

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 1^{er} 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 de 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	<p><i>Systèmes électroniques BES</i> à impact élevé et leurs :</p> <ul style="list-style-type: none"> • PCA associés. <p><i>Systèmes électroniques BES</i> à impact moyen et leurs :</p> <ul style="list-style-type: none"> • PCA associés. 	Tous les <i>actifs électroniques</i> 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 <i>actifs électroniques</i> 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	<p><i>Systèmes électroniques BES à impact élevé à connectivité externe routable et leurs :</i></p> <ul style="list-style-type: none"> • PCA associés. <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et leurs :</i></p> <ul style="list-style-type: none"> • PCA associés. 	Toute <i>connectivité externe routable</i> doit s'effectuer par l'intermédiaire d'un <i>point d'accès électronique</i> (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	<p><i>Points d'accès électronique associés à des systèmes électroniques BES à impact élevé.</i></p> <p><i>Points d'accès électronique associés à des systèmes électroniques BES à impact moyen.</i></p>	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	<p><i>Systèmes électroniques BES à impact élevé à connectivité par lien commuté et leurs :</i></p> <ul style="list-style-type: none"> • PCA associés. <p><i>Systèmes électroniques BES à impact moyen à connectivité par lien commuté et leurs :</i></p> <ul style="list-style-type: none"> • PCA associés. 	Lorsque techniquement faisable, effectuer l'authentification lors de l'établissement de la <i>connectivité par lien commuté</i> avec les <i>actifs électroniques</i> 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	<p><i>Points d'accès électronique associés à des systèmes électroniques BES à impact élevé.</i></p> <p><i>Points d'accès électronique associés à des systèmes électroniques BES à impact moyen situés dans des centres de contrôle.</i></p>	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	<p><i>Systèmes électroniques BES</i> à impact élevé et leurs :</p> <ul style="list-style-type: none"> • PCA associés. <p><i>Systèmes électroniques BES</i> à impact moyen à <i>connectivité externe routable</i> et leurs :</p> <ul style="list-style-type: none"> • PCA associés. 	Utiliser un <i>système intermédiaire</i> de façon à ce que l' <i>actif électronique</i> à initiant l' <i>accès distant interactif</i> n'ait pas directement accès à l' <i>actif électronique</i> visé.	Exemples non limitatifs de pièces justificatives : schémas de réseau ou documents sur l'architecture.
2.2	<p><i>Systèmes électroniques BES</i> à impact élevé et leurs :</p> <ul style="list-style-type: none"> • PCA associés. <p><i>Systèmes électroniques BES</i> à impact moyen à <i>connectivité externe routable</i> et leurs :</p> <ul style="list-style-type: none"> • PCA associés. 	Pour toutes les sessions d' <i>accès distant interactif</i> , utiliser un cryptage se terminant à un <i>système intermédiaire</i> .	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	<p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ul style="list-style-type: none"> • PCA associés. <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et leurs :</i></p> <ul style="list-style-type: none"> • PCA associés. 	Exiger l'authentification multifactorielle pour toutes les sessions d' <i>accès distant interactif</i> .	<p>Exemple non limitatif de pièce justificative : documents sur l'architecture décrivant les facteurs d'authentification utilisés.</p> <p>Exemples non limitatifs de facteurs d'authentification :</p> <ul style="list-style-type: none"> • 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

2. Tableau des éléments de conformité

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-005-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	Planification de l'exploitation et Exploitation du jour même	Moyen			L'entité responsable n'avait pas un moyen de détection des communications entrantes et sortantes malveillantes. (1.5)	<p>L'entité responsable n'avait pas documenté un ou plusieurs processus pour le <i>Tableau E1 (CIP-005-5) – Périmètre de sécurité électronique. (R1)</i></p> <p>OU</p> <p>L'entité responsable n'avait pas tous les <i>actifs électroniques</i> applicables qui sont reliés à un réseau au moyen d'un protocole routable à l'intérieur d'un périmètre de sécurité électronique (ESP) défini. (1.1)</p> <p>OU</p> <p>La <i>connectivité externe routable</i> à travers l'ESP n'était pas effectuée par l'intermédiaire d'un EAP identifié. (1.2)</p> <p>OU</p>

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-005-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						<p>L'entité responsable n'a pas exigé d'autorisations pour les accès entrants et sortants et refusé tout autre accès par défaut. (1.3)</p> <p>OU</p> <p>L'entité responsable n'a pas effectué l'authentification lors de l'établissement de la connectivité par lien commuté avec les <i>actifs électroniques</i> applicables, lorsque techniquement faisable. (1.4)</p>
E2	Planification de l'exploitation et Exploitation du jour même	Moyen	L'entité responsable n'a pas de processus documentés pour un ou plusieurs des éléments applicables des sections d'exigence 2.1 à 2.3.	L'entité responsable n'a pas mis en œuvre de processus pour un des éléments applicables des sections d'exigence 2.1 à 2.3.	L'entité responsable n'a pas mis en œuvre de processus pour deux des éléments applicables des sections d'exigence 2.1 à 2.3.	L'entité responsable n'a pas mis en œuvre de processus pour trois des éléments applicables des sections d'exigence 2.1 à 2.3.

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Principes directeurs et fondements techniques

Section 4 – Portée de l'applicabilité des normes CIP sur la cybersécurité

La section « 4. Applicabilité » des normes présente de l'information importante pour aider les entités responsables à déterminer la portée d'application des exigences CIP sur la cybersécurité.

La section « 4.1. Entités fonctionnelles » est la liste des entités fonctionnelles de la NERC auxquelles s'applique la norme. Si l'entité est enregistrée au titre d'une ou de plusieurs des entités fonctionnelles énumérées à la section 4.1, alors les normes CIP sur la cybersécurité de la NERC s'appliquent. Il est à noter qu'il y a une restriction à la section 4.1 qui limite l'applicabilité dans le cas des distributeurs à ceux qui détiennent certains types de systèmes et d'équipements énumérés à la section 4.2.

La section « 4.2. Installations » définit la portée des *installations*, systèmes et équipements détenus par l'entité responsable qualifiée à la section 4.1, qui est visée par les exigences de la norme. Tel qu'indiqué à la section exemption 4.2.3.5, cette norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou à impact moyen selon la catégorisation de la CIP-002-5. Outre l'ensemble des *installations* du BES, des *centres de contrôle* et des autres systèmes et équipements, la liste comprend l'ensemble des systèmes et équipements détenus par les distributeurs. Bien que le terme « *installations* » du glossaire de la NERC comprenne déjà la caractéristique BES, l'utilisation additionnelle du terme « BES » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité. Cela établit quels sont les *installations*, systèmes et équipements visés par les normes.

Exigence E1

L'exigence E1 de la norme CIP-005-5 exige l'isolation des *systèmes électroniques BES* des autres systèmes de degrés de confiance différents en demandant des *points d'accès électroniques* contrôlés entre les différentes zones de confiance. Les *périmètres de sécurité électronique* sont également utilisés comme première couche de défense pour certains *systèmes électroniques*

BES qui ne disposent pas intrinsèquement d'une protection électronique suffisante, notamment les dispositifs qui n'ont pas de fonction d'authentification.

Tous les systèmes électroniques *BES* applicables qui sont reliés à un réseau au moyen d'un protocole routable doivent avoir un *périmètre de sécurité électronique* (ESP) défini. Même les réseaux autonomes qui n'ont pas de connectivité externe avec d'autres réseaux doivent avoir un ESP défini. L'ESP établit une zone de protection autour d'un *système électronique BES* en plus de définir clairement, du point de vue des entités, quels sont les systèmes ou les *actifs électroniques* visés et quelles sont les exigences auxquelles elles doivent se conformer. L'ESP permet de définir :

- l'étendue des « *actifs électroniques protégés* associés » qui doivent également répondre à certaines exigences CIP, et
- la frontière à l'intérieur de laquelle tous les *actifs électroniques* doivent répondre aux exigences qui s'appliquent au *système électronique BES* ayant l'impact le plus élevé à l'intérieur de la zone (seuil de protection).

Les normes sur la cybersécurité (CIP) n'exigent pas une segmentation par réseaux des *systèmes électroniques BES* en fonction de leur catégorie d'impact. Un ESP peut comprendre des systèmes ayant des degrés d'impact différents. Cependant, tous les *actifs électroniques* et les *systèmes électroniques BES* qui se trouvent à l'intérieur de l'ESP doivent tous avoir un niveau de protection équivalent à celui du *système électronique BES* inclus dans l'ESP dont l'impact est le plus élevé (ce que l'on appelle le « seuil de protection ») lorsque l'expression « *actifs électroniques protégés* » est utilisée. Dans les normes sur la cybersécurité (CIP), on obtient le « seuil de protection » en définissant tous les *actifs électroniques* situés à l'intérieur d'un ESP comme « *actifs électroniques protégés* » ayant le même impact que le système à l'intérieur de l'ESP dont l'impact est le plus élevé, et ce, peu importe qu'ils aient un impact moindre.

Par exemple, si un ESP comprend à la fois un *système électronique BES* à impact élevé et un *système électronique BES* à impact faible, chaque *actif électronique* du *système électronique BES* à impact faible est considéré comme un « *actif électronique protégé* associé » du *système électronique BES* à impact élevé et il doit donc se conformer à toutes les exigences afférentes figurant dans les tableaux.

Lorsqu'un *actif électronique* est accessible par connectivité routable à travers l'ESP, les données qui entrent dans l'ESP ou en sortent doivent être contrôlées par un *point d'accès électronique* (EAP). Les entités responsables doivent savoir quelles données ont besoin de traverser l'EAP, et en justifier les raisons dans un document, afin de s'assurer que l'EAP limite les échanges aux communications nécessaires uniquement. Ces communications comprennent, sans s'y limiter, celles qui sont requises dans le cadre de l'exploitation normale, des interventions d'urgence, du soutien, de la maintenance et du dépannage.

L'EAP doit contrôler les échanges tant entrants que sortants. La norme exige dorénavant le contrôle des échanges sortants puisqu'elles constituent un premier indicateur de compromission et un mécanisme de défense de premier niveau contre les attaques de vulnérabilité du jour zéro. Si des *actifs électroniques* à l'intérieur de l'ESP sont compromis et tentent de communiquer avec des hôtes inconnus à l'extérieur de l'ESP (il s'agit habituellement

d'hôtes de « commande et contrôle », sur Internet, ou d'hôtes de rebond compromis au sein d'autres réseaux de l'entité responsable et qui agissent comme intermédiaires), l'EAP doit agir comme mécanisme de défense de premier niveau pour rompre la communication. Cela n'empêche pas l'entité responsable de contrôler les échanges sortants au niveau de granularité qu'elle considère comme approprié et d'autoriser de grandes plages d'adresses internes. L'intention du SDT est de faire en sorte que l'entité responsable connaisse les autres *actifs électroniques* ou plages d'adresses avec lesquels le *système électronique BES* a besoin de communiquer et qu'elle limite les communications à ces actifs et adresses connus. Par exemple, la plupart des *systèmes électroniques BES* au sein du réseau de l'entité responsable ne devraient pas pouvoir communiquer via un EAP avec n'importe quelle adresse dans le monde ; à tout le moins, ils devraient probablement être limités à l'espace d'adressage de l'entité responsable et, idéalement, à des plages de sous-réseaux distincts ou à des hôtes particuliers à l'intérieur de l'espace d'adressage de l'entité responsable. L'objectif du SDT n'est pas que l'entité responsable documente les activités internes des pare-feu dynamiques, où les connexions amorcées dans un sens sont autorisées dans l'autre sens. L'objectif est plutôt que l'entité responsable connaisse et documente les systèmes ou groupes de systèmes qui peuvent communiquer entre eux de part et d'autre de l'EAP afin que les connexions indésirables puissent être détectées et bloquées.

Cette exigence vise uniquement les communications auxquelles peuvent s'appliquer de manière universelle des listes d'accès ou des exigences de type « refus par défaut », soit celles qui utilisent aujourd'hui des protocoles routables. Elle ne s'applique pas aux connexions directes série non routables, car il n'existe aucun périmètre ou pare-feu de sécurité qui devrait être rendu obligatoire pour l'ensemble des entités et des communications série. Il est impossible de mettre en place un pare-feu ou un périmètre de sécurité pour un câble RS-232 reliant deux *actifs électroniques*. Sans mécanisme de sécurité faisant appel à un périmètre et pouvant être appliquée à pratiquement tous les cas, une telle exigence aurait pour effet d'engendrer de nombreuses exceptions liées à la faisabilité technique (TFE) plutôt que d'améliorer la sécurité.

Dans le cas de la connectivité par lien commuté, l'intention de l'équipe de rédaction de normes est de prévenir les situations où il serait possible d'établir une liaison directe avec un *actif électronique BES* au moyen d'un numéro de téléphone uniquement. Si un modem est configuré de manière à simplement répondre au téléphone et à établir la liaison avec l'*actif électronique BES* demandé sans authentifier le demandeur, il rend vulnérable le *système électronique BES*. En vertu de cette exigence, le modem doit authentifier le demandeur avant d'établir la communication avec le *système électronique BES*. Il peut s'agir par exemple de modems à fonction de rappel, de modems activés ou mis sous tension à distance et de modems mis sous tension au besoin par le personnel sur place et mis hors tension après utilisation en vertu d'une politique bien établie. L'exigence E2 s'applique également dans le cas d'une connectivité par lien commuté utilisée pour un *accès distant interactif*.

La norme ajoute une exigence pour les *centres de contrôle* concernant la détection des communications malveillantes. Ceci est en réponse à l'ordonnance 706 de la FERC, alinéas 496-503, stipulant qu'il faut prévoir deux dispositifs de sécurité distincts pour les ESP afin de préserver le périmètre de protection des *systèmes électroniques BES* advenant une défaillance

ou un défaut de configuration de l'un ou l'autre de ces dispositifs. L'ordonnance indique clairement qu'il ne s'agit pas simplement d'assurer une redondance des pare-feu ; le SDT a donc décidé d'ajouter l'exigence liée à la mise en œuvre de moyens de détection des communications malveillantes pour les ESP. Les technologies qui répondent à cette exigence comprennent notamment les systèmes de détection ou de prévention des intrusions (IDS/IPS) et d'autres formes d'inspection en profondeur des paquets. Ces technologies vont plus loin que les ensembles de règles associant ports, sources et destinations, et constituent par le fait même un autre mécanisme de sécurité distinct mis en œuvre par l'ESP.

Exigence E2

Voir le document de référence sur l'accès distant protégé (voir alerte d'accès distant).

Raisonnement

Pendant l'élaboration de cette norme, les références aux versions antérieures des normes CIP et le raisonnement derrière les exigences et leurs parties étaient intégrés à même la norme. Sur approbation du BOT, cette information a été déplacée à la présente section.

Raisonnement pour E1 :

Le *périmètre de sécurité électronique* (ESP) sert à contrôler les échanges de données à la frontière électronique externe du *système électronique BES*. Il constitue une première couche de défense contre les attaques provenant du réseau puisqu'il limite la reconnaissance des cibles, restreint et interdit les échanges en fonction d'un ensemble de règles définies et contribue à circonscrire les effets d'attaques réussies.

Sommaire des modifications apportées : L'exigence 1 de la norme CIP-005 insiste davantage sur les *points d'accès électroniques* distincts que sur le « périmètre » logique.

L'exigence 1.2 de la norme CIP-005 (versions 1 à 4) a été supprimée de la version 5. Cette exigence avait un caractère définitoire et servait à inclure les modems commutés utilisant des protocoles non routables dans le domaine d'application de la norme CIP 005. L'exclusion liée aux protocoles non routables n'existant plus en tant que critère spécifique d'applicabilité (norme CIP 002) dans la version 5, cette exigence est dorénavant inutile.

Les exigences 1.1 et 1.3 de la norme CIP-005 (versions 1 à 4) avaient également un caractère définitoire et ont été supprimées de la version 5 ; cependant, les concepts sous-jacents à ces deux exigences ont été intégrés aux définitions des termes *périmètre de sécurité électronique* (ESP) et *point d'accès électronique* (EAP).

Référence à une version précédente : (Partie 1.1) CIP-005-4, E1

Justification des modifications : (Partie 1.1)

Affirmation claire du fait que les *actifs électroniques BES* reliés au moyen d'un protocole routable doivent se situer à l'intérieur d'un *périmètre de sécurité électronique*.

Référence à une version précédente : (Partie 1.2) CIP-005-4, E1

Justification des modifications : (Partie 1.2)

Utilisation des termes définis *point d'accès électronique* et *système électronique BES*.

Référence à une version précédente : (Partie 1.3) CIP-005-4, E2.1

Justification des modifications : (Partie 1.3)

Utilisation du terme défini *point d'accès électronique* et insistance sur le fait que l'entité doit connaître les accès entrants et sortants via l'EAP qu'elle autorise et que les raisons pour lesquelles elle autorise ces accès sont justifiées.

Référence à une version précédente : (Partie 1.4) CIP-005-4, E2.3

Justification des modifications apportées : (Partie 1.4)

Explication plus claire du fait que la connectivité par lien commuté doit assurer l'authentification afin de rendre impossible l'accès direct au *système électronique BES* à l'aide d'un simple numéro de téléphone.

Référence à une version précédente : (Partie 1.5) CIP-005-4, E1

Justification des modifications : (Partie 1.5)

Conformité à l'Ordonnance 706 de la FERC, alinéas 496-503, en vertu de laquelle il faut prévoir deux dispositifs de sécurité distincts pour les ESP afin de préserver le périmètre de protection des *actifs électroniques* advenant une défaillance ou un défaut de configuration de l'un ou l'autre de ces dispositifs. L'Ordonnance indique clairement qu'il ne s'agit pas simplement d'assurer une redondance des pare-feu ; le SDT a donc décidé d'ajouter l'exigence liée à la mise en œuvre de moyens de détection des communications malveillantes pour les ESP.

Raisonnement pour E2 :

Les entités inscrites utilisent l'*accès distant interactif* pour accéder aux *actifs électroniques* en vue d'assurer le soutien et la maintenance des réseaux de systèmes de commande. La détection et le signalement des vulnérabilités dans les technologies et les méthodes d'accès distant, que l'on croyait sécurisées et qui étaient utilisées par des entités du secteur électrique, nécessitent que l'on apporte des modifications aux normes de contrôle de la sécurité au sein de l'industrie. Actuellement, aucune exigence n'oblige les gestionnaires d'un accès distant sécurisé à des *actifs électroniques* à se doter des mesures de protection mentionnées dans les normes CIP de la NERC. Des dispositifs de protection inadéquats peuvent permettre un accès non autorisé au réseau de l'organisation, ce qui pourrait entraîner des conséquences graves. Le document **Guidance for Secure Interactive Remote Access**, publié par la NERC en juillet 2011, renferme davantage de renseignements à cet égard.

Les procédures de contrôle de l'accès distant doivent prévoir des mesures de protection adéquates, notamment l'utilisation de techniques d'identification, d'authentification et de cryptage efficaces. L'accès distant au réseau et aux ressources de l'organisation ne doit être permis que si les conditions suivantes sont remplies : les utilisateurs autorisés sont authentifiés, les données sont cryptées dans tout le réseau et les privilèges sont restreints.

Le *système intermédiaire* sert de mandataire pour l'utilisateur distant. Au lieu de faire en sorte que tous les protocoles dont l'utilisateur pourrait avoir besoin pour accéder aux *actifs électroniques* à l'intérieur du *périmètre de sécurité électronique* puissent traverser ce *périmètre de sécurité électronique* pour atteindre l'ordinateur distant, on ne laisse passer que le protocole nécessaire pour commander à distance l'hôte de rebond. Ainsi, on peut établir des règles de pare-feu beaucoup plus contraignantes que s'il fallait autoriser l'ordinateur distant à se connecter directement aux *actifs électroniques* se trouvant dans le *périmètre de sécurité électronique*. Un *système intermédiaire* permet aussi de protéger les *actifs électroniques* des vulnérabilités de l'ordinateur distant.

L'application d'une méthode d'authentification multifactorielle offre une couche de protection supplémentaire. En effet, les mots de passe peuvent être devinés, volés, piratés, trouvés ou divulgués. Pour découvrir un mot de passe, on peut lancer des attaques automatisées, notamment des attaques par force brute – essais de tous les mots de passe possible – ou des attaques par dictionnaire – essais de mots ou combinaisons de mots. Toutefois, un mot de passe ou un NIP n'a aucune valeur si l'on n'acquiert pas en même temps les autres facteurs requis pour l'authentification, comme un jeton ou une empreinte digitale.

Le cryptage protège les données transmises entre l'ordinateur distant et le *système intermédiaire*. Il faut crypter les données pour pouvoir les transférer de manière sécuritaire, notamment lorsqu'il existe un risque d'interception non autorisée sur les voies de communication utilisées, particulièrement sur Internet.

Sommaire des modifications apportées : Il s'agit d'une nouvelle exigence pour appuyer la poursuite des efforts de l'équipe d'intervention rapide dans le cadre du projet 2010-15 (révision accélérée de la norme CIP-005-3).

Référence à une version précédente : (Partie 2.1) Nouveau

Justification des modifications apportées : (Partie 2.1)

Nouvelle exigence visant à poursuivre les efforts de l'équipe d'intervention rapide affectée au projet 2010-15 (révision accélérée de la norme CIP-005-3).

Référence à une version précédente : (Partie 2.2) CIP-007-5, E3.1

Justification des modifications apportées : (Partie 2.2)

Nouvelle exigence visant à poursuivre les efforts de l'équipe d'intervention rapide affectée au projet 2010-15 (révision accélérée de la norme CIP-005-3). Cette exigence vise à protéger la confidentialité et l'intégrité de chaque session d'*accès distant interactif*.

Référence à une version précédente : (Partie 2.3) CIP-007-5, E3.2

Justification des modifications apportées : (Partie 2.3)

Nouvelle exigence visant à poursuivre les efforts de l'équipe d'intervention rapide affectée au projet 2010-15 (révision accélérée de la norme CIP-005-3). Les méthodes d'authentification multifactorielle sont décrites dans la Homeland Security Presidential Directive 12 (HSPD-12) du 12 août 2007.

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 de la surveillance de l'application des normes ».	
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	Émission d'une ordonnance de la FERC approuvant CIP-005-5 (L'ordonnance entre en vigueur le 3 février 2014)	

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.

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