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 systèmes, *installations* 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 de l'entité 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.

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 de l'entité 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 de l'entité 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 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 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 systèmes, *installations* 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 de l'entité 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.

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 de l'entité 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 de l'entité 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 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-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 des mesures pour assurer la conformité

L'entité régionale joue le rôle de responsable des mesures pour assurer la conformité (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 de non-conformité
- 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-006-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	**Planification à long terme** **Exploitation du jour même**	**Moyen**	L'entité responsable a un processus pour consigner l'accès physique autorisé dans tout *périmètre de sécurité physique* avec l'information suffisante permettant d'identifier la personne, ainsi que la date et l'heure de l'accès, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (1.8) OU L'entité responsable a un processus pour consigner l'accès physique autorisé dans tout *périmètre de sécurité physique* avec l'information suffisante permettant d'identifier la personne, ainsi que la date et l'heure de l'accès, mais n'a pas	L'entité responsable a un processus pour alerter en cas d'accès physique non autorisé aux *systèmes de contrôle des accès physiques* et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (1.7) OU L'entité responsable a un processus pour alerter en cas d'accès physique non autorisé aux *systèmes de contrôle des accès physiques*, mais n'a pas identifié, évalué ou corrigé les lacunes. (1.7) OU L'entité responsable a un processus pour communiquer les	L'entité responsable a un processus pour alerter en cas de détection d'un accès non autorisé au point d'accès physique d'un *périmètre de sécurité physique,* et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (1.5) OU L'entité responsable a un processus pour alerter en cas de détection d'un accès non autorisé au point d'accès physique d'un *périmètre de sécurité physique*, mais n'a pas identifié, évalué ou corrigé les lacunes. (1.5) OU L'entité responsable a	L'entité responsable n'a pas documenté ou mis en œuvre de mesures opérationnelles ou administratives permettant de restreindre l'accès physique. (1.1) OU L'entité responsable a documenté et mis en œuvre des mesures opérationnelles ou administratives permettant de restreindre l'accès physique, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (1.1) OU L'entité responsable a documenté et mis en œuvre des mesures

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			identifié, évalué ou corrigé les lacunes. (1.8) OU L'entité responsable a un processus pour conserver les registres d'accès physique pendant 90 jours civils et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (1.9) OU L'entité responsable a un processus pour conserver les registres d'accès physique pendant 90 jours civils, mais n'a pas identifié, évalué ou corrigé les lacunes. (1.9)	alertes au personnel désigné dans les 15 minutes, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (1.7) OU L'entité responsable a un processus pour communiquer les alertes au personnel désigné dans les 15 minutes, mais n'a pas identifié, évalué ou corrigé les lacunes. (1.7)	un processus pour communiquer les alertes au personnel désigné dans les 15 minutes, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (1.5) OU L'entité responsable a un processus pour communiquer les alertes au personnel désigné dans les 15 minutes, mais n'a pas identifié, évalué ou corrigé les lacunes. (1.5) OU L'entité responsable a un processus pour surveiller les accès physiques non autorisés à un *système de contrôle des accès physiques*, et a	opérationnelles ou administratives permettant de restreindre l'accès physique, mais n'a pas identifié, évalué ou corrigé les lacunes. (1.1) OU L'entité responsable a documenté et mis en œuvre des mécanismes de contrôle des accès physiques, mais au moins un mécanisme de contrôle n'existe pas pour restreindre l'accès aux systèmes applicables. (1.2) L'entité responsable a documenté et mis en œuvre des mécanismes de contrôle des accès physiques, restreint l'accès aux systèmes applicables en utilisant au moins un

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (1.6) OU L'entité responsable a un processus pour surveiller les accès physiques non autorisés à un *système de contrôle des accès physiques*, mais n'a pas identifié, évalué ou corrigé les lacunes. (1.6)	mécanisme de contrôle, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (1.2) OU L'entité responsable a documenté et mis en œuvre des mécanismes de contrôle des accès physiques, restreint l'accès aux systèmes applicables en utilisant au moins un mécanisme de contrôle, mais n'a pas identifié, évalué ou corrigé les lacunes. (1.2) OU L'entité responsable a documenté et mis en œuvre des mécanismes de contrôle des accès physiques, mais au moins deux mécanismes de

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						contrôle différents n'existent pas pour restreindre l'accès aux systèmes applicables. (1.3) OU L'entité responsable a documenté et mis en œuvre des mesures opérationnelles ou administratives, restreint l'accès aux systèmes applicables en utilisant au moins deux mécanismes de contrôle différents, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (1.3) OU L'entité responsable a documenté et mis en œuvre des mesures opérationnelles ou administratives, restreint l'accès aux

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						systèmes applicables en utilisant au moins deux mécanismes de contrôle différents, mais n'a pas identifié, évalué ou corrigé les lacunes. (1.3) OU L'entité responsable n'a pas de processus pour surveiller les accès non autorisés au point d'accès physique d'un *périmètre de sécurité physique*. (1.4) OU L'entité responsable a un processus pour surveiller les accès non autorisés au point d'accès physique d'un *périmètre de sécurité physique*, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (1.4)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						OU L'entité responsable a un processus pour surveiller les accès non autorisés au point d'accès physique d'un *périmètre de sécurité physique*, mais n'a pas identifié, évalué ou corrigé les lacunes. (1.4) OU L'entité responsable n'a pas de processus pour alerter en cas de détection d'un accès non autorisé au point d'accès physique d'un *périmètre de sécurité physique* ou pour communiquer ces alertes au personnel désigné dans les 15 minutes. (1.5) OU L'entité responsable

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						n'a pas de processus pour surveiller chaque *système de contrôle des accès physiques* pour les accès physiques non autorisés à un *système de contrôle des accès physiques*. (1.6) OU L'entité responsable n'a pas de processus pour alerter en cas d'accès physique non autorisé aux *systèmes de contrôle des accès physiques* ou pour communiquer ces alertes au personnel désigné dans les 15 minutes. (1.7) OU L'entité responsable n'a pas de processus pour consigner l'accès physique autorisé dans chaque *périmètre de*

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						sécurité physique avec l'information suffisante permettant d'identifier la personne, ainsi que la date et l'heure de l'accès. (1.8) OU L'entité responsable n'a pas de processus pour conserver les registres d'accès physique pendant 90 jours civils. (1.9)
E2	**Exploitation du jour même**	**Moyen**	Sans objet	L'entité responsable a inclus un programme de contrôle des visiteurs qui exige la consignation de la date et l'heure de chaque première entrée et de chaque dernière sortie du visiteur, le nom du visiteur et le nom de son répondant, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes.	L'entité responsable a inclus un programme de contrôle des visiteurs qui exige un accompagnement continu des visiteurs à l'intérieur de tout *périmètre de sécurité physique,* et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (2.1) OU	L'entité responsable n'a pas inclus ou mis en œuvre un programme de contrôle des visiteurs qui exige un accompagnement continu des visiteurs à l'intérieur de tout *périmètre de sécurité physique.* (2.1) OU L'entité responsable n'a pas inclus ou mis en

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				(2.2) OU L'entité responsable a inclus un programme de contrôle des visiteurs qui exige la consignation de la date et l'heure de la première entrée et de la dernière sortie du visiteur, le nom du visiteur et le nom de son répondant, mais n'a pas identifié, évalué ou corrigé les lacunes. (2.2) OU L'entité responsable a inclus un programme de contrôle des visiteurs pour conserver les registres des visiteurs durant au moins 90 jours civils, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes.	L'entité responsable a inclus un programme de contrôle des visiteurs qui exige un accompagnement continu des visiteurs à l'intérieur de tout *périmètre de sécurité physique*, mais n'a pas identifié, évalué ou corrigé les lacunes. (2.1)	œuvre un programme de contrôle des visiteurs qui exige la consignation de la date et l'heure de la première entrée et de la dernière sortie du visiteur, le nom du visiteur et le nom de son répondant. (2.2) OU L'entité responsable n'a pas inclus ou mis en œuvre un programme de contrôle des visiteurs pour conserver les registres des visiteurs durant au moins 90 jours. (2.3)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				(2.3) OU L'entité responsable a inclus un programme de contrôle des visiteurs pour conserver les registres des visiteurs durant au moins 90 jours civils, mais n'a pas identifié, évalué ou corrigé les lacunes. (2.3)		
E3	**Planification à long terme**	**Moyen**	L'entité responsable a documenté et mis en œuvre un programme de maintenance et d'essai des *systèmes de contrôle des accès physiques* et des composants matériels ou dispositifs installés localement au *périmètre de sécurité physique,* mais n'a pas complété l'essai exigé à l'intérieur de 24 mois civils, mais a complété	L'entité responsable a documenté et mis en œuvre un programme de maintenance et d'essai des *systèmes de contrôle des accès physiques* et des composants matériels ou dispositifs installés localement au *périmètre de sécurité physique,* mais n'a pas complété l'essai exigé à l'intérieur de 25 mois civils, mais a complété	L'entité responsable a documenté et mis en œuvre un programme de maintenance et d'essai des *systèmes de contrôle des accès physiques* et des composants matériels ou dispositifs installés localement au *périmètre de sécurité physique,* mais n'a pas complété l'essai exigé à l'intérieur de 26 mois civils, mais a complété	L'entité responsable n'a pas documenté et mis en œuvre un programme de maintenance et d'essai des *systèmes de contrôle des accès physiques* et des composants matériels ou dispositifs installés localement au *périmètre de sécurité physique.* (3.1) OU

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			l'essai exigé à l'intérieur de 25 mois civils. (3.1)	l'essai exigé à l'intérieur de 26 mois civils. (3.1)	l'essai exigé à l'intérieur de 27 mois civils. (3.1)	L'entité responsable a documenté et mis en œuvre un programme de maintenance et d'essai des *systèmes de contrôle des accès physiques* et des composants matériels ou dispositifs installés localement au *périmètre de sécurité physique,* mais n'a pas complété l'essai exigé à l'intérieur de 27 mois civils. (3.1)

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.

Généralités

Même si l'accent n'est plus mis sur l'établissement et la gestion d'un périmètre physique complètement étanche (« à six parois »), il est attendu que dans de nombreux cas ceci demeurera le mécanisme principal pour le contrôle, l'alerte et la journalisation des accès aux *systèmes électroniques BES*. Ensemble, ces mécanismes constitueront de fait le plan de sécurité physique permettant de gérer les accès physiques aux *systèmes électroniques BES*.

Exigence E1

Les méthodes de contrôle des accès physiques comprennent :

- Carte d'accès : Un dispositif d'accès électronique pour lequel les droits d'accès du détenteur de la carte sont prédéfinis dans une base de données informatique. Les droits d'accès peuvent différer d'un périmètre à un autre.
- Systèmes de verrouillage : Ceux-ci incluent notamment les serrures à « clé à copie restreinte », les serrures magnétiques qui peuvent être déverrouillées à distance et les sas de sécurité.

- Personnel de sécurité : Personne responsable de la surveillance des accès physiques, qui peut se trouver sur place ou dans un poste de surveillance à distance.
- Autres dispositifs d'authentification : Lecteur biométrique, clavier numérique, jeton ou tout autre dispositif équivalent permettant de contrôler l'accès physique au *périmètre de sécurité physique*.

Les méthodes de surveillance des accès physiques comprennent :

- Système d'alarme : Système qui émet une alarme pour indiquer qu'un mouvement a été détecté à l'intérieur d'un périmètre ou qu'une porte, une barrière ou une fenêtre a été ouverte sans autorisation. L'alarme doit être signalée au personnel d'intervention désigné dans un délai d'au plus 15 minutes.
- Postes de garde : Surveillance des points d'accès physique assurée par le personnel chargé de contrôler les accès physiques.

Les méthodes de journalisation des accès comprennent :

- Registre informatisé : Journal électronique produit par le système de contrôle d'accès et d'alerte adopté par l'entité responsable.
- Enregistrement vidéo : Saisie électronique d'images vidéo de qualité suffisante pour permettre l'identification d'une personne.
- Registre manuel : Journal, feuille de signature ou autre relevé des accès physiques tenu par un gardien de sécurité ou une autre personne autorisée à contrôler et à surveiller les accès physiques.

L'ordonnance 706 de la FERC, paragraphe 572, donne pour directive d'utiliser au moins deux mécanismes différents et complémentaires pour le contrôle des accès physiques afin d'assurer une défense en profondeur. Elle n'exige pas l'utilisation d'un minimum de deux *périmètres de sécurité physique* et elle n'exclut pas l'utilisation de périmètres en couches. En présence d'un périmètre de sécurité physique unique, il serait acceptable d'utiliser au point d'accès une authentification à deux facteurs. Dans ce cas, les mécanismes de contrôle pourraient comprendre par exemple une carte d'accès combinée à un code NIP (élément détenu par l'utilisateur et élément connu de l'utilisateur), une carte d'accès combinée à un lecteur biométrique (élément détenu par l'utilisateur et élément qui le caractérise) ou encore une clé physique combinée à une serrure de porte et à une télécaméra de surveillance, où un gardien disposerait des renseignements nécessaires pour authentifier les personnes, en les observant ou en leur parlant, avant de leur accorder un accès (élément détenu par l'utilisateur et élément qui le caractérise). Il est possible de mettre en œuvre l'authentification à deux facteurs au moyen d'un seul *système de contrôle des accès physiques*, à condition d'utiliser plus d'une méthode d'authentification. En présence d'un périmètre de sécurité physique en couches, il serait acceptable de combiner une barrière verrouillée et un bâtiment de contrôle verrouillé, à condition que l'accès à ces deux points d'entrée ne puisse être autorisé à l'aide du même facteur d'authentification (comme une clé ou une carte d'accès).

Les entités peuvent choisir de situer certains PACS à l'intérieur d'un PSP pour contrôler les accès aux *systèmes électroniques BES* visés. Ces PACS n'ont pas à respecter les exigences 1.1, 1.7 et 1.8 en plus de celles qui s'appliquent déjà au PSP.

Exigence E2

Les données d'accès des visiteurs doivent être consignées une seule fois par visite et non chaque fois que celui-ci entre dans le *périmètre de sécurité physique* et qu'il en sort durant sa visite, et ce, afin de permettre au visiteur de sortir temporairement du périmètre au besoin (pour aller récupérer un objet à l'extérieur, par exemple) sans avoir à s'enregistrer chaque fois pour y entrer de nouveau.

Le SDT a également établi qu'il faudrait consigner le nom d'un répondant en mesure de fournir des renseignements supplémentaires sur une visite dans l'éventualité où l'on aurait besoin de réponses à certaines questions. Ce répondant peut être l'accompagnateur du visiteur, mais il n'est pas nécessaire de consigner le nom de toutes les personnes qui ont accompagné un visiteur.

Exigence E3

Cette exigence introduit les essais devant être effectués sur le matériel et les dispositifs installés localement pour assurer le contrôle des accès aux *périmètres de sécurité physique*, ainsi que l'émission d'alertes et la consignation de données les concernant. Il s'agit notamment des détecteurs de mouvement, des mécanismes de verrouillage électroniques et des lecteurs de carte d'accès, qui ne sont pas considérés comme faisant partie du *système de contrôle des accès physiques*, mais qui sont nécessaires à la protection des *systèmes électroniques BES*.

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 :

Chaque entité responsable doit s'assurer de restreindre et de gérer adéquatement les accès physiques à tous les *systèmes électroniques BES*. Les entités peuvent choisir de situer certains PACS à l'intérieur d'un PSP pour contrôler les accès aux *systèmes électroniques BES* visés. Ces PACS n'ont pas à respecter les exigences 1.1, 1.7 et 1.8 en plus de celles qui s'appliquent déjà au PSP.

Sommaire des modifications apportées : Le contenu de la norme CIP-006-5 a été rédigé de manière à constituer un programme de sécurité physique ; en ce sens, cette version de la norme diffère des précédentes, qui exigeaient uniquement des plans de sécurité physique et non, spécifiquement, un programme de sécurité physique.

Des détails ont été ajoutés pour prendre en compte les directives de l'ordonnance 706 de la FERC, paragraphe 572, qui prônent une approche de défense en profondeur pour la sécurité physique.

Des exemples ont été ajoutés pour prendre en compte les directives de l'ordonnance 706 de la FERC, paragraphe 575, qui prônent une approche de défense en profondeur pour la sécurité physique.

Référence à une version précédente : (Partie 1.1) CIP-006-4c, E2.1 visant les *systèmes de contrôle des accès physiques*. Nouvelle exigence visant les *systèmes électroniques BES* à impact moyen sans connectivité externe routable.

Justification des modifications : (Partie 1.1)

Prévoir à la base un programme de mesures de protection (y compris ce que l'entité compte faire pour la protection des *systèmes électroniques BES* à impact moyen sans *connectivité externe routable*, qui ne sont pas visés en 1.2, sans toutefois nécessiter une liste détaillée des personnes y ayant accès). Les *systèmes de contrôle des accès physiques* proprement dits ne nécessitent pas un niveau de protection équivalent à celui qui est exigé en 1.2 à 1.5.

Référence à une version précédente : (Partie 1.2) CIP-006-4c, E3 et E4

Justification des modifications : (Partie 1.2)

La présente exigence a été rendue plus générale pour permettre le recours à d'autres mesures de restriction des accès physiques. Les exemples de méthodes que peut prendre l'entité responsable pour restreindre l'accès aux *systèmes électroniques BES* ont été déplacés à la section Principes directeurs et fondements techniques.

Référence à une version précédente : (Partie 1.3) CIP-006-4c, E3 et E4

Justification des modifications : (Partie 1.3)

Les exemples de méthodes que peut prendre l'entité responsable pour restreindre l'accès aux *systèmes électroniques BES* ont été déplacés à la section Principes directeurs et fondements techniques. La présente exigence a été rendue plus générale pour permettre le recours à d'autres mesures de restriction des accès physiques.

Des exemples ont été ajoutés pour prendre en compte les directives de l'ordonnance 706 de la FERC, paragraphe 572, qui prônent une approche de défense en profondeur pour la sécurité physique.

Des exemples de mesures de défense en profondeur ont été ajoutés, notamment l'authentification multifactorielle et les *périmètres de sécurité physique* en couches, pour prendre en compte les directives de l'ordonnance 706 de la FERC, paragraphe 575.

Référence à une version précédente : (Partie 1.4) CIP-006-4c, E5

Justification des modifications : (Partie 1.4)

Les exemples de méthodes de surveillance ont été déplacés à la section Principes directeurs et fondements techniques.

Référence à une version précédente : (Partie 1.5) CIP-006-4c, E5

Justification des modifications : (Partie 1.5)

Les exemples de méthodes de surveillance ont été déplacés à la section Principes directeurs et fondements techniques.

Référence à une version précédente : (Partie 1.6) CIP-006-4c, E5

Justification des modifications : (Partie 1.6)

La présente exigence tient compte de l'exigence 5 de la norme précédente, CIP-006-4c, concernant les *systèmes de contrôle des accès physiques*.

Référence à une version précédente : (Partie 1.7) CIP-006-4c, E5

Justification des modifications : (Partie 1.7)

La présente exigence tient compte de l'exigence 5 de la norme précédente, CIP-006-4c, concernant les *systèmes de contrôle des accès physiques*.

Référence à une version précédente : (Partie 1.8) CIP-006-4c, E6

Justification des modifications : (Partie 1.8)

L'exigence 6 de la norme précédente, CIP-006-4c, portait plus précisément sur la consignation des accès aux points d'accès visés. La présente exigence encadre de façon plus générale la consignation des accès physiques autorisés au *périmètre de sécurité physique*.

Les exemples de méthodes de consignation ont été déplacés à la section Principes directeurs et fondements techniques.

Référence à une version précédente : (Partie 1.9) CIP-006-4c, E7
Justification des modifications : (Partie 1.9)

Aucune modification.

Raisonnement pour E2 :

Contrôler quand le personnel n'ayant pas un accès physique autorisé sans accompagnement peut se trouver à l'intérieur d'un *périmètre de sécurité physique* protégeant des *systèmes électroniques BES*, ou des *systèmes de contrôle ou de surveillance des accès électroniques*, selon le tableau E2.

Sommaire des modifications apportées : Restructuration sous forme de tableau. Ajout effectué initialement dans la version 3 en réponse à l'ordonnance de la FERC du 30 septembre 2009.

Référence à une version précédente : (Partie 2.1) CIP-006-4c, E1.6.2

Justification des modifications : (Partie 2.1)

Ajout d'une mention à l'effet que cette mesure n'est pas obligatoire dans des *circonstances CIP exceptionnelles*.

Référence à une version précédente : (Partie 2.2) CIP-006-4c, E1.6.1
Justification des modifications : (Partie 2.2)

Ajout d'une mention à l'effet que cette mesure n'est pas obligatoire dans des *circonstances CIP exceptionnelles* ; prise en compte de la possibilité qu'une même personne puisse entrer et sortir plusieurs fois au cours d'une journée (consignation de la première entrée et de la dernière sortie) ; consignation du nom du répondant pour le visiteur. Il n'est pas obligatoire de consigner le nom de la personne qui accompagne le visiteur ni les changements d'accompagnateur.

Référence à une version précédente : (Partie 2.3) CIP-006-4c, E7

Justification des modifications : (Partie 2.3)

Aucune modification n'a été apportée.

Raisonnement pour E3 :

Faire en sorte que tous les dispositifs et *systèmes de contrôle des accès physiques* continuent de fonctionner correctement.

Sommaire des modifications apportées : Restructuration sous forme de tableau.

Ajout de détails pour prendre en compte les directives de l'ordonnance 706 de la FERC, paragraphe 581, exigeant que les essais soient effectués plus d'une fois tous les trois ans.

Référence à une version précédente : (Partie 3.1) CIP-006-4c, E8.1 et E8.2

Justification des modifications : (Partie 3.1)

Ajout de détails pour prendre en compte les directives de l'ordonnance 706 de la FERC, paragraphe 581, exigeant que les essais soient effectués plus d'une fois tous les trois ans. Le SDT a convenu que les essais auraient lieu tous les deux ans, car elle considérait que des essais annuels seraient trop fréquents.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	16 janvier 2006	E3.2 — Remplacement de « Control Center » par « control center » dans la version anglaise.	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. À l'exigence 1.6, suppression de la phrase traitant de la mise hors service d'un composant ou d'un système en vue d'effectuer la vérification conformément à l'ordonnance de la FERC du 30 septembre 2009.	
3	16 décembre 2009	Approbation par le Conseil d'administration de la NERC.	
3	31 mars 2010	Approbation par la FERC.	
4	24 janvier 2011	Approbation par le Conseil d'administration de la NERC.	
5	26 novembre 2012	Adoption par le Conseil d'administration de la NERC.	Modifiée en coordination avec les autres normes CIP et révision du

Version	Date	Intervention	Suivi des modifications
			format selon le gabarit RBS.
5	22 novembre 2013	Émission d'une ordonnance de la FERC approuvant CIP-006-5.	
5	9 juillet 2014	Émission d'une lettre d'ordonnance de la FERC approuvant les révisions des VRF et des VSL de certaines normes CIP.	L'exigence E3 de la CIP-006-5 modifiée de faible à moyen.

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 :

- 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 au Québec :

5.1. Adoption de la norme par la Régie de l'énergie : 29 juillet 2016

5.2. Adoption de l'annexe par la Régie de l'énergie : 29 juillet 2016

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

Pour les entités qui possèdent des actifs classés critiques aux fins des normes CIP (version 1) :

- 1er janvier 2017 pour les systèmes électroniques BES dont l'impact est « moyen » ou « élevé » ;
- 1er octobre 2017 pour les systèmes électroniques BES dont l'impact est « faible ».

Pour les entités qui ne possèdent ni des actifs critiques aux fins de normes CIP (version 1), ni des installations de production à vocation industrielle:

- 1er octobre 2018 pour les systèmes électroniques BES dont l'impact est « moyen » ou « élevé » ;
- 1er octobre 2019 pour les systèmes électroniques BES dont l'impact est « faible ».

Pour les entités qui possèdent des installations de production à vocation industrielle :

- 1er avril 2019 pour les systèmes électroniques BES dont l'impact est « moyen » ou « élevé » ;
- 1er avril 2020 pour les systèmes électroniques BES dont l'impact est « faible ».

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

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	29 juillet 2016	Nouvelle annexe. Décision D-2016-119 émise par la Régie de l'énergie : • Adoption de la norme et son annexe Québec • Suspension de l'application de la norme et de son annexe Québec pour les entités qui possèdent des installations de production à vocation industrielle	Nouvelle
1	16 septembre 2016	Décision D-2016-138 émise par la Régie de l'énergie reportant la date d'entrée en vigueur en ce qui a trait aux systèmes électroniques BES dont l'impact est « moyen » ou « élevé ».	Révision
2	21 mars 2017	Décision D-2017-031 émise par la Régie de l'énergie : • Levée de suspension d'application de la norme et de son annexe Québec pour les entités qui possèdent des installations de production à vocation industrielle • Fixe la date d'entrée en vigueur pour les entités qui possèdent des installations de production à vocation industrielle.	Révision