A. Introduction

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

2. **Numéro :** CIP-005-7

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 de la présente norme, les entités fonctionnelles indiquées ci-après sont appelées collectivement « entités responsables ». Si certaines exigences visent plus spécifiquement une entité fonctionnelle ou un sous-ensemble 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 systèmes, *installations* et équipements suivants pour la protection ou la remise en charge du *BES* :

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

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

   4.1.2.1.2. effectue des délestages automatiques de *charge* de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

   4.1.2.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une *norme de fiabilité* de la NERC ou de l'*entité régionale*.

   4.1.2.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une *norme de fiabilité* de la NERC ou de l'*entité régionale*.

   4.1.2.4. *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 prochains groupes de production à démarrer.

   4.1.3. ***Exploitant d'installation de production***

   4.1.4. ***Propriétaire d'installation de production***

   4.1.5. ***Coordonnateur de la fiabilité***

   4.1.6. ***Exploitant de réseau de transport***

   4.1.7. ***Propriétaire d'installation de transport***

4.2. ***Installations*** **:** Dans le contexte de la présente norme, les systèmes, *installations* et équipements suivants détenus par une entité responsable indiquée à la section 4.1 sont visés par les exigences. Si certaines exigences visent plus spécifiquement un type ou un sous-ensemble de systèmes, d'*installations* ou d'équipements, ceux-ci sont précisés explicitement.

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

4.2.1.1. Système de DSF ou de DST qui :

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

4.2.1.1.2. effectue des délestages de *charge* automatiques de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

4.2.1.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une *norme de fiabilité* de la NERC ou de l'*entité régionale*.

4.2.1.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une *norme de fiabilité* de la NERC ou de l'*entité régionale*.

4.2.1.4. *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 prochains groupes de production 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-005-7 :

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 *périmètres de sécurité électronique* 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 au règlement 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 ont déterminé n'avoir aucun *système électronique BES* classé dans les catégories « impact élevé » ou « impact moyen » selon le processus d'inventaire et de catégorisation prescrit dans la norme CIP-002.

5. Date d'entrée en vigueur :

Voir le plan de mise en œuvre du projet 2019-03.

6. Contexte :

La norme CIP-005 fait partie d'une série de normes CIP sur la cybersécurité qui exigent l'inventaire et la catégorisation initiales des *systèmes électroniques BES*, ainsi qu'un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.

La plupart des exigences commencent ainsi : « Chaque entité responsable doit mettre en œuvre un ou plusieurs [processus, plans, etc.] documentés qui couvrent tous les alinéas 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 doit inclure tout ce qu'elle le juge nécessaire dans ses processus documentés, en s'assurant de bien couvrir les exigences pertinentes.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », dans la mesure où la compréhension relève du bon sens. 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 des exemples qui figurent 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 concernant plusieurs *systèmes électroniques BES*.

Les mesures auxquelles renvoie l'énoncé initial de l'exigence correspondent simplement aux processus documentés eux-mêmes. La colonne « Mesures » présente des exemples de pièces justificatives attestant la documentation et la mise en œuvre des éléments pertinents dans les processus documentés ; ces exemples sont présentés à titre indicatif, et leur liste ne doit pas être considérée comme 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 de DSF et de DST. Ce seuil particulier de 300 MW pour les systèmes de DSF et de DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes de DST et de DSF, qui constituent des efforts de dernier

recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances des systèmes de 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 de 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. L'équipe de rédaction (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 », selon les processus d'inventaire et de catégorisation de la norme CIP-002.
- ***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 », selon les processus d'inventaire et de catégorisation de la norme CIP-002.
- ***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.
- ***Systèmes de contrôle des accès physiques* (*PACS*)** – Désigne tout *système de contrôle des accès physiques* associé à un *système électronique BES* à impact élevé ou moyen visé.

- ***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'événements et d'alerte.

B. Exigences et mesures

E1. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-005-7) – *Périmètre de sécurité électronique*.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation et exploitation le même jour]

M1. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-005-7) – *Périmètre de sécurité électronique*, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-005-7) – *Périmètre de sécurité électronique*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.1	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : • les *PCA* associés.	Tous les *actifs électroniques* visés 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* visés à identifiant unique qui sont reliés au moyen d'un protocole routable dans chaque *ESP*.
1.2	*Systèmes électroniques BES* à impact élevé à *connectivité externe routable* et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : • les *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, y compris 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-005-7) – *Périmètre de sécurité électronique*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.4	*Systèmes électroniques BES* à impact élevé à *connectivité par lien commuté* et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité par lien commuté* et : • les *PCA* associés.	Lorsque techniquement faisable, effectuer l'authentification lors de l'établissement de la *connectivité par lien commuté* avec les *actifs électroniques* visés.	Exemple non limitatif de pièce justificative : processus documenté décrivant la méthode utilisée par l'entité responsable afin d'assurer l'authentification des accès effectués pour 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 doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, et lorsque c'est techniquement faisable, couvrent tous les alinéas applicables du tableau E2 (CIP-005-7) – Gestion des accès distants. *[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation et exploitation le même jour]*

M2. Les pièces justificatives doivent comprendre les processus documentés qui, collectivement, traitent de chacun des alinéas applicables du tableau E2 (CIP-005-7) – Gestion des accès distants, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-005-7) – Gestion des accès distants			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : • les *PCA* associés.	Pour tous les *accès distants interactifs*, utiliser un *système intermédiaire* de façon que l'*actif électronique* qui commande 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 : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : • les *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-005-7) – Gestion des accès distants			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.3	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : • les *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.
2.4	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : • les *PCA* associés.	Disposer d'une ou de plusieurs méthodes permettant de déterminer les sessions actives d'accès distant par des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système).	Exemples non limitatifs de pièces justificatives : documentation des méthodes utilisées pour déterminer les sessions actives d'accès distant par des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système), par exemple : • méthodes d'accès aux informations journalisées ou de surveillance pour déterminer les

Tableau E2 (CIP-005-7) – Gestion des accès distants			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
			sessions actives d'accès distant par des fournisseurs ; • méthodes de surveillance de l'activité (par exemple, tableaux des connexions ou compteurs de règles dans un pare-feu, ou surveillance de l'activité des utilisateurs) ou des ports ouverts (par exemple, commandes netstat ou connexes pour afficher les ports en activité) permettant de déterminer les sessions actives d'accès distant de système à système ; ou • méthodes de contrôle des accès distants commandés par les fournisseurs, par exemple l'exigence que ceux-ci téléphonent pour demander un deuxième facteur d'identification afin d'établir un accès distant.

Tableau E2 (CIP-005-7) – Gestion des accès distants			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.5	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : • les *PCA* associés.	Disposer d'une ou de plusieurs méthodes permettant de désactiver les accès distants actifs des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système).	Exemples non limitatifs de pièces justificatives : documentation des méthodes utilisées pour désactiver les accès distants actifs des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système), par exemple : • méthodes permettant de désactiver l'accès distant des fournisseurs au *point d'accès électronique* applicable dans le cas d'un accès distant de système à système ; ou • méthodes permettant de désactiver l'*accès distant interactif* des fournisseurs au *système intermédiaire* applicable.

E3. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent les alinéas applicables du tableau E3 (CIP-005-7) – Gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS*.
[Facteur de risque de non-conformité : Moyen] [Horizon : planification de l'exploitation et exploitation le même jour]

M3. Les pièces justificatives doivent comprendre les processus documentés qui, collectivement, traitent de chacun des alinéas applicables du tableau E3 (CIP-005-7) – Gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS*, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E3 (CIP-005-7) – Gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*EACMS* et *PACS* associés à des *systèmes électroniques BES* à impact élevé *EACMS* et *PACS* associés à des *systèmes électroniques BES* à impact moyen à *connectivité externe routable*	Disposer d'une ou de plusieurs méthodes pour déterminer les connexions à distance authentifiées commandées par des fournisseurs.	Exemples non limitatifs de pièces justificatives : documentation des méthodes utilisées pour déterminer les connexions à distance authentifiées commandées par des fournisseurs, notamment : • méthodes d'accès aux informations journalisées ou de surveillance pour déterminer les connexions à distance authentifiées commandées par des fournisseurs.

Tableau E3 (CIP-005-7) – Gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*EACMS* et *PACS* associés à des *systèmes électroniques BES* à impact élevé *EACMS* et *PACS* associés à des *systèmes électroniques BES* à impact moyen à *connectivité externe routable*	Disposer d'une ou de plusieurs méthodes pour interrompre les connexions à distance authentifiées commandées par des fournisseurs, et pour contrôler la possibilité de reconnexion.	Exemples non limitatifs de pièces justificatives : documentation des méthodes utilisées pour interrompre les connexions à distance authentifiées commandées par des fournisseurs avec les systèmes visés. Par exemple, interrompre un outil, un processus ou une session actif commandé par un fournisseur, ou abandonner au niveau du pare-feu une connexion active commandée par un fournisseur. Les méthodes permettant de contrôler la possibilité de reconnexion, si nécessaire, pourraient être par exemple : désactiver un compte Active Directory ; désactiver un jeton de sécurité ; restreindre au niveau du pare-feu des adresses IP en provenance de fournisseurs ; ou débrancher physiquement un câble réseau afin d'empêcher la reconnexion.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Le terme « *responsable des mesures pour assurer la conformité* » (*CEA*) désigne la NERC ou l'*entité régionale*, ou toute entité désignée par un organisme gouvernemental pertinent, dans leurs rôles respectifs visant à surveiller et à assurer la conformité avec les *normes de fiabilité* obligatoires et exécutoires de la NERC dans leurs territoires respectifs.

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 attestant sa conformité pendant la période complète écoulée depuis le dernier audit.

L'entité visée doit conserver les données ou pièces justificatives attestant sa conformité selon les modalités indiquées ci-après, à moins que son *CEA* lui demande de conserver certaines pièces justificatives plus longtemps dans le cadre d'une enquête.

- Chaque entité visée doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité visée 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 dossiers de l'audit le plus récent ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Programme de surveillance de la conformité et d'application des normes

Selon la définition des règles de procédure de la NERC, l'expression « programme de surveillance de la conformité et d'application des normes » désigne la liste des processus qui serviront à évaluer les données ou l'information afin de déterminer les résultats de conformité avec la *norme de fiabilité*.

Niveaux de gravité de la non-conformité (VSL)

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E1.			L'entité responsable n'avait pas un moyen de détection des communications entrantes et sortantes malveillantes. (1.5)	L'entité responsable n'avait pas documenté un ou plusieurs processus pour le tableau E1 (CIP-005-7) – *Périmètre de sécurité électronique*. (E1) OU Tous les *actifs électroniques* visés de l'entité responsable qui sont reliés à un réseau au moyen d'un protocole routable n'étaient pas à l'intérieur d'un *périmètre de sécurité électronique* (*ESP*) défini. (1.1) OU La *connectivité externe routable* à travers l'*ESP* n'était pas effectuée par l'intermédiaire d'un *EAP* identifié. (1.2) OU L'entité responsable n'a pas exigé d'autorisations pour les accès entrants et sortants et refusé tout autre accès par défaut. (1.3) OU L'entité responsable n'a pas effectué l'authentification lors de l'établissement de la connectivité par lien commuté avec les *actifs*

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
				électroniques visés, lorsque techniquement faisable. (1.4)
E2.	L'entité responsable n'a pas de processus documentés pour un ou plusieurs des éléments visés des alinéas 2.1 à 2.3.	L'entité responsable n'a pas mis en œuvre de processus pour un des éléments visés des alinéas 2.1 à 2.3.	L'entité responsable n'a pas mis en œuvre de processus pour deux des éléments visés des alinéas 2.1 à 2.3. OU L'entité responsable ne disposait pas : soit d'une ou de plusieurs méthodes permettant de déterminer les sessions actives d'accès distant par des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système) (2.4) ; soit d'une ou de plusieurs méthodes permettant de désactiver les accès distants actifs des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système (2.5).	L'entité responsable n'a pas mis en œuvre de processus pour trois des éléments visés des alinéas 2.1 à 2.3. OU L'entité responsable ne disposait : ni d'une ou de plusieurs méthodes permettant de déterminer les sessions actives d'accès distant par des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système) (2.4) ; ni d'une ou de plusieurs méthodes permettant de désactiver les accès distants actifs des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système) (2.5).
E3.	L'entité responsable n'a pas documenté un ou plusieurs processus spécifiés au tableau E3 (CIP-005-7) – Gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS*. (E3)	L'entité responsable disposait d'une ou de plusieurs méthodes spécifiées à l'alinéa 3.1 pour les *EACMS*, mais ne disposait d'aucune méthode pour déterminer les connexions à distance authentifiées	L'entité responsable n'a pas mis en œuvre de processus pour l'alinéa 3.1 ou 3.2. (E3) OU L'entité responsable disposait d'une ou de plusieurs méthodes spécifiées à l'alinéa 3.1 pour les *PACS*, mais ne disposait d'aucune	L'entité responsable n'a mis en œuvre aucun processus du tableau E3 (CIP-005-7) – Gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS*. (E3) OU

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
		commandées par des fournisseurs pour les *PACS*. (3.1) OU L'entité responsable disposait d'une ou de plusieurs méthodes spécifiées à l'alinéa 3.2 pour les *EACMS*, mais ne disposait d'aucune méthode pour interrompre les connexions à distance authentifiées commandées par des fournisseurs pour les *PACS*. (3.2)	méthode pour déterminer les connexions à distance authentifiées commandées par des fournisseurs pour les *EACMS*. (3.1) OU L'entité responsable disposait d'une ou de plusieurs méthodes spécifiées à l'alinéa 3.2 pour les *PACS*, mais ne disposait d'aucune méthode pour interrompre les connexions à distance authentifiées commandées par des fournisseurs ou pour contrôler la possibilité de reconnexion pour les *EACMS*. (3.2)	L'entité responsable ne disposait d'aucune des méthodes spécifiées aux alinéas 3.1 et 3.2. (E3)

D. Différences régionales

Aucune.

E. Documents connexes

- Plan de mise en œuvre du projet 2019-03.
- Justification technique de la norme CIP-005-7.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	16 janvier 2006	E3.2 — Remplacement de « Control Center » par « control center ».	24 mars 2006
2	30 septembre 2009	Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes. Suppression de la mention sur la prise en compte des considérations d'affaires. Remplacement de l'organisation régionale de fiabilité par l'*entité régionale* comme entité responsable. Reformulation de la date d'entrée en vigueur. Remplacement de « Responsabilité de la surveillance de la conformité » par « *Responsable des mesures pour assurer la conformité* ».	
3	16 décembre 2009	Changement du numéro de version de -2 à -3. Approbation par le Conseil d'administration de la NERC.	
3	31 mars 2010	Approbation par la FERC.	
4	30 décembre 2010	Ajout de critères précis pour l'identification des actifs critiques.	Mise à jour
4	24 janvier 2011	Approbation par le Conseil d'administration de la NERC.	Mise à jour
5	26 novembre 2012	Adoption par le Conseil d'administration de la NERC.	Modifiée en coordination avec les autres normes CIP et révision du format selon le gabarit RBS.
5	22 novembre 2013	Ordonnance de la FERC approuvant la norme CIP-005-5.	
6	20 juillet 2017	Modifications visant à répondre à certaines directives de l'Ordonnance 829 de la FERC.	Révision
6	10 août 2017	Adoption par le Conseil d'administration de la NERC.	

6	18 octobre 2018	Ordonnance de la FERC approuvant la norme CIP-005-6. Dossier RM17-13-000.	
7	1er août 2019	Modifications visant à répondre à certaines prescriptions de l'Ordonnance 850 de la FERC.	Révision
7	5 novembre 2020	Adoption par le Conseil d'administration de la NERC.	
7	18 mars 2021	Lettre d'ordonnance RD21-2-000 de la FERC approuvant la *norme de fiabilité* CIP-005-7.	
7	1er octobre 2022	Date d'entrée en vigueur.	

Annexe CIP-005-7-QC-1

Dispositions particulières applicables au Québec visant la norme CIP-005-7 – Cybersécurité – Périmètres de sécurité électronique

La présente annexe établit les dispositions particulières d'application au Québec de la norme qu'elle vise. Les dispositions de la norme visée et de l'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 a préséance.

A. Introduction

1. Titre : Aucune disposition particulière.

2. Numéro : Aucune disposition particulière.

3. Objet : Aucune disposition particulière.

4. Applicabilité :

4.1. Entités fonctionnelles

Aucune disposition particulière.

4.2. 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 :

- Toute installation de production qui répond aux deux conditions suivantes : (1) la puissance nominale de l'installation est de 300 MVA ou moins et (2) aucun groupe de l'installation ne peut être synchronisé avec un réseau voisin.
- Postes élévateurs des installations de production identifiées au point précédent.

5. Date d'entrée en vigueur :

5.1.	Adoption de la norme par la Régie de l'énergie :	11 février 2022
5.2.	Adoption de l'annexe par la Régie de l'énergie :	11 février 2022
5.3.	Date d'entrée en vigueur de la norme et de l'annexe au Québec :	1er octobre 2023

6. Contexte : Aucune disposition particulière.

B. Exigences et mesures

Aucune disposition particulière.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Au Québec, le terme *responsable des mesures pour assurer la conformité* désigne la Régie de l'énergie dans le rôle visant à surveiller la conformité avec la *norme de fiabilité* visée et à la présente annexe, et à assurer l'application de celles-ci.

1.2. Conservation des pièces justificatives

Aucune disposition particulière.

1.3. Programme de surveillance de la conformité et d'application des normes

La Régie de l'énergie établit les processus de surveillance qui servent à évaluer les données ou l'information afin de déterminer la conformité ou la non-conformité avec la *norme de fiabilité* visée et avec la présente annexe.

Niveaux de gravité de la non-conformité (VSL)

Aucune disposition particulière.

D. Différences régionales

Aucune disposition particulière.

E. Documents connexes

Aucune disposition particulière.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	11 février 2022	Nouvelle annexe en suivi de la décision D-2022-021.	Nouvelle