôle défini à l'intérieur de 60 et en moins de 90 jours civils suivant un des changements suivants que l'entité responsable juge qu'il pourrait avoir un impact sur la capacité d'exécuter le plan : (3.2) • Rôles et responsabilités, ou • Intervenants, ou • Changements technologiques.	OU L'entité responsable n'a pas mis à jour le ou les plans de rétablissement ou avisé chaque personne ou groupe jouant un rôle défini à l'intérieur de 90 jours civils suivant un des changements suivants que l'entité responsable juge qu'il pourrait avoir un impact sur la capacité d'exécuter le plan : (3.2) • Rôles et responsabilités, ou • Intervenants, ou • Changements technologiques.	

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Annexe QC-CIP-009-5
Dispositions particulières de la norme CIP-009-5 applicables au Québec

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son 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 aura préséance.

A. Introduction

1. **Titre :** Cybersécurité — Plans de rétablissement des systèmes électroniques BES

2. **Numéro :** CIP-009-5

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

Entités fonctionnelles

Aucune disposition particulière

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 :

- Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur 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 201x

5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 201x

5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : xx mois 201x

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. **Processus de surveillance de la conformité**

1.1. Responsable de la surveillance de l'application des normes

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et d'évaluation de la conformité

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	Xx mois 201x	Nouvelle annexe	Nouvelle

A. Introduction

1. Titre : Cybersécurité — Gestion des changements de configuration et analyses de vulnérabilité

2. Numéro : CIP-010-1

3. Objet : Prévenir et détecter les changements non autorisés aux *systèmes électroniques BES* au moyen d'exigences relatives à la gestion des changements de configuration et aux analyses de vulnérabilité, afin de protéger les *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou des instabilités dans le BES.

4. Applicabilité :

4.1. Entités fonctionnelles : Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

4.1.1 Responsable de l'équilibrage

4.1.2 Distributeur qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du BES :

4.1.2.1 Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :

4.1.2.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.1.2.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.1.2.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

4.2. Installations : Dans le contexte des exigences de la présente norme, les *installations*, systèmes et équipements suivants détenus par chaque entité responsable indiquée à la section 4.1 sont ceux auxquels ces exigences sont applicables. Dans le cas des exigences de cette norme qui visent un type particulier d'*installations*, de système ou d'équipements, ou un sous-ensemble d'*installations*, de systèmes ou d'équipements, ceux-ci sont précisés explicitement.

4.2.1 Distributeur : Un ou plusieurs des *installations*, systèmes et équipements suivants détenus par le distributeur pour la protection ou la remise en charge du BES :

4.2.1.1 Chaque système de DSF ou de DST qui :

4.2.1.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.2.1.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

4.2.3 Exemptions : Sont exemptés de la norme CIP-010-1 :

4.2.3.1 Les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire ;

4.2.3.2 les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électroniques* distincts ;

4.2.3.3 les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme à la norme CFR 10, section 73.54 ;

4.2.3.4 dans le cas des distributeurs, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus ;

4.2.3.5 les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* catégorisés comme impact élevé ou impact moyen en conformité avec le processus d'identification et de catégorisation de la CIP-002-5.

5. Dates de mise en vigueur

1. **24 mois minimum** – La norme CIP-010-1 entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.
2. Dans les juridictions où aucune approbation réglementaire n'est requise, la norme CIP-010-1 entrera en vigueur le premier jour du neuvième trimestre civil suivant l'approbation par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte :

La norme CIP-010-1 fait partie d'une série de normes CIP sur la cybersécurité. La norme CIP-002-5 exige l'identification et la catégorisation initiales des *systèmes électroniques BES*. Les normes CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 et CIP-011-1 exigent un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*. Cette série de normes CIP est appelée « version 5 des normes CIP sur la cybersécurité ».

La plupart des exigences commencent ainsi : « Chaque entité responsable doit mettre en œuvre un ou plusieurs [processus, plans, etc.] documentés qui correspondent à toutes les parties d'exigence applicables du tableau [référence au tableau]. » Le tableau en référence précise les éléments qui doivent être inclus dans les procédures pour le thème commun de l'exigence.

Le SDT a intégré à la présente norme une reconnaissance à l'effet que certaines exigences ne devraient pas mettre l'accent sur les cas individuels de défaillance comme seul motif d'infraction à la norme. En particulier, le SDT a intégré une approche visant à habiliter l'industrie à identifier, à évaluer et à corriger les lacunes

dans la mise en œuvre de certaines exigences. L'intention est de changer la manière de considérer les infractions dans ces exigences, de sorte qu'il ne s'agisse plus de savoir *si* une lacune existe, mais plutôt d'identifier, d'évaluer et de corriger les lacunes. Ceci est présenté dans ces exigences en modifiant la notion de « mise en œuvre » de la façon suivante :

> Chaque entité responsable doit mettre en œuvre**, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes…**

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité devrait inclure autant qu'elle le juge nécessaire à leurs processus documentés, pourvu que les exigences pertinentes soient couvertes. Les processus documentés eux-mêmes n'ont pas à intégrer la démarche « détecter, évaluer et corriger les lacunes » décrite au paragraphe précédent, car cette démarche est liée à la manière de mettre en œuvre les processus documentés et pourrait être réalisée par d'autres mesures de contrôle ou de gestion de la conformité.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », lorsque cela a du sens et est communément compris. Par exemple, les processus documentés qui décrivent une réponse sont généralement appelés « plans » (plan d'action en cas d'incident, plan de rétablissement, etc.). De plus, un plan de sécurité peut décrire une approche comportant plusieurs procédures couvrant un thème étendu.

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont un exemple trouvé dans les normes. La mise en œuvre complète des normes CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

Les entités responsables peuvent mettre en œuvre des moyens communs qui répondent aux besoins de plusieurs *systèmes électroniques BES* à impact élevé et moyen. Par exemple, un même programme de formation pourrait répondre aux exigences en formation du personnel de plusieurs *systèmes électroniques BES*.

Les mesures présentent des exemples de pièces justificatives pour montrer la documentation et la mise en œuvre de l'exigence. Ces mesures servent à fournir des conseils aux entités sur ce qui peut constituer des dossiers de conformité acceptables et ne devraient pas être considérées comme une liste exhaustive.

Dans l'ensemble des normes, sauf indication particulière, les éléments présentés à la section Exigences et mesures sous forme de liste à puces sont liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances de systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes de DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

Colonnes « Systèmes visés » des tableaux

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. Le SDT CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- **Systèmes électroniques BES à impact élevé –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes électroniques BES à impact moyen –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes de contrôle ou de surveillance des accès électroniques (EACMS) –** Désigne tout *système de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d'authentification, et systèmes de surveillance de registre d'événement et d'alerte.
- **Systèmes de contrôle des accès physiques (PACS) –** Désigne tout *système de contrôle des accès physique*s associé à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.
- **Actifs électroniques protégés (PCA) –** Désigne tout *actif électronique protégé* associé à un *système électronique BES* à impact élevé ou moyen visé.

B. Exigences et mesures

E1. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-010-1) – Gestion des changements de configuration. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation].*

M1. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-010-1) – Gestion des changements de configuration, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-010-1) – Gestion des changements de configuration

Partie	Systèmes visés	Exigences	Mesures
1.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Établir une configuration de référence, individuellement ou par groupe, qui doit comprendre les points suivants : 1.1.1. système(s) d'exploitation (y compris la version), ou système embarqué en l'absence de système d'exploitation indépendant ; 1.1.2. tout logiciel commercial ou logiciel libre (y compris la version) installé intentionnellement ; 1.1.3. tout logiciel personnalisé installé ; 1.1.4. tout port logique accessible par le réseau ; et 1.1.5. toute rustine de sécurité appliquée.	Exemples non limitatifs de pièces justificatives : • feuille de calcul indiquant les éléments de configuration de référence requis pour chaque *actif électronique*, individuellement ou par groupe ; ou • enregistrement dans un système de gestion d'actifs indiquant les éléments de configuration de référence requis pour chaque *actif électronique*, individuellement ou par groupe.

Tableau E1 (CIP-010-1) – Gestion des changements de configuration			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Autoriser et documenter tout changement par rapport à la configuration de référence existante.	Exemples non limitatifs de pièces justificatives : • enregistrement de demande de changement et autorisation électronique correspondante (accordée par une personne ou un groupe dûment habilité), pour chaque changement, dans un système de gestion des changements ; ou • documentation attestant que le changement a été effectué conformément à l'exigence.
1.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Pour tout changement par rapport à la configuration de référence existante, mettre à jour la configuration de référence dans les 30 jours civils suivant l'exécution du changement.	Exemple non limitatif de pièce justificative : documentation de la configuration de référence avec mise à jour datée d'au plus 30 jours civils après la date d'exécution du changement.

Tableau E1 (CIP-010-1) – Gestion des changements de configuration			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.4	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Pour tout changement par rapport à la configuration de référence existante : 1.4.1. avant le changement, déterminer les mécanismes de cybersécurité de CIP-005 et CIP-007 qui pourraient être touchés par le changement ; 1.4.2. après le changement, vérifier que les mécanismes de cybersécurité déterminés en 1.4.1 ne sont pas dégradés ; et 1.4.3. documenter les résultats de la vérification.	Exemple non limitatif de pièce justificative : liste de mécanismes de cybersécurité vérifiés ou mis à l'essai, avec résultats d'essai datés.

Tableau E1 (CIP-010-1) – Gestion des changements de configuration			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.5	*Systèmes électroniques BES* à impact élevé.	Lorsque techniquement faisable, pour chaque changement par rapport à la configuration de référence existante : 1.5.1. avant de mettre en œuvre un changement dans l'environnement de production, mettre à l'essai le changement dans un environnement d'essai ou mettre à l'essai le changement dans un environnement de production où l'essai est effectué d'une manière qui réduit au minimum les effets adverses, en simulant la configuration de référence de manière à s'assurer que les mécanismes de cybersécurité de CIP-005 et CIP-007 ne sont pas dégradés ; et 1.5.2. documenter les résultats des essais et, si un environnement d'essai est utilisé, les différences entre celui-ci et l'environnement de production, y compris la description des mesures visant à tenir compte des différences de fonctionnement entre les environnements d'essai et de production.	Exemple non limitatif de pièce justificative : liste des mécanismes de cybersécurité mis à l'essai avec résultats d'essai concluants, liste de différences entre les environnements d'essai et de production et description des mesures visant à tenir compte des différences de fonctionnement, y compris la date de l'essai.

E2. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-010-1) – Surveillance de configuration. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]*.

M2. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-010-1) – Surveillance de configuration, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-010-1) – Surveillance de la configuration			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PCA associés.	Surveiller au moins une fois tous les 35 jours civils les changements dans la configuration de référence (tel que décrit à l'exigence E1, partie 1.1). Documenter tout changement non autorisé détecté et faire enquête.	Exemples non limitatifs de pièces justificatives : registres d'un système de surveillance de configuration et dossiers d'enquête pour tout changement non autorisé détecté.

E3. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E3 (CIP-010-1) – Analyses de vulnérabilité. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification à long terme et planification de l'exploitation]*

M3. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E3 (CIP-010-1) – Analyses de vulnérabilité, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E3 (CIP-010-1) – Analyses de vulnérabilité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Au moins tous les 15 mois civils, effectuer une analyse de vulnérabilité sur papier ou active.	Exemples non limitatifs de pièces justificatives : • document indiquant la date de l'analyse (effectuée au moins une fois tous les 15 mois civils), les mécanismes évalués pour chaque *système électronique BES* et la méthode d'analyse ; ou • document indiquant la date de l'analyse et le résultat produit par tout outil utilisé pour l'analyse.

Tableau E3 (CIP-010-1) – Analyses de vulnérabilité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*Systèmes électroniques BES* à impact élevé.	Lorsque techniquement faisable, au moins une fois tous les 36 mois civils : 3.2.1 effectuer une analyse de vulnérabilité active dans un environnement d'essai, ou effectuer une analyse de vulnérabilité active dans un environnement de production où l'essai est réalisé d'une manière qui réduit au minimum les effets adverses, en simulant la configuration de référence du *système électronique BES* dans un environnement de production ; et 3.2.2 documenter les résultats des essais et, si un environnement d'essai a été utilisé, les différences entre l'essai et l'environnement de production, y compris la description des mesures visant à tenir compte des différences de fonctionnement entre les environnements d'essai et de production.	Exemples non limitatifs de pièces justificatives : document indiquant la date de l'analyse (effectuée au moins une fois tous les 36 mois civils), résultat produit par les outils utilisés pour effectuer l'analyse et liste des différences entre les environnements de production et d'essai, avec explications sur la prise en compte des différences dans l'analyse.

Tableau E3 (CIP-010-1) – Analyses de vulnérabilité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PCA associés.	Avant d'ajouter un nouvel *actif électronique* visé à un environnement de production, effectuer une analyse de vulnérabilité active du nouvel *actif électronique*, sauf dans des *circonstances CIP exceptionnelles* ou pour un remplacement d'un *actif électronique* existant par un équivalent dont la configuration de référence simule celle de l'*actif électronique* remplacé ou d'un autre *actif électronique* existant.	Exemples non limitatifs de pièces justificatives : document indiquant la date de l'analyse (effectuée avant la mise en service du nouvel *actif électronique*) et le résultat produit par les outils utilisés pour l'analyse.
3.4	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Documenter les résultats des analyses effectuées conformément aux parties 3.1, 3.2 et 3.3 ainsi que le plan d'action visant à corriger ou à atténuer les vulnérabilités identifiées lors des analyses, en précisant la date prévue d'achèvement du plan d'action et l'état d'exécution de toute mesure de correction ou d'atténuation.	Exemples non limitatifs de pièces justificatives : document donnant les résultats de l'examen ou de l'analyse, liste des mesures à prendre, dates proposées d'achèvement du plan d'action et dossier de l'état d'exécution des mesures à prendre (procès-verbaux de réunion d'étape, mises à jour dans un système de bons de travail ou suivi des mesures au moyen d'une feuille de calcul).

C. Conformité

1. Processus de surveillance de la conformité :

1.1. Responsable de la surveillance de l'application des normes :

L'entité régionale joue le rôle de responsable de la surveillance de l'application des normes (CEA), à moins que l'entité concernée soit détenue, exploitée ou contrôlée par l'entité régionale. Dans de tels cas, le rôle de CEA est confié à l'ERO, à une entité régionale approuvée par la FERC ou à un autre organisme gouvernemental pertinent.

1.2. Conservation des pièces justificatives :

Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces justificatives afin de démontrer sa conformité. Dans les cas où la période de conservation des pièces justificatives indiquée est plus courte que le temps écoulé depuis le dernier audit, le CEA peut demander à l'entité de fournir d'autres pièces justificatives pour montrer qu'elle était conforme pendant la période complète écoulée depuis le dernier audit.

L'entité responsable doit conserver les données ou pièces justificatives attestant de sa conformité de la façon indiquée ci-après, à moins que son CEA lui demande de conserver certains documents plus longtemps dans le cadre d'une enquête :

- Chaque entité responsable doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité responsable est jugée non conforme, elle doit conserver l'information relative à cette non-conformité jusqu'à ce que les correctifs aient été appliqués et approuvés ou pendant la période indiquée ci-dessus, selon la durée la plus longue.
- Le CEA doit conserver les derniers dossiers d'audit ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Processus de surveillance et d'évaluation de la conformité :

- Audits de conformité
- Déclarations sur la conformité
- Contrôles ponctuels
- Enquêtes sur les non-conformités
- Déclarations volontaires
- Plaintes

1.4. Autres informations sur la conformité :

- Aucun

2. Tableau des éléments de conformité

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	**Planification de l'exploitation**	**Moyen**	L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend seulement quatre des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1) OU L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend tous les éléments de référence exigés en 1.1.1 à 1.1.5 et a identifié les lacunes, mais elle n'a pas évalué et corrigé les lacunes. (1.1)	L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend seulement trois des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1) OU L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend quatre des éléments de référence exigés en 1.1.1 à 1.1.5 et a identifié les lacunes, mais elle n'a pas évalué et corrigé les lacunes. (1.1)	L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend seulement deux des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1) OU L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend trois des éléments de référence exigés en 1.1.1 à 1.1.5 et a identifié les lacunes, mais elle n'a pas évalué et corrigé les lacunes. (1.1)	L'entité responsable n'a documenté ou mis en œuvre aucun processus de gestion des changements de configuration. (E1) OU L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend seulement un des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1) OU L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			OU L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend tous les éléments de référence exigés en 1.1.1 à 1.1.5, mais elle n'a pas identifié, évalué et corrigé les lacunes. (1.1) OU L'entité responsable a un ou des processus pour réaliser les étapes de 1.4.1 et 1.4.2 pour un ou des changements par rapport à la configuration de référence existante et a identifié les lacunes dans la documentation	OU L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend quatre des éléments de référence exigés en 1.1.1 à 1.1.5, mais elle n'a pas identifié, évalué et corrigé les lacunes. (1.1) OU L'entité responsable a un ou des processus pour déterminer les mécanismes de sécurité requis dans CIP-005 et CIP-007 qui pourraient être touchés par un ou des changements par rapport à la configuration de	OU L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend trois des éléments de référence exigés en 1.1.1 à 1.1.5, mais elle n'a pas identifié, évalué et corrigé les lacunes. (1.1) OU L'entité responsable a un ou des processus qui exigent l'autorisation et la documentation des changements par rapport à la configuration de référence existante et a identifié les lacunes, mais elle n'a pas évalué	comprend deux des éléments de référence exigés en 1.1.1 à 1.1.5 ou moins et a identifié les lacunes, mais elle n'a pas évalué et corrigé les lacunes. (1.1) OU L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprend deux des éléments de référence exigés en 1.1.1 à 1.1.5 ou moins, mais elle n'a pas identifié, évalué et corrigé les lacunes. (1.1) OU L'entité responsable n'a pas un ou des processus qui exigent

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			de vérification, mais elle n'a pas évalué ou corrigé les lacunes. (1.4.3). OU L'entité responsable a un ou des processus pour réaliser les étapes de 1.4.1 et 1.4.2 pour un ou des changements par rapport à la configuration de référence existante, mais elle n'a pas identifié, évalué ou corrigé les lacunes dans la documentation de vérification. (1.4.3).	référence existante et a identifié les lacunes dans la détermination des mécanismes de sécurité affectés, mais elle n'a pas évalué ou corrigé les lacunes. (1.4.1) OU L'entité responsable a un ou des processus pour déterminer les mécanismes de sécurité requis dans CIP-005 et CIP-007 qui pourraient être touchés par un ou des changements par rapport à la configuration de référence existante, mais elle n'a pas identifié, évalué ou corrigé les lacunes dans la détermination des mécanismes de sécurité affectés.	ou corrigé les lacunes. (1.2) OU L'entité responsable a un ou des processus qui exigent l'autorisation et la documentation des changements par rapport à la configuration de référence existante, mais elle n'a pas identifié, évalué ou corrigé les lacunes. (1.2) OU L'entité responsable a un ou des processus pour mettre à jour la configuration de référence dans les 30 jours civils suivant l'exécution de changements par rapport à la	l'autorisation et la documentation des changements par rapport à la configuration de référence existante. (1.2) OU L'entité responsable n'a pas un ou des processus pour mettre à jour la configuration de référence dans les 30 jours civils suivant l'exécution de changements par rapport à la configuration de référence existante. (1.3) OU L'entité responsable a un ou des processus pour déterminer les mécanismes de sécurité requis dans

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				(1.4.1)	configuration de référence existante et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes. (1.3) OU L'entité responsable a un ou des processus pour mettre à jour la configuration de référence dans les 30 jours civils suivant l'exécution de changements par rapport à la configuration de référence existante, mais elle n'a pas identifié, évalué ou corrigé les lacunes. (1.3) OU L'entité responsable a un ou des processus pour vérifier que les	CIP-005 et CIP-007 qui pourraient être touchés par un ou des changements par rapport à la configuration de référence existante, mais elle n'a pas vérifié et documenté que les mécanismes requis n'étaient pas affectés négativement suivant le changement. (1.4.2 et 1.4.3) OU L'entité responsable n'a pas de processus pour mettre à l'essai les changements dans un environnement qui simule la configuration de référence avant de mettre en œuvre un changement par rapport à la configuration de

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					mécanismes de sécurité requis dans CIP-005 et CIP-007 ne sont pas affectés négativement par un ou des changements par rapport à la configuration de référence existante et a identifié les lacunes dans les mécanismes requis, mais elle n'a pas évalué ou corrigé les lacunes. (1.4.2) OU L'entité responsable a un ou des processus pour vérifier que les mécanismes de sécurité requis dans CIP-005 et CIP-007 ne sont pas affectés négativement par un ou des changements par rapport à la configuration de référence existante,	référence. (1.5.1) OU L'entité responsable n'a pas de processus pour documenter les résultats de l'essai et, si un environnement d'essai est utilisé, pour documenter les différences entre les environnements d'essai et de production. (1.5.2)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					mais elle n'a pas identifié, évalué ou corrigé les lacunes dans les mécanismes requis. (1.4.2) OU L'entité responsable a un processus pour mettre à l'essai les changements dans un environnement qui simule la configuration de référence avant de mettre en œuvre un changement par rapport à la configuration de référence, et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes. (1.5.1) OU L'entité responsable a un processus pour mettre à l'essai les	

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					changements dans un environnement qui simule la configuration de référence avant de mettre en œuvre un changement par rapport à la configuration de référence, mais elle n'a pas identifié, évalué ou corrigé les lacunes. (1.5.1) OU L'entité responsable a un processus pour documenter les résultats de l'essai et, si un environnement d'essai est utilisé, pour documenter les différences entre les environnements d'essai et de production, et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes.	

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					(1.5.2) OU L'entité responsable a un processus pour documenter les résultats de l'essai et, si un environnement d'essai est utilisé, pour documenter les différences entre les environnements d'essai et de production, mais elle n'a pas identifié, évalué ou corrigé les lacunes. (1.5.2)	
E2	**Planification de l'exploitation**	**Moyen**	Sans objet	Sans objet	Sans objet	L'entité responsable n'a pas documenté ou mis en œuvre un ou des processus pour surveiller, enquêter et documenter les changements non autorisés détectés à la référence au moins une fois tous les 35

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						jours civils. (2.1) OU L'entité responsable a documenté et mis en œuvre un ou des processus pour surveiller, enquêter et documenter les changements non autorisés détectés à la référence au moins une fois tous les 35 jours civils et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes. (2.1) OU L'entité responsable a documenté et mis en œuvre un ou des processus pour surveiller, enquêter et documenter les changements non autorisés détectés à la

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						référence au moins une fois tous les 35 jours civils, mais elle n'a pas identifié, évalué ou corrigé les lacunes. (2.1)
E3	**Planification à long terme et planification de l'exploitation**	**Moyen**	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 15 mois, mais en moins de 18 mois suivant la dernière analyse de l'un de ses *systèmes électroniques BES* visés. (3.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus	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 18 mois, mais en moins de 21 mois suivant la dernière analyse de l'un de ses *systèmes électroniques BES* visés. (3.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus	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 21 mois, mais en moins de 24 mois suivant la dernière analyse de l'un de ses *systèmes électroniques BES* visés. (3.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus	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

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active plus de 36 mois, mais en moins de 39 mois suivant la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2)	documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active plus de 39 mois, mais en moins de 42 mois suivant la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2)	documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active plus de 42 mois, mais en moins de 45 mois suivant la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2)	dernière analyse de l'un de ses *systèmes électroniques BES* visés. (3.1) OU 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 plus de 45 mois suivant la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2) OU L'entité responsable a mis en œuvre et documenté un ou plusieurs processus d'analyse de vulnérabilité pour

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						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) 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 n'a pas documenté les résultats des analyses de vulnérabilité, les plans d'action pour remédier ou mitiger les vulnérabilités relevées

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						dans les analyses, la date planifiée d'achèvement du plan d'action et l'état d'exécution des plans de mitigation. (3.4)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Annexe QC-CIP-010-1
Dispositions particulières de la norme CIP-010-1 applicables au Québec

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son 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 aura préséance.

A. Introduction

1. **Titre :** Cybersécurité — Gestion des changements de configuration et analyses de vulnérabilité

2. **Numéro :** CIP-010-1

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

   Entités fonctionnelles

   Aucune disposition particulière

   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 :

   - Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur 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 201x

   5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 201x

   5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : xx mois 201x

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable de la surveillance de l'application des normes

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et d'évaluation de la conformité

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	Xx mois 201x	Nouvelle annexe	Nouvelle

A. Introduction

1. Titre : Cybersécurité — Protection de l'information

2. Numéro : CIP-011-1

3. Objet : Empêcher tout accès non autorisé à l'information de *système électronique BES* en définissant des exigences de protection de l'information visant à prévenir toute compromission pouvant entraîner un fonctionnement incorrect ou une instabilité dans le BES.

4. Applicabilité :

4.1. Entités fonctionnelles : Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

4.1.1 Responsable de l'équilibrage

4.1.2 Distributeur qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du BES :

4.1.2.1 Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :

4.1.2.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.1.2.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.1.2.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.1.2.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

4.2. Installations : Dans le contexte des exigences de la présente norme, les *installations*, systèmes et équipements suivants détenus par chaque entité responsable indiquée à la section 4.1 sont ceux auxquels ces exigences sont applicables. Dans le cas des exigences de cette norme qui visent un type particulier d'*installations*, de système ou d'équipements, ou un sous-ensemble d'*installations*, de systèmes ou d'équipements, ceux-ci sont précisés explicitement.

4.2.1 Distributeur : Un ou plusieurs des *installations*, systèmes et équipements suivants détenus par le distributeur pour la protection ou la remise en charge du BES :

4.2.1.1 Chaque système de DSF ou de DST qui :

4.2.1.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et

4.2.1.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.

4.2.1.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

4.2.3 Exemptions : Sont exemptés de la norme CIP-011-1 :

4.2.3.1 Les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire ;

4.2.3.2 les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électroniques* distincts ;

4.2.3.3 les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme à la norme CFR 10, section 73.54 ;

4.2.3.4 dans le cas des distributeurs, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus ;

4.2.3.5 les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* catégorisés comme impact élevé ou impact moyen en conformité avec le processus d'identification et de catégorisation de la CIP-002-5.

5. Dates de mise en vigueur

1. **24 mois minimum** – La norme CIP-011-1 entrera en vigueur soit le 1er juillet 2015, soit le premier jour civil du neuvième trimestre civil suivant l'entrée en vigueur de l'ordonnance d'approbation réglementaire appropriée, selon le délai le plus long.
2. Dans les juridictions où aucune approbation réglementaire n'est requise, la norme CIP-011-1 entrera en vigueur le premier jour du neuvième trimestre civil suivant l'approbation par le Conseil d'administration, ou selon les modalités d'approbation prévues par la loi pour les organismes gouvernementaux chargés de la fiabilité électrique (ERO).

6. Contexte :

La norme CIP-011-1 fait partie d'une série de normes CIP sur la cybersécurité. La norme CIP-002-5 exige l'identification et la catégorisation initiales des *systèmes électroniques BES*. Les normes CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 et CIP-011-1 exigent un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*. Cette série de normes CIP est appelée « version 5 des normes CIP sur la cybersécurité ».

La plupart des exigences commencent ainsi : « Chaque entité responsable doit mettre en œuvre un ou plusieurs [processus, plans, etc.] documentés qui correspondent à toutes les parties d'exigence applicables du tableau [référence au tableau]. » Le tableau en référence précise les éléments qui doivent être inclus dans les procédures pour le thème commun de l'exigence.

Le SDT a intégré à la présente norme une reconnaissance à l'effet que certaines exigences ne devraient pas mettre l'accent sur les cas individuels de défaillance comme seul motif d'infraction à la norme. En particulier, le SDT a intégré une approche visant à habiliter l'industrie à identifier, à évaluer et à corriger les lacunes dans la mise en œuvre de certaines exigences. L'intention est de changer la manière

de considérer les infractions dans ces exigences, de sorte qu'il ne s'agisse plus de savoir *si* une lacune existe, mais plutôt d'identifier, d'évaluer et de corriger les lacunes. Ceci est présenté dans ces exigences en modifiant la notion de « mise en œuvre » de la façon suivante :

> Chaque entité responsable doit mettre en œuvre**, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes…**

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité devrait inclure autant qu'elle le juge nécessaire à leurs processus documentés, pourvu que les exigences pertinentes soient couvertes. Les processus documentés eux-mêmes n'ont pas à intégrer la démarche « détecter, évaluer et corriger les lacunes » décrite au paragraphe précédent, car cette démarche est liée à la manière de mettre en œuvre les processus documentés et pourrait être réalisée par d'autres mesures de contrôle ou de gestion de la conformité.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », lorsque cela a du sens et est communément compris. Par exemple, les processus documentés qui décrivent une réponse sont généralement appelés « plans » (plan d'action en cas d'incident, plan de rétablissement, etc.). De plus, un plan de sécurité peut décrire une approche comportant plusieurs procédures couvrant un thème étendu.

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont un exemple trouvé dans les normes. La mise en œuvre complète des normes CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

Les entités responsables peuvent mettre en œuvre des moyens communs qui répondent aux besoins de plusieurs *systèmes électroniques BES* à impact élevé et moyen. Par exemple, un même programme de formation pourrait répondre aux exigences en formation du personnel de plusieurs *systèmes électroniques BES*.

Les mesures présentent des exemples de pièces justificatives pour montrer la documentation et la mise en œuvre de l'exigence. Ces mesures servent à fournir des conseils aux entités sur ce qui peut constituer des dossiers de conformité acceptables et ne devraient pas être considérées comme une liste exhaustive.

Dans l'ensemble des normes, sauf indication particulière, les éléments présentés à la section Exigences et mesures sous forme de liste à puces sont liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances de systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes de DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

Colonnes « Systèmes visés » des tableaux :
Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. Le SDT CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- **Systèmes électroniques BES à impact élevé –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes électroniques BES à impact moyen –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », conformément aux processus d'identification et de catégorisation de la norme CIP-002-5.
- **Systèmes de contrôle ou de surveillance des accès électroniques (EACMS) –** Désigne tout *système de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d'authentification, et systèmes de surveillance de registre d'événement et d'alerte.
- **Systèmes de contrôle des accès physiques (PACS) –** Désigne tout *système de contrôle des accès physique*s associé à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.
- **Actifs électroniques protégés (PCA) –** Désigne tout *actif électronique protégé* associé à un *système électronique BES* à impact élevé ou moyen visé.

B. Exigences et mesures

E1. Chaque entité responsable doit mettre en œuvre, d’une manière permettant d'identifier, d’évaluer et de corriger les lacunes, un ou plusieurs programmes documentés de protection de l’information qui, collectivement, comprennent toutes les parties d’exigence applicables du tableau E1 (CIP-011-1) – Protection de l’information. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]*

M1. Les pièces justificatives attestant du programme de protection de l’information doivent comprendre toutes les parties d’exigence applicables du tableau E1 (CIP-011-1) – Protection de l’information, et des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-011-1) – Protection de l'information			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; et 2. PACS associés.	Méthode(s) permettant d'identifier l'information qui répond à la définition d'*information de système électronique BES*.	Exemples non limitatifs de pièces justificatives acceptables : • méthode documentée permettant d'identifier l'*information de système électronique BES* à partir du programme de protection de l'information de l'entité ; ou • indications sur l'information (étiquetage, classification, etc.) qui identifie l'*information de système électronique BES* telle que désignée dans le programme de protection de l'information de l'entité ; ou • matériel de formation qui donne au personnel des connaissances suffisantes pour reconnaître l'*information de système électronique BES* ; ou • référentiel ou emplacement électronique et physique affecté au stockage de l'*information de système électronique BES* dans le cadre du programme de protection de l'information de l'entité.

Tableau E1 (CIP-011-1) – Protection de l'information			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; et 2. PACS associés.	Procédure(s) pour la protection et la manipulation sécuritaire de l'*information de système électronique BES*, y compris pour le stockage, le transport et l'utilisation.	Exemples non limitatifs de pièces justificatives acceptables : • procédures pour la protection et la manipulation sécuritaire de l'*information de système électronique BES*, portant sur des aspects comme le stockage, la sécurité pendant le transport et l'utilisation ; ou • enregistrements indiquant que l'*information de système électronique BES* est manipulée conformément aux procédures documentées de l'entité.

E2. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-011-1) – Réutilisation et élimination des *actifs électroniques BES*. *[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation]*

M2. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-011-1) – Réutilisation et élimination des *actifs électroniques BES*, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-011-1) – Réutilisation et élimination des actifs électroniques BES			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés.	Avant d'autoriser la réutilisation d'un *actif électronique* visé qui contient de l'*information de système électronique BES* (sauf si cet actif est réutilisé dans d'autres systèmes indiqués à la colonne Systèmes visés), l'entité responsable doit faire en sorte d'empêcher toute récupération non autorisée d'*information de système électronique BES* du support d'information de l'*actif électronique* en question.	Exemples non limitatifs de pièces justificatives acceptables : • enregistrements de suivi des mesures d'expurgation visant à empêcher toute récupération non autorisée d'*information de système électronique BES*, notamment par écrasement, purge ou destruction ; ou • enregistrements de suivi de mesures comme le cryptage, la rétention dans le *périmètre de sécurité physique* ou d'autres moyens d'empêcher la récupération non autorisée d'*information de système électronique BES*.

Tableau E2 (CIP-011-1) – Réutilisation et élimination des actifs électroniques BES			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; et *3.* PCA associés.	Avant l'élimination d'un *actif électronique* visé qui contient de l'*information de système électronique BES*, l'entité responsable doit faire en sorte d'empêcher toute récupération non autorisée d'*information de système électronique BES* de l'*actif électronique* en question, ou encore de détruire son support d'information.	Exemples non limitatifs de pièces justificatives acceptables : • enregistrements attestant que le support d'information a été détruit avant l'élimination d'un *actif électronique* visé ; ou • enregistrements attestant les mesures prises pour empêcher la récupération non autorisée d'*information de système électronique BES* d'un *actif électronique* visé avant son élimination.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable de la surveillance de l'application des normes

L’entité régionale joue le rôle de responsable de la surveillance de l’application des normes (CEA), à moins que l’entité concernée soit détenue, exploitée ou contrôlée par l’entité régionale. Dans de tels cas, le rôle de CEA est confié à l’ERO, à une entité régionale approuvée par la FERC ou à un autre organisme gouvernemental pertinent.

1.2. Conservation des pièces justificatives

Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces justificatives afin de démontrer sa conformité. Dans les cas où la période de conservation des pièces justificatives indiquée est plus courte que le temps écoulé depuis le dernier audit, le CEA peut demander à l’entité de fournir d’autres pièces justificatives pour montrer qu’elle était conforme pendant la période complète écoulée depuis le dernier audit.

L’entité responsable doit conserver les données ou pièces justificatives attestant de sa conformité de la façon indiquée ci-après, à moins que son CEA lui demande de conserver certains documents plus longtemps dans le cadre d’une enquête :

- Chaque entité responsable doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité responsable est jugée non conforme, elle doit conserver l’information relative à cette non-conformité jusqu’à ce que les correctifs aient été appliqués et approuvés ou pendant la période indiquée ci-dessus, selon la durée la plus longue.
- Le CEA doit conserver les derniers dossiers d’audit ainsi que tous les dossiers d’audit demandés et soumis par la suite.

1.3. Processus de surveillance et d’évaluation de la conformité

- Audits de conformité
- Déclarations sur la conformité
- Contrôles ponctuels
- Enquêtes sur les non-conformités
- Déclarations volontaires
- Plaintes

1.4. Autres informations sur la conformité

- Aucune

2. Tableau des éléments de conformité

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-011-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	**Planification de l’exploitation**	**Moyen**	Sans objet		L'entité responsable a mis en œuvre un programme de protection de l'*information de système électronique BES* qui comprend une ou plusieurs méthodes pour identifier l'*information de système électronique BES* et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes. (1.1) OU L'entité responsable a mis en œuvre un programme de protection de l'*information de système électronique BES* qui comprend une ou plusieurs méthodes pour identifier	L'entité responsable n'a pas documenté ou mis en œuvre un programme de protection de l'*information de système électronique BES.* (E1)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-011-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					l'*information de système électronique BES*, mais elle n'a pas identifié, évalué ou corrigé les lacunes. (1.1) OU L'entité responsable a mis en œuvre un programme de protection de l'*information de système électronique BES* qui comprend une ou plusieurs procédures pour la protection et la manipulation sécuritaire de l'*information de système électronique BES* et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes. (1.2) OU	

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-011-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					L'entité responsable a mis en œuvre un programme de protection de l'*information de système électronique BES* qui comprend une ou plusieurs procédures pour la protection et la manipulation sécuritaire de l'*information de système électronique BES*, mais elle n'a pas identifié, évalué ou corrigé les lacunes. (1.2)	
E2	**Planification de l’exploitation**	**Faible**	Sans objet	L'entité responsable a mis en œuvre un ou plusieurs processus documentés, mais n'a pas inclus de processus de réutilisation visant à empêcher la récupération non autorisée	L'entité responsable a mis en œuvre un ou plusieurs processus documentés, mais n'a pas inclus de processus de disposition ou de destruction de support afin d'empêcher la récupération non	L'entité responsable n'a pas documenté ou mis en œuvre aucun processus pour les parties d'exigence applicables du Tableau E2 (CIP 011 1) – Réutilisation et élimination des *actifs*

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-011-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				d'*information de système électronique BES* à partir de l'*actif électronique BES.* (2.1)	autorisée d'*information de système électronique BES* à partir de l'*actif électronique BES.* (2.2)	*électroniques BES.* (E2)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Annexe QC-CIP-011-1
Dispositions particulières de la norme CIP-011-1 applicables au Québec

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son 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 aura préséance.

A. Introduction

1. **Titre :** Cybersécurité — Protection de l'information

2. **Numéro :** CIP-011-1

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

   Entités fonctionnelles

   Aucune disposition particulière

   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 :

   - Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur 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 201x

   5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 201x

   5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : xx mois 201x

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. **Processus de surveillance de la conformité**

   1.1. Responsable de la surveillance de l'application des normes

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et d'évaluation de la conformité

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	Xx mois 201x	Nouvelle annexe	Nouvelle