NORMES DE FIABILITÉ DE LA NERC
(VERSION FRANÇAISE)

A. Introduction

1. Titre : Cybersécurité — Catégorisation des systèmes électroniques BES

2. Numéro : CIP-002-5.1

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

4. Applicabilité :

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

4.1.1. Responsable de l'équilibrage

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

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

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

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

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

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

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

4.1.3. Exploitant d'installation de production

4.1.4. Propriétaire d'installation de production

4.1.5. Coordonnateur des échanges ou Responsable des échanges

4.1.6. Coordonnateur de la fiabilité

4.1.7. Exploitant de réseau de transport

4.1.8. Propriétaire d'installation de transport

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

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

4.2.1.1. Chaque système de DSF ou de DST qui :

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

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

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

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

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

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

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

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

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

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

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

5. Dates d'entrée en vigueur :

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

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

6. Contexte :

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

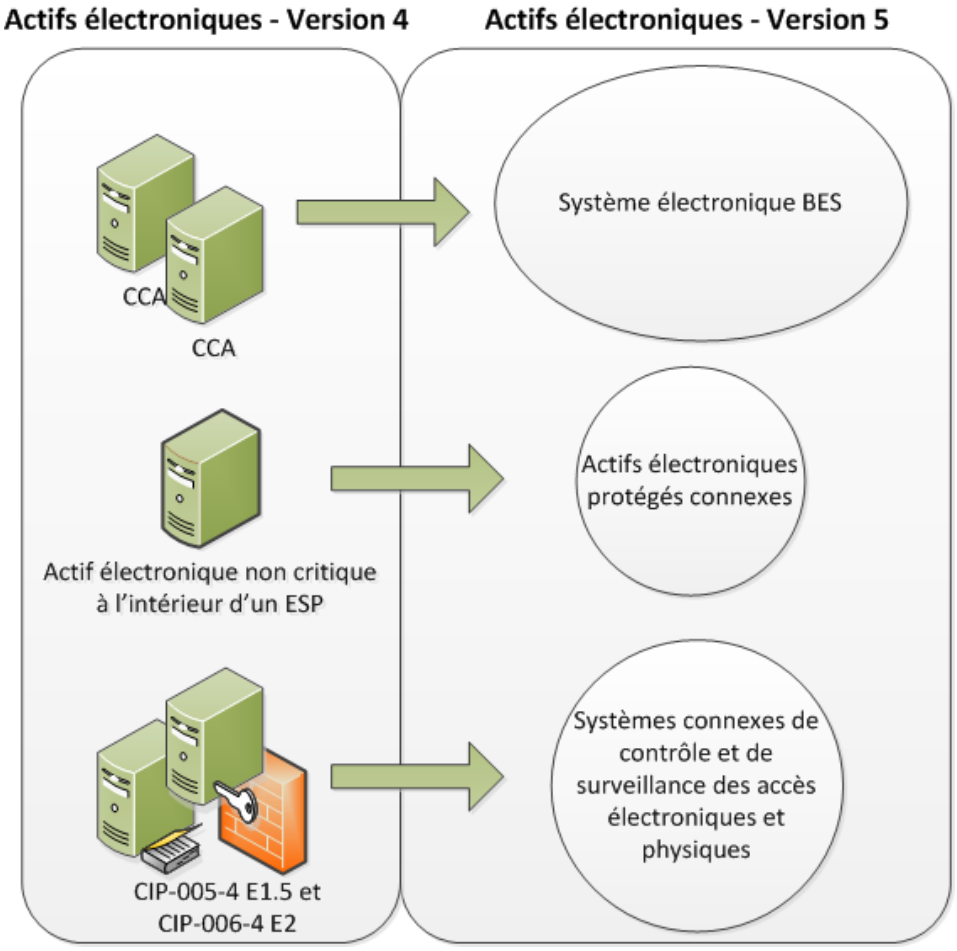
Dans l'ensemble des normes, sauf indication particulière, les éléments présentés sous forme de liste à puces dans les exigences sont des éléments liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

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

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

Systèmes électroniques BES

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



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

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

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

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

Exploitation fiable du BES

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

Exploitation en temps réel

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

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

Critères de catégorisation

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

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

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

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

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

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

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

B. Exigences et mesures

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

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

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

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

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

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

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

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

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

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

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

C. Conformité

1. Processus de surveillance de la conformité

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

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

1.2. Conservation des pièces justificatives

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

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

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

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

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

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

1.4. Autres informations sur la conformité

- Aucun

2. Tableau des éléments de conformité

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-002-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	**Planification de l'exploitation**	**Élevé**	Pour les entités responsables qui ont plus de 40 actifs BES au total à l'exigence E1, cinq pour cent ou moins des actifs BES n'ont pas été considérés conformément à l'exigence E1 ; OU Pour les entités responsables qui ont 40 actifs BES au total ou moins, 2 actifs BES ou moins à l'exigence E1 n'ont pas été considérés conformément à l'exigence E1 ; OU Pour les entités responsables qui ont plus de 100 *systèmes électroniques BES*	Pour les entités responsables qui ont plus de 40 actifs BES au total à l'exigence E1, plus de cinq pour cent, mais au plus 10 pour cent des actifs BES n'ont pas été considérés conformément à l'exigence E1 ; OU Pour les entités responsables qui ont 40 actifs BES au total ou moins, plus de deux, mais au plus quatre actifs BES à l'exigence E1 n'ont pas été considérés conformément à l'exigence E1 ; OU Pour les entités responsables qui ont	Pour les entités responsables qui ont plus de 40 actifs BES au total à l'exigence E1, plus de 10 pour cent, mais au plus 15 pour cent des actifs BES n'ont pas été considérés conformément à l'exigence E1 ; OU Pour les entités responsables qui ont 40 actifs BES au total ou moins, plus de quatre, mais au plus six actifs BES à l'exigence E1 n'ont pas été considérés conformément à l'exigence E1 ; OU Pour les entités responsables qui ont	Pour les entités responsables qui ont plus de 40 actifs BES au total à l'exigence E1, plus de 15 pour cent des actifs BES n'ont pas été considérés conformément à l'exigence E1 ; OU Pour les entités responsables qui ont 40 actifs BES au total ou moins, plus de six actifs BES à l'exigence E1 n'ont pas été considérés conformément à l'exigence E1 ; OU Pour les entités responsables qui ont plus de 100 *systèmes électroniques BES* d'impact élevé ou

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-002-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			d'impact élevé ou moyen au total, cinq pour cent ou moins des *systèmes électroniques BES* identifiés n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une catégorie plus basse; OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* d'impact élevé ou moyen ou moins au total, cinq des *systèmes électroniques BES* identifiés ou moins n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une catégorie plus basse; OU Pour les entités	plus de 100 *systèmes électroniques BES* d'impact élevé ou moyen au total, plus de cinq pour cent, mais au plus 10 pour cent des *systèmes électroniques BES* identifiés n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une catégorie plus basse ; OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* d'impact élevé ou moyen ou moins au total, plus de cinq, mais au plus 10 *systèmes électroniques BES* identifiés n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une	plus de 100 *systèmes électroniques BES* d'impact élevé ou moyen au total, plus de 10 pour cent, mais au plus 15 pour cent des *systèmes électroniques BES* identifiés n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une catégorie plus basse ; OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* d'impact élevé ou moyen ou moins au total, plus de 10, mais au plus 15 *systèmes électroniques BES* identifiés n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une	moyen au total, plus de 15 pour cent des *systèmes électroniques BES* identifiés n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une catégorie plus basse ; OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* d'impact élevé ou moyen ou moins au total, plus de 15 *systèmes électroniques BES* identifiés n'ont pas été catégorisés ou ont été incorrectement catégorisés dans une catégorie plus basse ; OU Pour les entités responsables qui ont plus de 100 *systèmes*

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-002-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			responsables qui ont plus de 100 *systèmes électroniques BES* d'impact élevé ou moyen au total, cinq pour cent ou moins des *systèmes électroniques BES* d'impact élevé ou moyen n'ont pas été identifiés; OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* d'impact élevé ou moyen ou moins au total, cinq *systèmes électroniques BES* d'impact élevé ou moyen ou moins n'ont pas été identifiés.	catégorie plus basse ; OU Pour les entités responsables qui ont plus de 100 *systèmes électroniques BES* d'impact élevé ou moyen au total, plus de cinq pour cent, mais au plus 10 pour cent des *systèmes électroniques BES* d'impact élevé ou moyen n'ont pas été identifiés ; OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* d'impact élevé ou moyen ou moins au total, plus de cinq, mais au plus 10 *systèmes électroniques BES* d'impact élevé ou moyen ou moins n'ont	catégorie plus basse ; OU Pour les entités responsables qui ont plus de 100 *systèmes électroniques BES* d'impact élevé ou moyen au total, plus de 10 pour cent, mais au plus 15 pour cent des *systèmes électroniques BES* d'impact élevé ou moyen n'ont pas été identifiés ; OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* d'impact élevé ou moyen ou moins au total, plus de 10, mais au plus 15 *systèmes électroniques BES* d'impact élevé ou moyen ou moins n'ont	*électroniques BES* d'impact élevé ou moyen au total, plus de 15 pour cent des *systèmes électroniques BES* d'impact élevé ou moyen n'ont pas été identifiés ; OU Pour les entités responsables qui ont 100 *systèmes électroniques BES* d'impact élevé ou moyen ou moins au total, plus de 15 *systèmes électroniques BES* d'impact élevé ou moyen ou moins n'ont pas été identifiés.

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-002-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				pas été identifiés.	pas été identifiés.	
E2	**Planification de l'exploitation**	**Faible**	L'entité responsable n'a pas complété son passage en revue et sa mise à jour pour l'identification exigée en E1 à l'intérieur de 15 mois civils, mais en au plus 16 mois civils du passage en revue précédent. (E2.1) OU L'entité responsable n'a pas complété son approbation des identifications exigées en E1 par le *cadre supérieur CIP* ou son délégué conformément à l'exigence E2 à l'intérieur de 15 mois civils, mais en au plus 16 mois civils de l'approbation précédente. (E2.2)	L'entité responsable n'a pas complété son passage en revue et sa mise à jour pour l'identification exigée en E1 à l'intérieur de 16 mois civils, mais en au plus 17 mois civils du passage en revue précédent. (E2.1) OU L'entité responsable n'a pas complété son approbation des identifications exigées en E1 par le *cadre supérieur CIP* ou son délégué conformément à l'exigence E2 à l'intérieur de 16 mois civils, mais en au plus 17 mois civils de l'approbation précédente. (E2.2)	L'entité responsable n'a pas complété son passage en revue et sa mise à jour pour l'identification exigée en E1 à l'intérieur de 17 mois civils, mais en au plus 18 mois civils du passage en revue précédent. (E2.1) OU L'entité responsable n'a pas complété son approbation des identifications exigées en E1 par le *cadre supérieur CIP* ou son délégué conformément à l'exigence E2 à l'intérieur de 17 mois civils, mais en au plus 18 mois civils de l'approbation précédente. (E2.2)	L'entité responsable n'a pas complété son passage en revue et sa mise à jour pour l'identification exigée en E1 à l'intérieur de 18 mois civils du passage en revue précédent. (E2.1) OU L'entité responsable n'a pas complété son approbation des identifications exigées en E1 par le *cadre supérieur CIP* ou son délégué conformément à l'exigence E2 à l'intérieur de 18 mois civils de l'approbation précédente. (E2.2)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

CIP-002-5.1 – Annexe 1

Critères de degré d'impact

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

1. Impact élevé (H)

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

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

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

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

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

2. Impact moyen (M)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Impact faible (L)

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

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

3.2. Postes de transport ;

3.3. Ressources de production ;

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

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

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

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 qualifié à la section 4.1, qui est visée par les exigences de la norme. 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. Cette section est particulièrement importante dans la norme CIP-002-5.1 et délimite l'ensemble des *installations*, systèmes et équipements auxquels s'appliquent les critères de l'annexe 1. C'est important, car cela détermine les *installations*, systèmes et équipements qui sont classés dans la catégorie Impact faible, après filtrage de ceux qui répondent aux critères des catégories Impact élevé et Impact moyen.

Dans le but d'identifier les groupes d'*installations*, de systèmes et d'équipements (par leur emplacement ou autrement), l'entité responsable identifie les actifs de la façon décrite à l'exigence E1 de la norme CIP-002-5.1. Ceci est une démarche familière pour les entités responsables qui ont à se conformer aux versions 1, 2, 3 et 4 des normes CIP pour les *actifs critiques*. Comme dans les versions 1, 2, 3 et 4, les entités responsables peuvent utiliser des postes, des centrales et des centres de contrôle à des emplacements uniques pour désigner ces groupes d'installations, de systèmes et d'équipements.

CIP-002-5.1

La norme CIP-002-5.1 stipule que les entités responsables concernées doivent catégoriser leurs *systèmes électroniques BES* et les *actifs électroniques BES* connexes selon les critères de l'annexe 1. Un *actif électronique BES* inclut dans sa définition, « s'il était rendu indisponible, endommagé, ou mal utilisé , aurait, dans les 15 minutes un impact négatif sur l'exploitation fiable du BES ».

Ce qui suit donne des indications qu'une entité responsable peut utiliser pour identifier les *systèmes électroniques BES* qui seraient dans la portée. Le concept de fonction de fiabilité du BES est utile à cet égard, car il offre à l'entité responsable une méthode définie pour déterminer les *systèmes électroniques BES* auxquels s'applique la norme CIP-002-5.1. Ce concept établit une liste de fonctions de fiabilité du BES. Ces fonctions comprennent :

Réponse dynamique aux conditions du BES
Équilibre production-charge
Contrôle de la fréquence (puissance active)
Contrôle de la tension (puissance réactive)
Gestion des contraintes
Surveillance et contrôle
Remise en charge du BES
Connaissance de la situation
Coordination et communication en temps réel entre les entités

La responsabilité de l'exploitation fiable du BES est répartie entre toutes les catégories d'entités. Chaque catégorie d'entité apporte une contribution particulière à l'exploitation fiable et l'exposé qui suit aide à identifier quelle catégorie d'entité, dans le contexte des entités fonctionnelles auxquelles ces normes CIP s'appliquent, effectue quelle fonction de fiabilité, dans le cadre d'un processus pour identifier les *systèmes électroniques BES* qui seraient visés. Ce qui suit donne des indications pour aider les entités responsables à déterminer les fonctions de fiabilité applicables selon leur type de fonctions enregistrées.

Entité fonctionnelle	RC	BA	TOP	TO	DP	GOP	GO
Réponse dynamique		X	X	X	X	X	X
Équilibre production-charge	X	X	X	X	X	X	X
Contrôle de la fréquence		X				X	X
Contrôle de la tension			X	X	X		X
Gestion des contraintes	X		X			X	
Surveillance et contrôle			X			X	
Remise en charge			X			X	
Connaissance de la situation	X	X	X			X	
Coordination entre les entités	X	X	X	X		X	X

Réponse dynamique

La fonction de réponse dynamique comprend les actions effectuées par des *éléments* BES ou des sous-systèmes qui sont lancés automatiquement pour amorcer une réponse à une condition du BES. Ces actions sont lancées par un seul élément, un dispositif de commande, ou par une combinaison de ces éléments ou dispositifs agissant de concert pour effectuer une

action ou pour engendrer une condition en réponse à l'action ou à la condition initiale. Les types de réponses dynamiques qui peuvent être considérés comme ayant un impact potentiel sur le BES sont :

- Réserves tournantes (réserves pour contingence)
  - Fourniture d'une réserve de production au besoin (GO et GOP)
  - Surveillance que les réserves sont suffisantes (BA)
- Réponse du régulateur de vitesse
  - Système de commande agissant sur le régulateur de vitesse (GO)
- Systèmes de protection (transport et production)
  - Lignes, jeux de barres, transformateurs et groupes turbine-alternateur (DP, TO, TOP, GO et GOP)
  - Protection de zone sur défaillance de disjoncteur (DP, TO et TOP)
  - Protection de disjoncteur (DP, TO et TOP)
  - Courant, fréquence, vitesse, phase (TO, TOP, GO et GOP)
- *Automatismes de réseau* ou *plans de défense*
  - Capteurs, relais et disjoncteurs, possiblement logiciels (DP, TO et TOP)
- Protection par relais de surfréquence et de sous-fréquence (comprend le délestage de charge automatique)
  - Capteurs, relais et disjoncteurs (DP)
- Protection par relais de surtension et de sous-tension (comprend le délestage de charge automatique)
  - Capteurs, relais et disjoncteurs (DP)
- Stabilisateurs de puissance (GO)

Équilibre production-charge

La fonction d'équilibre production-charge comprend les activités, actions et conditions nécessaires pour surveiller et contrôler la production et la charge dans l'horizon de planification de l'exploitation et en temps réel. Les aspects de la fonction d'équilibre production-charge comprennent, mais n'y sont pas limités :

- Calcul de l'*écart de réglage de la zone* (ACE)
  - Sources de données sur le terrain (transits d'interconnexion en temps réel, sources de fréquence, écart de temps, etc.) (TO et TOP)
  - Logiciels utilisés pour effectuer les calculs (BA)
- Réponse à la demande

  - Capacité de détecter les besoins de modulation de la charge (BA)
  - Capacité de moduler la charge (TOP et DP)
- Délestages de *charge* commandés manuellement
  - Capacité de détecter les besoins de modulation de la charge (BA)
  - Capacité de moduler la charge (TOP et DP)
- Réserve arrêtée (réserve pour contingence)
  - Connaissance de l'état de marche, de la capacité, du taux de rampe et du temps de démarrage des groupes (GO et BA)
  - Démarrage des groupes de production et fourniture de l'énergie (GOP)

Contrôle de la fréquence (puissance active)

La fonction de contrôle de la fréquence comprend les activités, actions et conditions qui assurent, en temps réel, que la fréquence demeure à l'intérieur de limites acceptables pour la fiabilité et l'exploitabilité du BES. Les aspects de la fonction de contrôle de la fréquence comprennent, mais y sont limités :

- Contrôle de la production (par exemple, AGC)
  - ACE, sortie des groupes courante, taux de rampe, caractéristiques des groupes de production (BA, GOP et GO)
  - Logiciels pour le calcul des réglages à apporter aux groupes (BA)
  - Transmission des réglages aux différents groupes (GOP)
  - Mise en œuvre d'ajustements par les dispositifs de réglage des groupes (GOP)
- Régulation (réserves réglantes)
  - Source de fréquence, programme (BA)
  - Système de commande de régulateur (GO)

Contrôle de la tension (puissance réactive)

La fonction de contrôle de la tension comprend les activités, actions et conditions qui assurent, en temps réel, que la tension demeure à l'intérieur de limites acceptables pour la fiabilité et l'exploitabilité du BES. Les aspects de la fonction de contrôle de la tension comprennent, mais n'y sont pas limités :

- Régulation automatique de la tension (AVR)
  - Capteurs, système de commande de stator et rétroaction (GO)
- Ressources capacitives

  - État, commande (manuelle ou automatique) et rétroaction (TOP, TO et DP)
- Ressources inductives (changeurs de prises de transformateur ou bobines d'inductance)
  - État, commande (manuelle ou automatique) et rétroaction (TOP, TO et DP)
- Compensateurs statiques (SVC)
  - État, calculs, commande (manuelle ou automatique) et rétroaction (TOP, TO et DP)

Gestion des contraintes

La gestion des contraintes comprend les activités, actions et conditions qui sont nécessaires pour assurer que les éléments du BES fonctionnent à l'intérieur de leurs limites de conception et des contraintes établies pour la fiabilité et l'exploitabilité du BES. Les aspects de la gestion des contraintes comprennent, mais n'y sont pas limités :

- *Capacité de transfert disponible* (ATC) (TOP)
- Programmes d'échange (TOP et RC)
- Corrections à la répartition de la production et affectation des groupes (GOP)
- Détermination et surveillance des SOL et des IROL (TOP et RC)
- Détermination et surveillance des interfaces de transit (TOP et RC)

Surveillance et contrôle

La fonction de surveillance et de contrôle comprend les activités, actions et conditions qui assurent la surveillance et le contrôle des *éléments* BES. Voici un exemple d'aspect de la fonction de surveillance et de contrôle :

- Toutes les méthodes de manœuvre des disjoncteurs et des sectionneurs
  - SCADA (TOP et GOP)
  - Automatisation des postes (TOP)

Remise en charge du BES

La fonction de remise en charge du BES comprend les activités, actions et conditions nécessaires pour passer d'un état de panne à une situation d'exploitation permettant le transport d'énergie sans aide externe. Les aspects de la fonction de remise en charge du BES comprennent, mais n'y sont pas limités :

- Remise en charge, y compris le chemin de démarrage planifié
  - Au moyen de groupes à démarrage autonome (TOP et GOP)
  - Au moyen de lignes d'interconnexion (TOP et GOP)

- Alimentation électrique externe de centrale nucléaire (TOP, TO, BA, RC, DP, GO et GOP)
- Coordination (TOP, TO, BA, RC, DP, GO et GOP)

Connaissance de la situation

La fonction de connaissance de la situation comprend les activités, actions et conditions établies par des politiques, des directives ou des procédures d'exploitation normalisées nécessaires pour évaluer la situation courante du BES et de prévoir les effets de changements planifiés ou non planifiés sur les conditions d'exploitation. Les aspects de la fonction de connaissance de la situation comprennent :

- Surveillance et alarmes (tel qu'alarmes EMS) (TOP, GOP, RC et BA)
- Gestion des changements (TOP, GOP, RC et BA)
- Planification du jour même et du jour suivant (TOP)
- Analyse des contingences (RC)
- Surveillance de la fréquence (BA et RC)

Coordination entre les entités

La fonction de coordination et de communication entre les entités comprend les activités, actions et conditions établies par des politiques, des directives ou des procédures d'exploitation normalisées nécessaires pour la coordination et la communication entre les entités responsables afin d'assurer la fiabilité et l'exploitabilité du BES. Les aspects de la fonction de coordination et de communication entre les entités comprennent :

- Échanges programmés (BA, TOP, GOP et RC)
- Données d'exploitation et état des installations (TO, TOP, GO, GOP, RC et BA)
- Directives d'exploitation (TOP, RC et BA)

Applicabilité aux distributeurs

Il est attendu que seuls les *distributeurs* qui détiennent ou exploitent des installations qui se qualifient à la section Applicabilité seront visés par la version 5 des normes de cybersécurité. Les *distributeurs* qui ne détiennent ni n'exploitent des installations qui se qualifient ne sont pas visés par ces normes. Les critères d'applicabilité sont fondés sur les exigences d'inscription au titre de *distributeur* et sur les exigences de la norme EOP 005 de la NERC visant les *distributeurs*.

Exigence E1

L'exigence E1 met en oeuvre une méthode de catégorisation des *systèmes électroniques BES* selon leur impact sur le BES. Dans l'équation traditionnelle d'évaluation du risque, cette

méthode réduit la mesure du risque à l'évaluation de l'impact (la conséquence), en supposant un indice de vulnérabilité de 1 (les systèmes sont présumés vulnérables) et une probabilité de menace de 1 (probabilité de 100 %). Les critères de l'annexe 1 expriment le degré d'impact des actifs BES desservis par les *systèmes électroniques BES*.

Les entités responsables sont tenues d'inventorier et de catégoriser les *systèmes électroniques BES* dont l'impact est élevé ou moyen. Les *systèmes électroniques BES* pour les actifs BES qui ne répondent pas aux critères 1.1 à 1.4 et 2.1 à 2.11 de l'annexe 1 sont classés par défaut dans la catégorie Impact faible.

Annexe 1

Application générale

Dans l'application des critères de l'annexe 1, les entités responsables doivent prendre note que l'approche utilisée est basée sur l'impact du *système électronique BES* tel que mesuré par les critères précis définis à l'annexe 1.

- Lorsque l'équipe de rédaction utilise le terme « *installations* », les entités responsables disposent d'une certaine latitude pour déterminer les *installations* concernées. Le terme « *installation* » est défini dans le glossaire de la NERC comme un « ensemble d'équipements électriques qui fonctionnent comme un seul élément du *système de production-transport d'électricité* (exemples : ligne, groupe de production, compensateur shunt, transformateur, etc.). » Dans la plupart des cas, les critères réfèrent à un groupe d'*installations* dans un emplacement donné qui contribue à l'exploitation fiable du BES. Par exemple, pour les actifs de *transport*, le poste peut être désigné comme le groupe d'*installations*. Cependant, dans un poste qui comprend à la fois de l'équipement utilisé pour l'exploitation du BES et de l'équipement utilisé seulement pour les opérations de distribution, il peut être préférable pour l'entité responsable de considérer seulement le groupe d'installations utilisé pour l'exploitation du BES. Dans ce cas, l'entité responsable peut désigner le groupe d'installations par son emplacement, avec des restrictions pour cibler le groupe d'installations qui contribue à l'exploitation fiable du BES, comme étant les *installations* qui sont visées par les critères de catégorisation des *systèmes électroniques BES*. Les *installations* de production sont discutées séparément à la section Production ci-après. Dans la norme CIP-002-5.1, ces groupes d'*installations*, de systèmes et d'équipements sont parfois appelés « actifs BES ». Par exemple, un actif BES identifié peut être un poste, une centrale de production ou un *centre de contrôle* nommé. Les entités responsables disposent d'une souplesse dans la manière de grouper les *installations*, systèmes et équipements à un emplacement donné.
- Dans certains cas, un *système électronique BES* peut être catégorisé par le respect de plusieurs critères. Dans de tels cas, l'entité responsable peut choisir de documenter tous les critères qui mènent à la catégorisation. Cela évitera une catégorisation incorrecte lorsqu'il ne répond plus à l'un des critères, mais qu'il répond encore à un autre.

- Il est recommandé que chaque *système électronique BES* soit inventorié par une seule entité responsable. En cas de propriété commune, il est conseillé aux entités responsables propriétaires de s'entendre formellement sur la désignation de l'entité responsable de la conformité aux normes.

Impact élevé (H)

Cette catégorie comprend les *systèmes électroniques BES*, utilisés par et dans des *centres de contrôle* (et les centres informatiques connexes inclus dans la définition de *centres de contrôle*), qui s'acquittent des obligations fonctionnelles du *coordonnateur de la fiabilité* (RC), du *responsable de l'équilibrage* (BA), de l'*exploitant de réseau de transport* (TOP) ou de l'*exploitant d'installation de production* (GOP) telles que définies dans le modèle fonctionnel de la NERC à la rubrique « Tasks » de la fonction pertinente et à la rubrique « Relationship with Other Entities » de l'entité fonctionnelle, et qui répondent aux critères 1.1, 1.2, 1.3 ou 1.4 de l'annexe 1. Bien que les entités inscrites au titre des entités fonctionnelles susmentionnées soient explicitement visées, il peut y avoir des cas d'ententes par lesquelles certaines des obligations fonctionnelles d'un exploitant de réseau de transport (TOP) sont déléguées à un propriétaire d'installation de transport (TO). Dans de tels cas, les *systèmes électroniques BES* des *centres de contrôle* du TO qui s'acquittent de ces obligations fonctionnelles pourraient être classés dans la catégorie Impact élevé. Les critères sont axés spécifiquement sur les obligations fonctionnelles, et non nécessairement sur les installations du RC, du BA, du TOP ou du GOP. Il est à noter que la définition de *centre de contrôle* renvoie spécifiquement aux tâches de fiabilité du RC, du BA, du TOP et du GOP. Un *système électronique BES* de TO dans une installation de TO qui ne remplit pas ces tâches, et qui n'a pas d'entente avec un TOP pour les remplir, ne répond pas à la définition de *centre de contrôle*. Cependant, si ce *système électronique BES* commande une ou des installations qui répondent aux critères de la catégorie Impact moyen, ce *système électronique BES* serait catégorisé comme un *système électronique BES* à impact moyen.

Le seuil de 3 000 MW défini au critère 1.2 pour les *centres de contrôle* de BA assure une différentiation suffisante du seuil défini pour les *centres de contrôle* à impact moyen de BA. Une analyse des empreintes des BA montre que la plupart des BA dont l'impact est important sont couverts par ce critère.

Des seuils supplémentaires, définis dans les critères, s'appliquent à cette catégorie.

Impact moyen (M)

Production

Les critères de la catégorie Impact moyen de l'annexe 1 qui s'appliquent généralement aux propriétaires et aux *exploitants d'installation de production* (GO et GOP) sont les critères 2.1, 2.3, 2.6, 2.9 et 2.11. Le critère 2.13, qui s'applique aux *centres de contrôle* de BA, est également inclus ici.

- Le critère 2.1 désigne comme Impact moyen les *systèmes électroniques BES* qui influent sur des ressources de production dont la capacité en puissance active nette est supérieure à 1 500 MW. Le critère de 1 500 MW est partiellement tiré des exigences de *réserve pour contingence* de la norme BAL-002 de la NERC, dont l'objet est de « s'assurer que le responsable de l'équilibrage peut utiliser sa réserve pour contingence afin d'équilibrer les ressources et la demande, et rétablir la fréquence de l'Interconnexion dans les limites établies après une *perturbation à déclarer* ». En particulier, elle exige qu'« au minimum, le *responsable de l'équilibrage* ou le *groupe de partage des réserves* doit disposer d'une *réserve pour contingence* suffisante afin de se protéger contre la contingence simple la plus grave. » L'équipe de rédaction a utilisé 1 500 MW comme chiffre provenant des *réserves pour contingence* les plus importantes exploitées par divers BA dans toutes les régions.

  Par l'utilisation de la capacité en puissance active nette, l'équipe de rédaction a cherché à utiliser une valeur qui pourrait être vérifiée d'après les exigences existantes proposées dans la norme MOD-024 de la NERC et compte tenu des efforts de développement actuels dans ce secteur.

  En utilisant le critère précis de 1 500 MW, l'intention de l'équipe de rédaction est de s'assurer que les *systèmes électroniques BES* ayant des vulnérabilités en mode commun qui pourraient entraîner la perte de 1 500 MW ou plus de production à une même centrale pour un groupe de production ou un ensemble de groupe de production soit protégés adéquatement.

  L'équipe de rédaction a aussi utilisé d'autres paramètres de temps et de valeur pour s'assurer que les critères précis et leurs valeurs de comparaison soient relativement stables au cours de la période d'examen. Lorsque plusieurs valeurs de capacité en puissance active nette pouvaient être utilisées pour classer une installation selon ces critères précis, la valeur la plus élevée a été utilisée.

- Pour le critère 2.3, l'équipe de rédaction a cherché à s'assurer que les *systèmes électroniques BES* pour les *installations* de production désignées par le *coordonnateur de la planification* ou le *planificateur de réseau de transport* comme étant nécessaires pour éviter des *impacts négatifs sur la fiabilité* du BES dans un horizon de planification d'un an ou plus soient catégorisés comme Impact moyen. En spécifiant un horizon de planification d'un an ou plus, l'intention est de s'assurer qu'il s'agit de groupes qui sont identifiés dans le cadre d'une planification de fiabilité « à long terme », s'étendant sur une période d'exploitation d'au moins 12 mois. Cela ne signifie pas nécessairement que le jour où le groupe sera exploité est dans plus d'un an, mais plutôt que la période de planification est de plus d'un an ; on cherche spécifiquement à éviter que le critère s'applique à une production destinée à remédier à des problèmes urgents de fiabilité à court terme. De telles installations peuvent être désignées comme « indispensables à la fiabilité » (*Reliability Must Run*), et il ne faut pas les confondre avec les installations de production désignées comme indispensables (*must run*) pour la stabilisation du marché. Comme l'emploi de l'expression « *must run* » entraîne une certaine confusion à bien des égards, l'équipe de rédaction a choisi de l'éviter et a formulé l'exigence dans un langage de fiabilité plus générique. En

particulier, l'accent mis sur la prévention des *impacts négatifs sur la fiabilité* impose que ces groupes soient désignés comme indispensables aux fins de la fiabilité au-delà de l'échelle locale. Les groupes désignés comme indispensables au maintien de la tension à l'échelle locale ne seraient généralement pas désignés comme tel. En l'absence de *coordonnateur de la planification* désigné, le *planificateur de réseau de transport* est l'entité inscrite qui effectue cette désignation.

Si des études de réseau permettent de conclure que le fonctionnement d'un groupe est indispensable à la fiabilité du BES, par exemple en cas de contingence de catégorie C3 telle que définie dans la TPL-003, les *systèmes électroniques BES* pour ce groupe sont alors catégorisés comme Impact moyen.

Les normes TPL exigent que, si les études et plans indiquent le besoin d'actions supplémentaires, ces études et plans soient communiqués par le *coordonnateur de la planification* ou le *planificateur de réseau de transport* par écrit à l'entité régionale/RRO. Les actions nécessaires pour la mise en œuvre de ces plans par les parties concernées (propriétaires ou exploitants d'installation de production, *coordonnateurs de la fiabilité* ou autre partie nécessaire) sont habituellement officialisées sous la forme d'une entente ou d'un contrat.

- Le critère 2.6 vise les *systèmes électroniques BES* des *installations* de production désignées comme essentiels pour le calcul des IROL et de leurs contingences associées, tel que spécifié par la norme FAC-014-2, *Établir et communiquer les limites d'exploitation du réseau*, exigences E5.1.1 et E5.1.3.

  Les IROL peuvent être basés sur des phénomènes de *réseau* dynamiques comme l'instabilité ou l'effondrement de la tension. Le calcul de ces IROL et de leurs contingences associées tient souvent compte de l'effet de l'inertie de la production et de la réponse des AVR.

- Le critère 2.9 catégorise les *systèmes électroniques BES* associés aux *automatismes de réseau* et aux *plans de défense* comme Impact moyen. Les *automatismes de réseau* et les *plans de défense* peuvent être mis en œuvre pour prévenir les perturbations qui entraineraient un dépassement des IROL s'ils n'assuraient pas la fonction requise au moment voulu ou s'ils avaient un fonctionnement non conforme à leurs critères de conception. Les *propriétaires d'installation de production* et les *exploitants d'installation de production* qui possèdent des *systèmes électroniques BES* pour de tels automatismes de réseau et plans de défense les classent dans la catégorie Impact moyen.

- Le critère 2.11 classe dans la catégorie Impact moyen les *systèmes électroniques BES* utilisés par et dans des *centres de contrôle* qui s'acquittent des obligations fonctionnelles de l'*exploitant d'installation de production* pour une production totale de 1 500 MW ou plus dans une seule Interconnexion, et qui n'ont pas déjà été inclus dans la partie 1.

- Le critère 2.13 classe dans la catégorie Impact moyen les *centres de contrôle* de BA qui « contrôlent » une production de 1 500 MW ou plus dans une même Interconnexion et qui n'ont pas déjà été inclus dans la partie 1. Le seuil de 1 500 MW est cohérent avec le degré d'impact et le raisonnement indiqué pour le critère 2.1.

Transport

Le SDT utilise les expressions « Transmission Facilities at a single station or substation » et « Transmission stations or substations » pour reconnaître l'existence des termes « stations » et « substations ». Plusieurs entités de l'industrie considèrent un « substation » comme étant un emplacement avec des frontières physiques (Ex. : clôture, mur, etc.) qui renferme au moins un autotransformateur. Des emplacements ne renfermant pas d'autotransformateurs existent également, et plusieurs entités de l'industrie réfèrent à ces emplacements comme étant des « stations » ou « switchyards ». Par conséquent, le SDT a choisi d'utiliser les deux termes « station » et « substation » pour référer aux emplacements où des ensembles d'installations de transport existent.

- Les critères 2.2, 2.4 à 2.10 et 2.12 de l'annexe 1 s'appliquent aux *propriétaires d'installation de transport* et aux *exploitants de réseau de transport*. Dans plusieurs de ces critères, le seuil d'impact est défini comme la capacité de défaillance ou de compromission d'un système à entraîner le dépassement d'une ou de plusieurs *limites d'exploitation pour la fiabilité de l'Interconnexion* (IROL). Le critère 2.2 couvre les *systèmes électroniques BES* pour les *installations* de *réseaux* de *transport* qui fournissent des ressources de puissance réactive permettant d'améliorer et de préserver la fiabilité du BES. La valeur nominale est utilisée ici, car il n'y a pas d'exigence de la NERC pour vérifier la capacité réelle de ces *installations*. La valeur de 1 000 Mvar utilisée dans ce critère est une valeur jugée raisonnable pour déterminer la criticité de l'impact.

- Le critère 2.4 couvre les *systèmes électroniques BES* pour toute *installation* de *transport* située dans un poste exploité à 500 kV ou plus. Bien que l'équipe de rédaction considère que les *installations* exploitées à 500 kV ou plus ne nécessitent pas de précisions supplémentaires quant à leur rôle dans le système de réseaux interconnectés formant le BES, les *installations* dans le bas de la fourchette THT devraient avoir des critères supplémentaires pour inclusion dans la catégorie Impact moyen.

  Il est à noter que si le jeu de barres collectrices d'une centrale de production (la centrale est plus petite que le seuil établi pour la production au critère 2.1) est exploité à 500 kV, ce jeu de barres devrait être considéré comme une *installation* de raccordement de la production et non comme une *installation* de *transport*, selon le document « *Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface »*. Ce jeu de barres collectrices ne serait pas une installation pour un *système électronique BES* à impact moyen, car il ne touche pas significativement le réseau de *transport* à 500 kV ; il ne touche qu'une centrale qui se trouve sous le seuil de production.

- Le critère 2.5 couvre les *systèmes électroniques BES* pour les installations dans le bas de la fourchette de transport du BES avec des qualifications pour l'inclusion, si elles sont jugées très susceptibles d'avoir un impact significatif sur le BES. Bien que ce critère ait été défini dans le cadre du raisonnement exigeant la protection contre tout impact significatif sur le BES, l'équipe de rédaction a inclus dans ce critère des qualifications supplémentaires qui assurerait un degré suffisant d'impact sur le BES. Ainsi, l'équipe de rédaction :

    - exclut les installations radiales qui fournirait du support pour une seule installation de production ;

    - spécifie le raccordement à au moins trois postes de transport pour s'assurer que le degré d'impact soit approprié.

  La valeur pondérée totale de 3 000 a été obtenue à partir des valeurs pondérées liées à trois lignes à 345 kV et à cinq lignes à 230 kV à un poste de transport. La valeur pondérée totale sert à représenter l'impact réel sur le BES, indépendamment de la tension nominale de chaque ligne et de la combinaison de lignes de différentes tensions nominales.

  De plus, dans le document *Integrated Risk Assessment Approach – Refinement to Severity Risk Index – Attachment 1* de la NERC, le rapport a utilisé une charge de ligne moyenne en MVA basée sur la tension nominale :

    - 230 kV –> 700 MVA

    - 345 kV –> 1 300 MVA

    - 500 kV –> 2 000 MVA

    - 765 kV –> 3 000 MVA

  Pour ce qui est de déterminer les lignes visées et les raccordements à d'« autres postes de transport », les éléments suivants devraient être considérés :

    - Dans le cas des autotransformateurs d'un poste, les entités responsables disposent d'une latitude pour déterminer si les groupes d'*installations* sont considérés comme un seul emplacement de poste ou plusieurs postes. Dans la plupart des cas, les entités responsables les considèreraient probablement comme des *installations* à un seul poste, à moins qu'elles soient dispersées géographiquement. Dans le cas de transformateurs situés à l'intérieur d'une clôture d'un poste, les autotransformateurs peuvent ne pas compter comme des raccordements distincts à d'autres postes. L'utilisation de *systèmes électroniques BES* communs serait de nature à invalider toute autre considération. Dans le cas d'autotransformateurs dispersés géographiquement par rapport à un emplacement de poste, le calcul tiendrait compte de tous les raccordements d'arrivée et de départ à chaque poste.

    - Les lignes à dérivations multiples sont considérées représenter une seule valeur pondérée par ligne et influent sur le nombre de raccordements à d'autres postes.

Ainsi, une seule ligne à 230 kV à dérivations multiples entre trois postes de *transport* représenterait une valeur pondérée totale de 700 et raccorde des *installations* de *transport* d'un seul poste à deux autres postes de *transport*.

- Les lignes multiples entre deux postes de transport sont considérées représenter plusieurs valeurs pondérées par ligne, mais ces lignes multiples entre les deux postes raccordent seulement un poste à un autre poste. Ainsi, deux lignes à 345 kV entre deux postes de *transport* représenteraient une valeur pondérée totale de 2 600, et raccorde les *installations* de *transport* d'un seul poste à un autre poste de *transport*.

La qualification du critère 2.5 pour les *installations* de *transport* dans un poste de *transport* est basée sur deux conditions distinctes :

1. La première condition est que les installations de transport à un seul poste dans le cas où le poste est raccordé, à des niveaux de tension de 200 kV ou plus, à trois (3) autres postes, à trois autres postes. Cette condition vise à assurer que les raccordements exploités à de tensions de 500 kV ou plus soient également compris dans le compte des raccordements à d'autres postes.
2. La deuxième condition est que la valeur totale de toutes les lignes d'arrivée ou de départ du poste doit dépasser 3 000. Cette condition ne comprend pas la considération des lignes exploitées à moins de 200 kV ou à 500 kV et plus, ce dernier cas se qualifiant déjà comme impact moyen selon le critère 2.4 : il n'y a pas de valeur à assigner aux lignes dont la tension est de moins de 200 kV ou de 500 kV et plus dans le tableau des valeurs pour la contribution la valeur combinée de 3 000.

Les *installations* de *transport* dans le poste doivent répondre à ces deux conditions pour être considérées comme se qualifiant au critère 2.5.

- Le critère 2.6 couvre les *systèmes électroniques BES* pour les *installations* de *transport* qui ont été identifiées comme essentielles pour le calcul des IROL et de leurs contingences associées, tel que spécifié par la FAC-014-2, **Établir et communiquer les limites d'exploitation du réseau**, E5.1.1 et E5.1.3.

- Le critère 2.7 est tiré de la norme NUC-001 de la NERC, exigence E9.2.2, pour le support des *installations* nucléaires. NUC-001 assure que la fiabilité des NPIR est assurée par une coordination adéquate entre le propriétaire ou l'*exploitant d'installation de production* nucléaire et son fournisseur de *transport* « afin que l'exploitation et les arrêts de centrale se déroulent en toute sécurité. ». En particulier, il y a des exigences spécifiques pour coordonner la sécurité physique et la cybersécurité de ces interfaces.

- Le critère 2.8 désigne comme Impact moyen les *systèmes électroniques BES* qui ont un impact sur les *installations* de *transport* nécessaires pour des installations de production qui respectent les conditions du critère 2.1 (*installations* de production avec une sortie de plus

de 1 500 MW) et 2.3 (*installations* de production généralement désignées comme indispensables à la fiabilité de la zone étendue dans l'horizon de planification). L'entité responsable peut demander une déclaration formelle du propriétaire d'installation de production quant à la qualification des *installations* de production raccordées à ses réseaux de *transport*.

- Le critère 2.9 désigne comme Impact moyen les *systèmes électroniques BES* pour les *automatismes de réseau* (SPS), des *plans de défense* (RAS) ou des systèmes de manoeuvre automatisés pour s'assurer de l'exploitation du BES à l'intérieur des IROL. La dégradation, la compromission ou l'indisponibilité de ces *systèmes électroniques BES* entraînerait le dépassement des IROL s'ils ne fonctionnaient pas tels que conçus. Selon la définition de IROL, la perte ou la compromission de l'un ou l'autre de ceux-ci ont des impacts sur la *zone étendue*.

- Le critère 2.10 désigne comme Impact moyen les *systèmes électroniques BES* pour les systèmes ou *éléments* qui effectuent, sans intervention humaine, un délestage de charge automatique de 300 MW ou plus. Le SDT a passé un temps considérable à discuter de la formulation du critère 2.10, et choisi le mot « chaque » pour indiquer que le critère s'applique à un système ou une *installation* distincte. Dans la rédaction de ce critère, l'équipe de rédaction a cherché à inclure seulement les systèmes qui ne nécessitent pas d'intervention humaine, et a ciblé en particulier les *installations* et les systèmes de délestage de charge en sous-fréquence (DSF) et les systèmes et les *éléments* de délestage de charge en sous-tension (DST) qui seraient visés par une exigence de délestage de charge régionale visant à prévenir un *impact négatif sur la fiabilité*. Ceux-ci comprennent les systèmes automatisés DSF et DST capables de délester 300 MW de charge ou plus. Il est à noter que les systèmes qui ont besoin d'une intervention humaine pour leur armement, mais qui une fois armés se déclenchent automatiquement, doivent être considérés comme ne nécessitant pas d'intervention humaine et devraient être désignés comme Impact moyen. Le seuil de 300 MW a été défini comme la valeur de charge totale en MW la plus élevée, définie selon les normes de délestage de charge régionales pertinentes, pour les 12 mois précédents pour tenir compte des fluctuations saisonnières.

  Ce seuil particulier de 300 MW provient de la version 1 des normes CIP. Le SDT est d'avis que ce seuil doit être inférieur à l'exigence de production de 1 500 MW puisqu'il concerne spécifiquement le DST et le DSF, qui constituent des efforts de dernier recours pour sauver le système de production-transport d'électricité et requièrent donc un seuil plus bas. Un examen des tolérances de DSF définies dans les normes de fiabilité régionales pour les besoins 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 du DSF.

  Dans l'ERCOT, les charges agissant comme des ressources (*Loads Acting as Resources* (LaaR)) du programme de réponse à la demande ne fait pas partie du programme de délestage régional, mais d'un marché de services complémentaires. En général, les programmes de réponse à la demande semblables qui ne font pas partie des programmes

de délestage de charge de fiabilité de la NERC ou régionaux, mais qui sont offerts comme composantes d'un marché de services complémentaires, ne se qualifient pas selon ce critère.

Le langage utilisé dans la section 4 pour les DSF et DST et dans le critère 2.10 de l'annexe 1 est formulé de manière à être cohérent avec les exigences énoncées dans les normes PRC pour les DSF et DST.

- Le critère 2.12 catégorise comme Impact moyen les *systèmes électroniques BES* utilisés par et dans les *centres de contrôle* et les centres informatiques connexes qui s'acquittent des obligations fonctionnelles d'un *exploitant de réseau de transport* et qui n'ont pas déjà été catégorisés comme Impact élevé.

- Le critère 2.13 catégorise comme Impact moyen les *centres de contrôle* de BA qui « contrôlent » une production de 1 500 MW ou plus dans une même *Interconnexion*. Le seuil de 1 500 MW est cohérent avec le degré d'impact et le raisonnement indiqué pour le critère 2.1.

Impact faible (L)

Les *systèmes électroniques BES* non catégorisés comme Impact élevé ou Impact moyen tombent par défaut dans la catégorie Impact faible. Il est à noter que les *systèmes électroniques BES* à impact faible n'ont pas à être identifiés distinctement.

Installations de remise en charge

- Plusieurs discussions sur la version 5 des normes CIP suggèrent que des entités qui possèdent des *ressources à démarrage autonome* et des *chemins de démarrage* pourraient choisir de retirer ces services afin d'éviter des coûts de conformité plus élevés. Par exemple, un *coordonnateur de la fiabilité* a signalé une diminution de 25 % du nombre des *ressources à démarrage autonome* depuis l'entrée en vigueur de la version 1 des normes, et un nombre accru d'entités pourraient décider de faire un tel choix avec la version 5.

  Devant ce constat, l'équipe de rédaction de la version 5 des normes CIP a consulté informellement les comités de planification et d'exploitation de la NERC. Ces comités indiquent avoir déjà constaté une diminution du nombre des *ressources à démarrage autonome* en raison d'une augmentation des coûts de conformité aux CIP, des règles environnementales et d'autres risques ; le fait de les maintenir, dans la version 5, dans une catégorie qui augmenterait substantiellement les coûts de conformité pourrait entraîner un amoindrissement encore plus grand d'un bassin de ressources vulnérable.

  En réponse à ces considérations, l'équipe de rédaction a recatégorisé les actifs de remise en charge, comme les *ressources à démarrage autonome* et les *chemins de démarrage*, les faisant passer de la catégorie Impact moyen (comme c'était le cas dans les premières versions de travail) à la catégorie Impact faible. Cela ne libère pas les propriétaires de ces actifs de toute responsabilité, comme cela aurait été le cas dans les versions 1 à 4 de la

norme CIP-002 (puisque seuls les *actifs électroniques* à connectivité routable qui sont essentiels aux actifs de remise en charge sont inclus dans ces versions). En vertu de la catégorisation Impact faible, ces actifs seront protégés dans les domaines de sensibilisation à la cybersécurité, de contrôle des accès physiques et de contrôle des accès électroniques, et seront soumis à des obligations quant aux interventions en cas d'incident. Il s'agit néanmoins, en fin de compte, d'un gain net pour la fiabilité du BES, puisque beaucoup de ces actifs ne répondent pas aux critères d'inclusion des versions 1 à 4.

En pesant les risques pour la fiabilité générale du BES, l'équipe de rédaction a conclu que cette recatégorisation représente l'option la moins préjudiciable à la fonction de remise en charge, et donc à la fiabilité générale du BES. Le retrait des *ressources à démarrage autonome* et des *chemins de démarrage* de la catégorie Impact moyen est dans l'intérêt de la fiabilité d'ensemble, car autrement on assisterait vraisemblablement à une diminution du nombre des *ressources à démarrage autonome* nécessaires pour une remise en charge rapide en cas de besoin.

Les *systèmes électroniques BES* pour les ressources de production qui ont été désignées comme *ressources à démarrage autonome* dans le plan de remise en charge de l'*exploitant de réseau de transport* tombent par défaut dans la catégorie Impact faible. La norme EOP-005-2 de la NERC stipule que l'*exploitant de réseau de transport* doit avoir un plan de remise en charge, et que ce plan doit préciser la liste de ses *ressources à démarrage autonome* ainsi que les exigences d'essai de ces ressources. Ce critère se limite aux *ressources à démarrage autonome* désignées comme telles dans le plan de remise en charge de l'*exploitant de réseau de transport*. Le terme « plan de capacité de démarrage autonome » a été retiré du Glossaire.

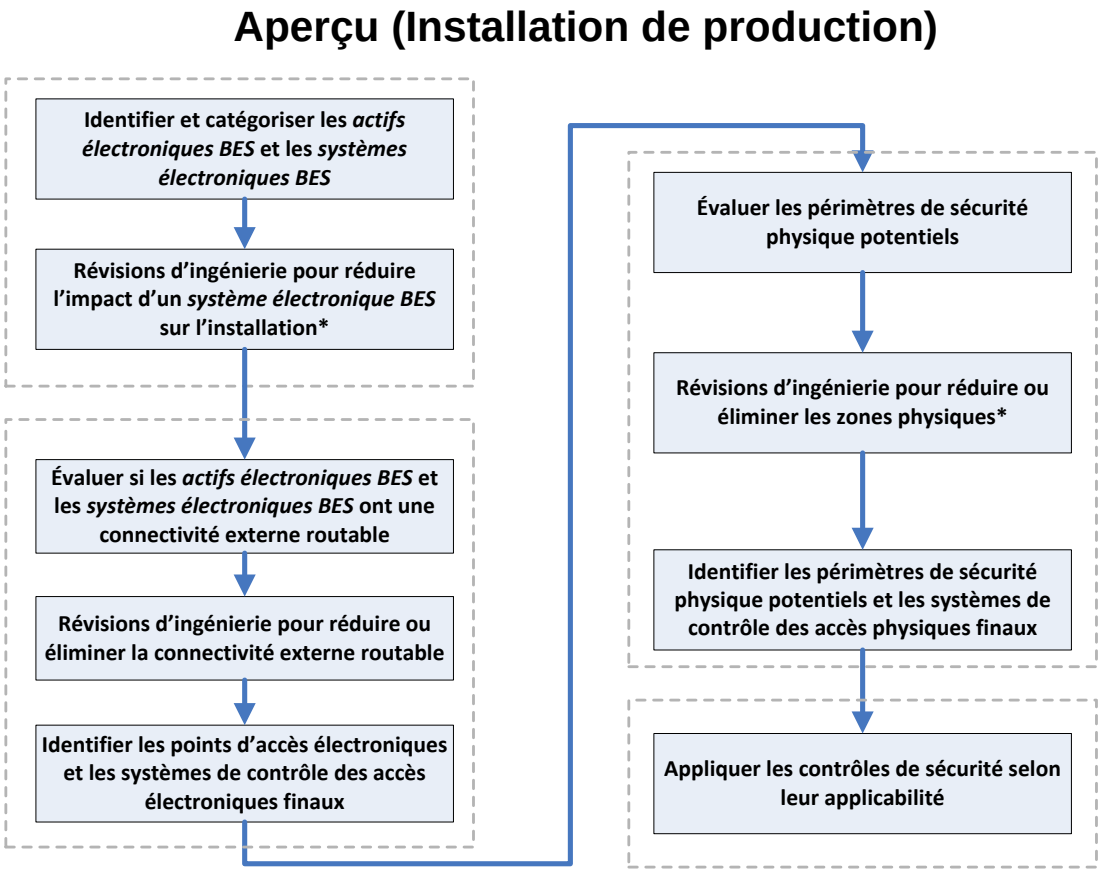
En ce qui concerne la communication aux propriétaires et aux exploitants d'actifs du BES de leur rôle dans le plan de remise en charge, l'*exploitant de réseau de transport* est tenu par la norme EOP-005-2 de la NERC de « fournir aux entités déclarées dans son plan de remise en charge approuvé une description de tout changement apporté à leurs rôles et à leurs tâches particulières avant la date d'entrée en vigueur du plan ».

- Les *systèmes électroniques BES* des *installations* et des *éléments* comprenant les *chemins de démarrage* et respectant les exigences relatives aux manœuvres initiales depuis la *ressource à démarrage autonome* jusqu'au premier point de raccordement du ou des groupes de production à démarrer, indiqués dans le plan de remise en charge de l'*exploitant de réseau de transport*, tombent par défaut dans la catégorie Impact faible ; ces systèmes sont néanmoins désignés explicitement dans la version 5 des normes CIP. Cette exigence d'inclusion à la portée est tirée des exigences de la norme EOP-005-2 de la NERC, qui stipule que l'*exploitant de réseau de transport* doit indiquer dans son plan de remise en charge les *chemins de démarrage* et les exigences concernant les manœuvres initiales depuis la *ressource à démarrage autonome* jusqu'aux groupes de production à démarrer.

  Les *distributeurs* noteront qu'ils ont peut-être des *systèmes électroniques BES* visés par la présente norme s'ils ont des *éléments* indiqués dans le plan de remise en charge de l'*exploitant de réseau de transport* et qui font partie du *chemin de démarrage*.

Cas d'utilisation : déroulement du processus CIP

Le cas suivant de déroulement du processus CIP pour un exploitant ou un propriétaire d'installation de production a été fourni par un participant à l'élaboration de la version 5 des normes et est présenté ici à titre d'exemple d'un processus utilisé pour identifier et catégoriser les *systèmes électroniques BES* et les *actifs électroniques BES* ; à examiner, à élaborer et à mettre en œuvre des stratégies d'atténuation des risques globaux ; et à appliquer les mesures de sécurité pertinentes.



*** - Les révisions d'ingénierie devront être évalués quant à la justification de leur coût, aux exigences opérationnelles et de sécurité, aux besoins de soutien et aux limitations techniques.**

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 :

Les *systèmes électroniques BES* à chaque emplacement ont un impact sur l'exploitation fiable du *système de production-transport d'électricité* qui varie. L'annexe 1 fournit un ensemble de critères précis que l'entité responsable doit utiliser pour identifier ces *systèmes électroniques BES* selon leur impact sur le BES. Les *systèmes électroniques BES* doivent être identifiés et catégorisés selon leur impact, de sorte que les mesures appropriées puissent être appliquées, proportionnellement à leur impact. Ces catégories d'impact constitueront la base de l'application des exigences pertinentes de CIP-003 à CIP-011.

Raisonnement pour E2 :

Les listes exigées par l'exigence E1 sont revues sur une base périodique pour s'assurer que tous les *systèmes électroniques BES* pertinents ont été correctement identifiés et catégorisés. Toute erreur de catégorisation ou non-catégorisation d'un système électronique BES peut entraîner l'adoption de mesures de cybersécurité inadéquates ou l'absence de contrôles de cybersécurité, qui peuvent mener à une compromission ou une mauvaise utilisation susceptible de nuire au fonctionnement en temps réel du BES. L'approbation par le *cadre supérieur CIP* assure une bonne supervision du processus par le personnel approprié de l'entité responsable.

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 « Responsabilité du contrôle de la conformité ».	
3	16 décembre 2009	Changement du numéro de version de -2 à -3. Approbation par le Conseil d'administration de la NERC.	Mise à jour
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	Approbation par le Conseil d'administration de la NERC.	Modifiée en coordination avec les autres normes CIP et révision du format selon le gabarit RBS.

Version	Date	Intervention	Suivi des modifications
5.1	30 septembre 2013	Remplacement de « Devices » par « Systems » dans une définition de la section « Contexte ».	Errata
5.1	22 novembre 2013	Émission d'une ordonnance de la FERC approuvant CIP-002-5.1. (L'ordonnance entre en vigueur le 3 février 2014)	

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

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe aura préséance.

A. Introduction

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

2. **Numéro :** CIP-002-5.1

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

Entités fonctionnelles

Aucune disposition particulière

Installations

La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

- Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur un réseau voisin.
- Postes élévateurs des installations de production identifiées au point précédent.

5. **Date d'entrée en vigueur au Québec :**

5.1. Adoption de la norme par la Régie de l'énergie : xx mois 201x

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

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

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

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

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

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

CIP-002-5.1 — Annexe 1

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

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

A. Introduction

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

2. Numéro : CIP-003-5

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

4. Applicabilité :

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

4.1.1 Responsable de l'équilibrage

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

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

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

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

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

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

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

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

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

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

4.2.1.1 Chaque système de DSF ou de DST qui :

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

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

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

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

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

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

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

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

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

5. Dates d'entrée en vigueur :

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

6. Contexte :

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

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

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

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

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

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

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

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

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

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

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

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

B. Exigences et mesures

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

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

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

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

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

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

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

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

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

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

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

C. Conformité

1. Processus de surveillance de la conformité

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

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

1.2. Conservation des pièces justificatives

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

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

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

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

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

1.4. Autres informations sur la conformité

- Aucune

2. Tableau des éléments de conformité

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	**Planification de l'exploitation**	**Moyen**	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et à impact moyen, mais il n'a pas traité de l'un des neuf thèmes exigés par E1. (E1) OU L'entité responsable n'a pas complété sa revue d'une ou de plusieurs politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et à impact moyen tel que requis par E1 à l'intérieur de 15 mois civils, mais a complété cette revue en au plus	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et à impact moyen, mais il n'a pas traité de deux des neuf thèmes exigés par E1. (E1) OU L'entité responsable n'a pas complété sa revue d'une ou de plusieurs politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et à impact moyen tel que requis par E1 à l'intérieur de 16 mois civils, mais a complété cette revue en au plus	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et à impact moyen, mais il n'a pas traité de trois des neuf thèmes exigés par E1. (E1) OU L'entité responsable n'a pas complété sa revue d'une ou de plusieurs politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et à impact moyen tel que requis par E1 à l'intérieur de 17 mois civils, mais a complété cette revue en au plus	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et à impact moyen, mais il n'a pas traité de quatre ou plus des neuf thèmes exigés par E1. (E1) OU L'entité responsable n'avait aucune politique de cybersécurité documentée pour ses *systèmes électroniques BES* à impact élevé et à impact moyen tel que requis par E1. (E1) OU L'entité responsable n'a pas complété sa

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			16 mois civils suivant la revue précédente. (E1) OU L'entité responsable n'a pas complété son approbation d'une ou de plusieurs politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et à impact moyen tel que requis par E1 par le cadre supérieur CIP ou son délégué, à l'intérieur de 15 mois civils, mais a complété cette approbation en au plus 16 mois civils suivant l'approbation précédente. (E1)	17 mois civils suivant la revue précédente. (E1) OU L'entité responsable n'a pas complété son approbation d'une ou de plusieurs politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et à impact moyen tel que requis par E1 par le cadre supérieur CIP ou son délégué, à l'intérieur de 16 mois civils, mais a complété cette approbation en au plus 17 mois civils suivant l'approbation précédente. (E1)	18 mois civils suivant la revue précédente. (E1) OU L'entité responsable n'a pas complété son approbation d'une ou de plusieurs politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et à impact moyen tel que requis par E1 par le cadre supérieur CIP ou son délégué, à l'intérieur de 17 mois civils, mais a complété cette approbation en au plus 18 mois civils suivant l'approbation précédente. (E1)	revue d'une ou de plusieurs politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et à impact moyen tel que requis par E1 à l'intérieur de 18 mois civils suivant la revue précédente. (E1) OU L'entité responsable n'a pas complété son approbation d'une ou de plusieurs politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et à impact moyen tel que requis par E1 par le cadre supérieur CIP ou son délégué, à l'intérieur de 18 mois civils suivant l'approbation

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						précédente. (E1)
E2	**Planification de l'exploitation**	**Faible**	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour les actifs à degré d'impact faible qui traite de seulement trois des thèmes exigés par E2 et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (E2) OU L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour les actifs à degré d'impact faible qui traite de seulement trois des thèmes exigés par E2, mais n'a pas identifié, évalué ou corrigé les	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour les actifs à degré d'impact faible qui traite de seulement deux des thèmes exigés par E2 et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (E2) OU L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour les actifs à degré d'impact faible qui traite de seulement deux des thèmes exigés par E2, mais n'a pas identifié, évalué ou corrigé les	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour les actifs à degré d'impact faible qui traite de seulement un des thèmes exigés par E2 et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (E2) OU L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour les actifs à degré d'impact faible qui traite de seulement un des thèmes exigés par E2, mais n'a pas identifié, évalué ou corrigé les	L'entité responsable n'a pas documenté ou mis en œuvre une politique de cybersécurité pour les actifs à degré d'impact faible qui traite des thèmes exigés par E2. (E2) OU L'entité responsable n'a pas complété sa revue d'une ou de plusieurs politiques de cybersécurité documentées pour les actifs à degré d'impact faible tel que requis par E2 à l'intérieur de 18 mois civils suivant la revue précédente. OU L'entité responsable n'a pas complété son approbation d'une ou

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			lacunes. OU L'entité responsable n'a pas complété sa revue d'une ou plusieurs politiques de cybersécurité documentées pour les actifs à degré d'impact faible tel que requis par E2 à l'intérieur de 15 mois civils, mais a complété cette revue en au plus 16 mois civils suivant la revue précédente. (E2) OU L'entité responsable n'a pas complété son approbation de une ou plusieurs politiques de cybersécurité documentées pour les actifs à degré d'impact faible tel que requis par E2 par le *cadre*	lacunes. OU L'entité responsable n'a pas complété sa revue d'une ou plusieurs politiques de cybersécurité documentées pour les actifs à degré d'impact faible tel que requis par E2 à l'intérieur de 16 mois civils, mais a complété cette revue en au plus 17 mois civils suivant la revue précédente. (E2) OU L'entité responsable n'a pas complété son approbation de une ou plusieurs politiques de cybersécurité documentées pour les actifs à degré d'impact faible tel que requis par E2 par le *cadre*	lacunes. OU L'entité responsable n'a pas complété sa revue d'une ou plusieurs politiques de cybersécurité documentées pour les actifs à degré d'impact faible tel que requis par E2 à l'intérieur de 17 mois civils, mais a complété cette revue en au plus 18 mois civils suivant la revue précédente. (E2) OU L'entité responsable n'a pas complété son approbation de une ou plusieurs politiques de cybersécurité documentées pour les actifs à degré d'impact faible tel que requis par E2 par le *cadre*	plusieurs politiques de cybersécurité documentées pour les actifs à degré d'impact faible tel que requis par E2 par le *cadre supérieur CIP*, à l'intérieur de 18 mois civils suivant l'approbation précédente. (E2)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			supérieur CIP, à l'intérieur de 15 mois civils, mais a complété cette approbation en au plus 16 mois civils suivant l'approbation précédente. (E2)	*supérieur CIP*, à l'intérieur de 16 mois civils, mais a complété cette approbation en au plus 17 mois civils suivant l'approbation précédente. (E2)	*supérieur CIP*, à l'intérieur de 17 mois civils, mais a complété cette approbation en au plus 18 mois civils suivant l'approbation précédente. (E2)	
E3	**Planification de l'exploitation**	**Moyen**	L'entité responsable a désigné un *cadre supérieur CIP* par nom, mais n'a pas documenté les changements au cadre supérieur CIP à l'intérieur de 30 jours civils, mais a documenté ce changement en moins de 40 jours civils suivant le changement.	L'entité responsable a désigné un *cadre supérieur CIP* par nom, mais n'a pas documenté les changements au cadre supérieur CIP à l'intérieur de 40 jours civils, mais a documenté ce changement en moins de 50 jours civils suivant le changement.	L'entité responsable a désigné un *cadre supérieur CIP* par nom, mais n'a pas documenté les changements au cadre supérieur CIP à l'intérieur de 50 jours civils, mais a documenté ce changement en moins de 60 jours civils suivant le changement.	L'entité responsable n'a pas désigné un *cadre supérieur CIP* par nom. OU L'entité responsable a désigné un *cadre supérieur CIP* par nom, mais n'a pas documenté les changements au cadre supérieur CIP à l'intérieur de 60 jours civils suivant le changement.
E4	**Planification de l'exploitation**	**Faible**	L'entité responsable a désigné un délégué par nom, titre, date de la délégation et actes	L'entité responsable a désigné un délégué par nom, titre, date de la délégation et actes	L'entité responsable a utilisé une autorité déléguée pour les actions permises par	L'entité responsable a utilisé une autorité déléguée pour les actions permises par

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			délégués, mais n'a pas documenté les changements au délégué à l'intérieur de 30 jours civils, mais a documentés ce changement en moins de 40 jours civils suivant le changement. (E4)	délégués, mais n'a pas documenté les changements au délégué à l'intérieur de 40 jours civils, mais a documentés ce changement en moins de 50 jours civils suivant le changement. (E4)	les normes CIP, a un processus pour déléguer les actes du *cadre supérieur CIP*, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (E4) OU L'entité responsable a utilisé une autorité déléguée pour les actions permises par les normes CIP, a un processus pour déléguer les actes du *cadre supérieur CIP*, mais n'a pas identifié, évalué ou corrigé les lacunes. (E4) OU L'entité responsable a désigné un délégué par nom, titre, date de la délégation et actes délégués, mais n'a pas documenté les	les normes CIP, mais n'a pas de processus pour déléguer les actes du *cadre supérieur CIP*. (E4) OU L'entité responsable a désigné un délégué par nom, titre, date de la délégation et actes délégués, mais n'a pas documenté les changements au délégué à l'intérieur de 60 jours civils suivant le changement. (E4)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					changements au délégué à l'intérieur de 50 jours civils, mais a documentés ce changement en moins de 60 jours civils suivant le changement. (E4)	

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 qualifié à la section 4.1, qui est visée par les exigences de la norme. 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

Le nombre de politiques et leur formulation particulière sont guidés par la structure de gestion de l'entité responsable et son contexte opérationnel. Ces politiques peuvent être intégrées à un programme général de protection de l'information pour l'ensemble de l'organisation, ou plutôt à des programmes particuliers. La politique de cybersécurité doit traiter suffisamment en détail des neuf thèmes indiqués dans l'exigence E1 de la norme CIP-003-5. L'entité responsable a le choix d'élaborer une politique de cybersécurité monolithique qui englobe tous ces thèmes, mais elle peut aussi créer une politique parapluie de haut niveau et confier les détails à des documents de niveau inférieur dans la hiérarchie documentaire. Dans le cas d'une politique parapluie de haut niveau, l'entité responsable devrait fournir la politique parapluie ainsi que les documents complémentaires afin de démontrer la conformité à l'exigence E1 de la norme CIP-003-5. La mise en œuvre de la politique de cybersécurité n'est pas traitée explicitement dans l'exigence E1 de la norme CIP-003-5, car on considère qu'elle se manifestera dans la bonne mise en œuvre des normes CIP-004 à CIP-011. Les entités responsables sont toutefois invitées à ne pas limiter la portée de leurs politiques de cybersécurité aux seules exigences des normes CIP-004 à CIP-011, mais plutôt à élaborer une politique de cybersécurité globale appropriée à leur organisation. L'évaluation, dans le cadre du programme de surveillance et de contrôle de conformité, des éléments de la politique qui s'étendent au-delà de la portée des normes CIP-004 à CIP-011 ne doivent pas être considérés comme donnant lieu à des infractions

potentielles. L'entité responsable devrait tenir compte des points suivants pour chacun des thèmes de sa politique de cybersécurité :

1.1 Personnel et formation (CIP-004)

- Position de l'organisation sur ce qui constitue une enquête acceptable sur les antécédents
- Mesures disciplinaires possibles pour les infractions à cette politique
- Gestion des comptes

1.2 *Périmètres de sécurité électronique* (CIP-005), y compris l'*accès distant interactif*

- Position de l'organisation sur l'utilisation des réseaux sans fil
- Désignation des méthodes d'authentification acceptables
- Désignation des ressources fiables et non fiables
- Surveillance et consignation des accès et des sorties aux *points d'accès électroniques*
- Tenue à jour des logiciels antimaliciels avant l'exécution de l'*accès distant interactif*
- Tenue à jour des correctifs pour le système d'exploitation et pour les applications qui exécutent l'*accès distant interactif*
- Désactivation des postes de travail VPN avec séparation des flux (*split tunneling*) ou à double résidence (*dual-homed*) avant l'exécution de l'*accès distant interactif*
- Pour les fournisseurs, les entrepreneurs ou les consultants, le recours à des clauses contractuelles qui exigent le respect des mesures de contrôle d'*accès distant interactif* de l'entité responsable

1.3 Sécurité physique des *systèmes électroniques BES* (CIP-006)

- Stratégie de protection des *actifs électroniques* contre les accès physiques non autorisés
- Méthodes acceptables de contrôle des accès physiques
- Surveillance et consignation des accès physiques

1.4 Gestion de la sécurité des systèmes (CIP-007)

- Stratégies de renforcement des systèmes
- Méthodes acceptables d'authentification et de contrôle d'accès
- Politiques sur les mots de passe comprenant longueur, complexité, mise en application et prévention des attaques exhaustives
- Surveillance et consignation des activités des *systèmes électroniques BES*

1.5 Déclaration des incidents et planification des mesures d'intervention (CIP-008)

- Détection des incidents de cybersécurité
- Notifications appropriées en cas de découverte d'un incident

- Obligations de signaler les *incidents de cybersécurité*

1.6 Plans de rétablissement des *systèmes électroniques BES* (CIP-009)

- Disponibilité des composants de rechange
- Disponibilité des sauvegardes système

1.7 Gestion des changements de configuration et analyses de vulnérabilité (CIP-010)

- Demandes de changement
- Approbation des changements
- Processus de réparation

1.8 Protection de l'information (CIP-011)

- Méthodes de contrôle d'accès à l'information
- Notification des divulgations non autorisées
- Accès à l'information selon le principe du besoin de savoir

1.9 Déclaration des *circonstances CIP exceptionnelles* et mesures d'intervention

- Processus de recours à des procédures spéciales en cas de circonstance CIP exceptionnelle
- Processus de tolérance des dérogations qui n'enfreignent pas les exigences CIP

L'équipe de rédaction des normes (SDT) a retiré les exigences relatives aux dérogations aux politiques de sécurité d'une entité responsable puisqu'il s'agit d'un enjeu de gestion générale qui ne relève pas des exigences de fiabilité. Le SDT considère qu'il s'agit d'une exigence de politique interne et non d'une exigence de fiabilité. Cependant, le SDT invite les entités responsables à maintenir cette pratique dans le cadre de sa politique de cybersécurité.

Dans le cas présent, et pour toutes les approbations subséquentes exigées par les normes CIP de la NERC, l'entité responsable est libre d'utiliser des approbations en version papier ou électronique, pourvu que la preuve soit suffisante pour garantir l'authenticité de l'approbateur.

Exigence E2

Comme pour l'exigence E1, le nombre de politiques et leur formulation particulière doivent être guidés par la structure de gestion de l'entité responsable et son contexte opérationnel. Ces politiques peuvent être intégrées à un programme général de protection de l'information pour l'ensemble de l'organisation, ou encore à des programmes particuliers. La politique de cybersécurité doit traiter suffisamment en détail des quatre thèmes indiqués dans l'exigence E2 de la norme CIP-003-5. L'entité responsable a le choix d'élaborer une politique de cybersécurité monolithique qui englobe tous ces thèmes, mais elle peut aussi créer une politique parapluie de haut niveau et confier les détails à des documents de niveau inférieur dans la hiérarchie documentaire. Dans le cas d'une politique parapluie de haut niveau, l'entité responsable devrait fournir la politique parapluie ainsi que les documents complémentaires afin de démontrer la conformité à l'exigence E2 de la norme CIP-003-5. L'exigence vise à définir un

ensemble de protections de base à appliquer à tous les *systèmes électroniques BES* à impact faible, sans leur imposer un fardeau administratif et de conformité indu. Le SDT considère que la conformité à cette exigence peut être démontrée raisonnablement par des preuves attestant des processus, des procédures ou des plans appropriés. Bien que le personnel d'audit puisse choisir d'examiner un échantillon de *système électronique BES* à impact faible, le SDT est convaincu que la méthode actuelle (au moment d'écrire ces lignes) consistant à examiner un échantillon statistique de système n'est pas nécessaire. Le SDT souligne par ailleurs que dans le thème 2.3, le SDT utilise le terme « contrôle des accès électroniques » est employé dans son sens général, soit celui de contrôle passif des accès, et non dans le sens technique particulier qui évoque la mise en œuvre de mécanismes d'authentification, d'autorisation et d'audit.

Exigence E3

L'esprit de l'exigence E3 de la norme CIP-003-5 reste pratiquement inchangé par rapport aux versions antérieures de la norme. La description spécifique du *cadre supérieur CIP* est maintenant comprise dans les termes définis, ce qui évite de l'expliciter dans le texte de la norme et de devoir créer des renvois à la norme dans d'autres documents. Le *cadre supérieur CIP* est appelé à jouer un rôle clé pour assurer la planification stratégique appropriée, la sensibilisation des dirigeants et du conseil d'administration et la gouvernance générale du programme.

Exigence E4

Comme l'indique le raisonnement pour l'exigence E4 de la norme CIP-003-5, cette exigence vise à démontrer une chaîne d'autorité et d'imputabilité claire en matière de sécurité. L'intention du SDT était de ne pas imposer une structure organisationnelle particulière ; elle laisse plutôt à l'entité responsable une ample marge de manœuvre pour adapter cette exigence à sa structure organisationnelle existante. Une entité responsable peut satisfaire à cette exigence au moyen d'un seul ou de plusieurs documents de délégation. L'entité responsable peut aussi déléguer les pouvoirs de délégation eux-mêmes pour augmenter la souplesse de mise en œuvre dans son organisation. Dans un tel cas, les délégations peuvent être dispersées dans de multiples documents, pourvu que l'ensemble de ces documents décrive une chaîne d'autorité claire qui remonte au *cadre supérieur CIP*. De plus, le *cadre supérieur CIP* pourrait aussi choisir de ne déléguer aucun pouvoir et de respecter cette exigence sans recourir à des documents de délégation.

L'entité responsable doit tenir à jour la documentation relative au *cadre supérieur CIP* et à ses délégations, afin d'éviter que des individus n'exercent des pouvoirs non documentés. Cependant, il n'est pas nécessaire de réaffirmer les délégations si le délégant change de poste ou est remplacé. Par exemple, supposons que Pierre Untel soit désigné comme *cadre supérieur CIP* et qu'il délègue une tâche au directeur de la maintenance des postes électriques. Si Pierre Untel est remplacé comme *cadre supérieur CIP*, la documentation du *cadre supérieur CIP* doit être mise à jour dans le délai prescrit, mais la délégation existante au directeur de la maintenance des postes électriques reste en vigueur telle qu'elle a été approuvée par le *cadre supérieur CIP* précédent, Pierre Untel.

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 :

Une ou plusieurs politiques de sécurité assurent une mise en œuvre efficace des exigences de la norme. Ces politiques visent à constituer les bases de la gestion et de la gouvernance pour toutes les exigences applicables au personnel auquel est accordé un accès électronique autorisé ou un accès physique autorisé sans accompagnement aux *systèmes électroniques BES*. L'entité responsable peut démontrer par ses politiques que ses dirigeants appuient les mesures d'imputabilité et de responsabilisation nécessaires pour une mise en œuvre efficace des exigences de la norme.

Le réexamen et l'approbation annuels de la politique de cybersécurité assurent la tenue à jour de cette politique et réaffirment périodiquement l'engagement des dirigeants envers la protection de ses *systèmes électroniques BES*.

Raisonnement pour E2 :

Une ou plusieurs politiques de sécurité assurent une mise en œuvre efficace des exigences de la norme. Ces politiques visent à constituer les bases de la gestion et de la gouvernance pour toutes les exigences applicables au personnel auquel est accordé un accès électronique autorisé ou un accès physique autorisé sans accompagnement aux *systèmes électroniques BES*. L'entité responsable peut démontrer par ses politiques que ses dirigeants appuient les mesures d'imputabilité et de responsabilisation nécessaires pour une mise en œuvre efficace des exigences de la norme.

À l'alinéa 2.3, la mention « pour les connexions externes à protocole routable et la *connectivité par ligne commutée* » réaffirme l'intention, exprimée dans l'ordonnance 761 de la FERC, paragraphe 87, que des protections de périmètre de sécurité électronique « sous une forme quelconque » soient appliquées à tous les *systèmes électroniques BES*, quel que soit leur degré d'impact. L'alinéa 2.3 utilise l'expression « connexions externes à protocole routable » plutôt que le terme défini « *connectivité externe routable* », celui-ci ayant des connotations très précises en rapport avec les *périmètres de sécurité électronique* et les *systèmes électroniques BES* à impact élevé ou moyen. L'emploi du terme défini « *connectivité externe routable* » dans le contexte de l'exigence E2 serait inapproprié, car la portée de l'exigence E2 est limitée aux *systèmes électroniques BES* à impact faible.

Le réexamen et l'approbation de la politique de cybersécurité au moins tous les 15 mois civils assurent la tenue à jour de cette politique et réaffirment périodiquement l'engagement des dirigeants envers la protection de ses *systèmes électroniques BES*.

Raisonnement pour E3 :

La désignation du *cadre supérieur CIP* et sa documentation assurent une autorité et une imputabilité claires pour le programme CIP dans l'organisation, en réponse à la recommandation 43 du rapport sur la panne de courant de 2003. La description des responsabilités du *cadre supérieur CIP* figure au Glossaire des termes utilisés dans les normes de fiabilité de la NERC, de telle sorte que ce terme peut être utilisé dans l'ensemble des normes CIP sans renvoi explicite.

L'ordonnance 706 de la FERC, paragraphe 296, pose la question de savoir si le cadre supérieur désigné devrait être un dirigeant de la société ou l'équivalent. Comme l'indique la définition du terme, le *cadre supérieur CIP* est « investi d'une autorité et d'une responsabilité étendues afin de mener et de gérer la mise en œuvre des normes », ce qui assure que le cadre supérieur détient une autorité suffisante au sein de l'entité responsable pour que la cybersécurité reçoive toute l'attention nécessaire. En outre, étant donné la variété des modèles de gestion des entités responsables (entités municipales, coopératives, organismes fédéraux, entreprises privées d'utilité publique et autres entités intermédiaires), le SDT est d'avis que l'exigence que le cadre supérieur soit « un dirigeant de la société ou l'équivalent » serait extrêmement difficile à interpréter et à mettre en application de manière homogène.

Raisonnement pour E4 :

Cette exigence vise à assurer une imputabilité claire au sein de l'organisation pour certains points relatifs à la sécurité. Elle fait aussi en sorte que les délégations soient tenues à jour et que nul n'exerce de pouvoirs sans délégation documentée.

Dans son ordonnance 706, paragraphes 379 et 381, la FERC indique que la recommandation 43 du rapport sur la panne de courant de 2003 réclame « des chaînes d'autorité et d'imputabilité claires en matière de sécurité ». C'est ce qui a amené le SDT à clarifier l'exigence en matière de délégation, de manière que la chaîne d'autorité en question soit claire et que les délégations de pouvoir soient dûment documentées.

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 « Responsable 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	24 janvier 2011	Approbation par le Conseil d'administration de la NERC.	Mise à jour en fonction des changements apportés à la norme CIP-002-4 (projet 2008-06)
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-003-5. (L'ordonnance entre en vigueur le 3 février 2014.)	

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

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe aura préséance.

A. Introduction

1. **Titre :** Cybersécurité — Mécanismes de gestion de la sécurité

2. **Numéro :** CIP-003-5

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

Entités fonctionnelles

Aucune disposition particulière

Installations

La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

- Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur un réseau voisin.
- Postes élévateurs des installations de production identifiées au point précédent.

5. **Date d'entrée en vigueur au Québec :**

5.1. Adoption de la norme par la Régie de l'énergie : xx mois 201x

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

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

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

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

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

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

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

A. Introduction

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

2. **Numéro :** CIP-004-5.1

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

4. **Applicabilité :**

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

   4.1.1. Responsable de l'équilibrage

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

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

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

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

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

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

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

   4.1.3. Exploitant d'installation de production

   4.1.4. Propriétaire d'installation de production

4.1.5. Coordonnateur des échanges ou Responsable des échanges

4.1.6. Coordonnateur de la fiabilité

4.1.7. Exploitant de réseau de transport

4.1.8. Propriétaire d'installation de transport

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

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

4.2.1.1. Chaque système de DSF ou de DST qui :

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

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

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

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

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

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

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

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

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

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

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

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

5. Dates d'entrée en vigueur :

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

6. Contexte :

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

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

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

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

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

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

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

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

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

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

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

Colonne « Systèmes visés » des tableaux

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

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

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

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

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

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

B. Exigences et mesures

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Conformité

1. Processus de surveillance de la conformité

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

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

1.2. Conservation des pièces justificatives

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

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

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

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

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

1.4. Autres informations sur la conformité

- Aucune

2. Tableau des éléments de conformité

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	**Planification de l'exploitation**	**Faible**	L'entité responsable n'a pas rappelé les pratiques de cybersécurité au cours d'un trimestre civil, mais l'a fait en moins de 10 jours civils après le début d'un trimestre calendrier subséquent. (1.1)	L'entité responsable n'a pas rappelé les pratiques de cybersécurité au cours d'un trimestre civil, mais l'a fait entre 10 et 30 jours civils après le début d'un trimestre calendrier subséquent. (1.1)	L'entité responsable n'a pas rappelé les pratiques de cybersécurité au cours d'un trimestre civil, mais l'a fait à l'intérieur du trimestre subséquent, mais plus de 30 jours suivant le début de ce trimestre civil. (1.1)	L'entité responsable n'a pas documenté ou mis en œuvre un processus de sensibilisation à la sécurité pour rappeler les pratiques de cybersécurité. (E1) OU L'entité responsable n'a pas rappelé les pratiques de cybersécurité et les pratiques de sécurité physique associées pour au moins deux trimestres civils. (1.1)
E2	**Planification de l'exploitation**	**Faible**	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas inclus un des thèmes de formation dans les parties 2.1.1 à 2.1.9 de l'exigence, et	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas inclus deux des thèmes de formation dans les parties 2.1.1 à 2.1.9 de l'exigence, et	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas inclus trois des thèmes de formation dans les parties 2.1.1 à 2.1.9 de l'exigence, et	L'entité responsable n'a pas mis en œuvre un programme de formation sur la cybersécurité axé sur les rôles, les fonctions ou les responsabilités de chacun. (E2)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			n'a pas identifié, évalué et corrigé les lacunes. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas formé une personne (à l'exception des *circonstances CIP exceptionnelles*) avant de lui accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement, et n'a pas identifié, évalué et corrigé les lacunes. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a	n'a pas identifié, évalué et corrigé les lacunes. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas formé deux personnes (à l'exception des *circonstances CIP exceptionnelles*) avant de leur accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement, et n'a pas identifié, évalué et corrigé les lacunes. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la	n'a pas identifié, évalué et corrigé les lacunes. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas formé trois personnes (à l'exception des *circonstances CIP exceptionnelles*) avant de leur accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement, et n'a pas identifié, évalué et corrigé les lacunes. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la	OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas inclus quatre ou plus des thèmes de formation dans les parties 2.1.1 à 2.1.9 de l'exigence, et n'a pas identifié, évalué et corrigé les lacunes. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas formé quatre personnes ou plus (à l'exception des *circonstances CIP exceptionnelles*) avant de leur accorder un accès électronique

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			pas formé une personne avec un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans les 15 mois civils suivant la date de complétion de la formation précédente, et n'a pas identifié, évalué et corrigé les lacunes. (2.3)	cybersécurité, mais n'a pas formé deux personnes avec un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans les 15 mois civils suivant la date de complétion de la formation précédente, et n'a pas identifié, évalué et corrigé les lacunes. (2.3)	cybersécurité, mais n'a pas formé trois personnes avec un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans les 15 mois civils suivant la date de complétion de la formation précédente, et n'a pas identifié, évalué et corrigé les lacunes. (2.3)	autorisé ou un accès physique autorisé sans accompagnement, et n'a pas identifié, évalué et corrigé les lacunes. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais n'a pas formé quatre personnes ou plus avec un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans les 15 mois civils suivant la date de complétion de la formation précédente, et n'a pas identifié, évalué et corrigé les lacunes. (2.3)
E3	**Planification de**	**Moyen**	L'entité responsable a un programme	L'entité responsable a un programme	L'entité responsable a un programme	L'entité responsable n'a pas inclus tous les

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
	l'exploitation		d'évaluation des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et fournisseurs de service, mais n'a pas effectué la PRA comme condition pour accorder l'accès électronique autorisé ou un accès physique autorisé sans accompagnement pour une personne, et n'a pas identifié, évalué et corrigé les lacunes. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique	d'évaluation des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et fournisseurs de service, mais n'a pas effectué la PRA comme condition pour accorder l'accès électronique autorisé ou un accès physique autorisé sans accompagnement pour deux personnes, et n'a pas identifié, évalué et corrigé les lacunes. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique	d'évaluation des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et fournisseurs de service, mais n'a pas effectué la PRA comme condition pour accorder l'accès électronique autorisé ou un accès physique autorisé sans accompagnement pour trois personnes, et n'a pas identifié, évalué et corrigé les lacunes. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique	éléments requis comme indiqué en 3.1 à 3.4 dans les programmes documentés d'évaluation des risques liés au personnel (PRA), pour les personnes, incluant les contractuels et les fournisseurs de service, pour l'obtention et la maintenance des accès électroniques autorisés ou des accès physiques autorisés sans accompagnement. (E3) OU L'entité responsable a un programme d'évaluation des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et fournisseurs de service, mais n'a pas effectué la PRA comme condition

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			autorisé sans accompagnement, mais n'a pas confirmé l'identité d'une personne, et n'a pas identifié, évalué et corrigé les lacunes. (3.1 et 3.4) OU L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas inclus les vérifications exigées indiquées en 3.2.1 et 3.2.2 pour un personne, et n'a pas	autorisé sans accompagnement, mais n'a pas confirmé l'identité de deux personnes, et n'a pas identifié, évalué et corrigé les lacunes. (3.1 et 3.4) OU L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas inclus les vérifications exigées indiquées en 3.2.1 et 3.2.2 pour deux personnes, et n'a pas	autorisé sans accompagnement, mais n'a pas confirmé l'identité de trois personnes, et n'a pas identifié, évalué et corrigé les lacunes. (3.1 et 3.4) OU L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas inclus les vérifications exigées indiquées en 3.2.1 et 3.2.2 pour trois personnes, et n'a pas	pour accorder l'accès électronique autorisé ou un accès physique autorisé sans accompagnement pour quatre personnes ou plus, et n'a pas identifié, évalué et corrigé les lacunes. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas confirmé l'identité de quatre personnes ou plus, et n'a pas identifié, évalué et corrigé les

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			identifié, évalué et corrigé les lacunes. (3.2 et 3.4) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas évalué la vérification des antécédents judiciaires pour l'autorisation d'accès pour une personne, et n'a pas identifié, évalué et corrigé les lacunes. (3.3 et 3.4) OU	identifié, évalué et corrigé les lacunes. (3.2 et 3.4) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas évalué la vérification des antécédents judiciaires pour l'autorisation d'accès pour deux personnes, et n'a pas identifié, évalué et corrigé les lacunes. (3.3 et 3.4) OU	identifié, évalué et corrigé les lacunes. (3.2 et 3.4) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas évalué la vérification des antécédents judiciaires pour l'autorisation d'accès pour trois personnes, et n'a pas identifié, évalué et corrigé les lacunes. (3.3 et 3.4) OU	lacunes. (3.1 et 3.4) OU L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas inclus les vérifications exigées indiquées en 3.2.1 et 3.2.2 pour quatre personnes ou plus, et n'a pas identifié, évalué et corrigé les lacunes. (3.2 et 3.4) OU L'entité responsable a effectué des

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			L'entité responsable n'a pas effectué des évaluations des risques liés au personnel (PRA) pour une personne avec un accès électronique autorisé ou un accès physique autorisé sans accompagnement à l'intérieur de 7 années civiles de la date de complétion de la PRA précédente, et n'a pas identifié, évalué et corrigé les lacunes. (3.5)	L'entité responsable n'a pas effectué des évaluations des risques liés au personnel (PRA) pour deux personnes avec un accès électronique autorisé ou un accès physique autorisé sans accompagnement à l'intérieur de 7 années civiles de la date de complétion de la PRA précédente, et n'a pas identifié, évalué et corrigé les lacunes. (3.5)	L'entité responsable n'a pas effectué des évaluations des risques liés au personnel (PRA) pour trois personnes avec un accès électronique autorisé ou un accès physique autorisé sans accompagnement à l'intérieur de 7 années civiles de la date de complétion de la PRA précédente, et n'a pas identifié, évalué et corrigé les lacunes. (3.5)	évaluations des risques liés au personnel (PRA) pour les personnes, incluant les contractuels et les fournisseurs de service, avec accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais n'a pas évalué la vérification des antécédents judiciaires pour l'autorisation d'accès pour quatre personnes ou plus, et n'a pas identifié, évalué et corrigé les lacunes. (3.3 et 3.4) OU L'entité responsable n'a pas effectué des évaluations des risques liés au personnel (PRA) pour quatre personnes ou plus avec un accès électronique autorisé

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						ou un accès physique autorisé sans accompagnement à l'intérieur de 7 années civiles de la date de complétion de la PRA précédente, et n'a pas identifié, évalué et corrigé les lacunes. (3.5)
E4	**Planification de l'exploitation et exploitation du jour même**	**Moyen**	L'entité responsable n'a pas vérifié que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur ont des registres d'autorisation pendant un trimestre civil, mais l'a fait moins de 10 jours civils après le début d'un trimestre civil subséquent, et n'a pas identifié, évalué et corrigé les lacunes. (4.2) OU	L'entité responsable n'a pas vérifié que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur ont des registres d'autorisation pendant un trimestre civil, mais l'a fait entre 10 et 20 jours civils après le début d'un trimestre civil subséquent, et n'a pas identifié, évalué et corrigé les lacunes. (4.2)	L'entité responsable n'a pas vérifié que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur ont des registres d'autorisation pendant un trimestre civil, mais l'a fait entre 20 et 30 jours civils après le début d'un trimestre civil subséquent, et n'a pas identifié, évalué et corrigé les lacunes. (4.2)	L'entité responsable n'a pas mis en œuvre un programme documenté pour la gestion des accès. (E4) OU L'entité responsable a mis en œuvre un ou plusieurs programmes documentés pour la gestion des accès qui comprennent un processus pour autoriser l'accès électronique, l'accès physique sans accompagnement, ou

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			L'entité responsable a mis en œuvre des processus pour vérifier que les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont corrects et nécessaires, dans les 15 mois civils suivant la vérification précédente, mais pour 5 % ou moins de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.3) OU L'entité responsable a mis en œuvre des processus pour vérifier que l'accès aux emplacements de	OU L'entité responsable a mis en œuvre des processus pour vérifier que les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont corrects et nécessaires, dans les 15 mois civils suivant la vérification précédente, mais pour plus de 5 % et moins de (ou égal à) 10 % de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.3) OU L'entité responsable a	OU L'entité responsable a mis en œuvre des processus pour vérifier que les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont corrects et nécessaires, dans les 15 mois civils suivant la vérification précédente, mais pour plus de 10 % et moins de (ou égal à) 15 % de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.3) OU L'entité responsable a	l'accès aux emplacements de stockage désignés où est située l'information de *système électronique BES*, et n'a pas identifié, évalué et corrigé les lacunes. (4.1) OU L'entité responsable n'a pas vérifié que les personnes ayant un accès électronique ou un accès physique sans accompagnement en vigueur ont des registres d'autorisation pendant deux trimestres civils consécutifs ou plus, et n'a pas identifié, évalué et corrigé les lacunes. (4.2) OU L'entité responsable a mis en œuvre des

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			stockage pour l'information de *système électronique BES* est correct et nécessaire, dans les 15 mois civils suivant la vérification précédente, mais pour 5 % ou moins de ses emplacements de stockage de l'information de *système électronique BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.4)	mis en œuvre des processus pour vérifier que l'accès aux emplacements de stockage pour l'information de *système électronique BES* est correct et nécessaire, dans les 15 mois civils suivant la vérification précédente, mais pour plus de 5 % et moins de (ou égal à) 10 % de ses emplacements de stockage de l'information de *système électronique BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.4)	mis en œuvre des processus pour vérifier que l'accès aux emplacements de stockage pour l'information de *système électronique BES* est correct et nécessaire, dans les 15 mois civils suivant la vérification précédente, mais pour plus de 10 % et moins de (ou égal à) 15 % de ses emplacements de stockage de l'information de *système électronique BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.4)	processus pour vérifier que les comptes utilisateurs, groupes de comptes utilisateurs ou catégories de rôles d'utilisateur, ainsi que leurs droits d'accès respectifs, sont corrects et nécessaires, dans les 15 mois civils suivant la vérification précédente, mais pour plus de 15 % de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.3) OU L'entité responsable a mis en œuvre des processus pour vérifier que l'accès aux emplacements de stockage pour l'information de

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						système électronique BES est correct et nécessaire, dans les 15 mois civils suivant la vérification précédente, mais pour 15 % ou plus de ses emplacements de stockage de l'information de *système électronique BES*, les droits d'accès étaient incorrects ou non nécessaires, et n'a pas identifié, évalué et corrigé les lacunes. (4.4)
E5	**Exploitation du jour même et planification de l'exploitation**	**Moyen**	L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès de la personne aux emplacements de stockage désignés pour l'information de système électronique BES, mais pour une personne, ne l'a pas	L'entité responsable a mis en œuvre un ou plusieurs processus pour retirer la capacité d'accès physique sans accompagnement et d'*accès distant interactif* lors d'un départ ou pour compléter le retrait dans les 24 heures du	L'entité responsable a mis en œuvre un ou plusieurs processus pour retirer la capacité d'accès physique sans accompagnement et d'*accès distant interactif* lors d'un départ ou pour compléter le retrait dans les 24 heures du	L'entité responsable n'a mis en œuvre aucun programme documenté pour la révocation des accès pour les accès électroniques, les accès physiques sans accompagnement, ou pour les emplacements de stockage des

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			fait avant la fin du jour civil suivant la date et l'heure à laquelle prend effet le départ, et n'a pas identifié, évalué et corrigé les lacunes. (5.3) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès de la personne aux comptes utilisateurs lors du départ, mais ne l'a pas fait dans les 30 jours civils suivant la date du départ pour une personne ou plus, et n'a pas identifié, évalué et corrigé les lacunes. (5.4) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour changer les mots	départ, mais n'a pas déclenché ces retraits pour une personne, et n'a pas identifié, évalué et corrigé les lacunes. (5.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer qu'une personne n'a plus besoin de conserver les accès à la suite d'une réaffectation ou d'une mutation, mais, pour une personne, n'a pas révoqué les accès électroniques autorisés aux comptes de la personne et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée, et n'a pas identifié, évalué et	départ, mais n'a pas déclenché ces retraits pour deux personnes, et n'a pas identifié, évalué et corrigé les lacunes. (5.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer qu'une personne n'a plus besoin de conserver les accès à la suite d'une réaffectation ou d'une mutation, mais, pour deux personnes, n'a pas révoqué les accès électroniques autorisés aux comptes de la personne et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée, et n'a pas identifié, évalué et	informations de *système électronique BES*. (E5) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour retirer la capacité d'accès physique sans accompagnement et d'*accès distant interactif* lors d'un départ ou pour compléter le retrait dans les 24 heures du départ, mais n'a pas déclenché ces retraits pour trois personnes ou plus, et n'a pas identifié, évalué et corrigé les lacunes. (5.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			de passe pour les comptes partagés connus de l'utilisateur lors du départ, de la réaffectation ou de la mutation, mais ne l'a pas fait dans les 30 jours civils suivant la date du départ, de la réaffectation ou de la mutation pour une personne ou plus, et n'a pas identifié, évalué et corrigé les lacunes. (5.5) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer et documenter les circonstances opérationnelles atténuantes suivant un départ, une réaffectation ou une mutation, mais n'a pas changé un ou plusieurs	corrigé les lacunes. (5.2) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès de la personne aux emplacements de stockage désignés pour l'information de système électronique BES, mais pour deux personnes, ne l'a pas fait avant la fin du jour civil suivant la date et l'heure à laquelle prend effet le départ, et n'a pas identifié, évalué et corrigé les lacunes. (5.3)	corrigé les lacunes. (5.2) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès de la personne aux emplacements de stockage désignés pour l'information de système électronique BES, mais pour trois personnes ou plus, ne l'a pas fait avant la fin du jour civil suivant la date et l'heure à laquelle prend effet le départ, et n'a pas identifié, évalué et corrigé les lacunes. (5.3)	qu'une personne n'a plus besoin de conserver les accès à la suite d'une réaffectation ou d'une mutation, mais, pour trois personnes ou plus, n'a pas révoqué les accès électroniques autorisés aux comptes de la personne et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée, et n'a pas identifié, évalué et corrigé les lacunes. (5.2)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-5.1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			mots de passe pour des comptes partagés connus de l'utilisateur dans les 10 jours civils suivant la fin des circonstances opérationnelles atténuantes, et n'a pas identifié, évalué et corrigé les lacunes. (5.5)			

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 :

Le programme de sensibilisation à la sécurité se veut un programme informatif et non un programme de formation officiel. Il devrait rappeler les pratiques de sécurité afin de tenir le personnel au courant des pratiques recommandées en matière de sécurité physique et électronique pour protéger les *systèmes électroniques BES*. L'entité responsable n'est pas tenue de fournir des documents qui attestent que chaque personne a reçu ou compris l'information, mais elle doit conserver en tout temps le matériel du programme utilisé, sous forme d'affiches, de notes de service ou de présentations.

Voici des exemples de mécanismes ou preuves de sensibilisation qu'on peut utiliser s'ils sont datés :

- communications ciblées (p. ex., courriels, notes de service, formation en ligne, etc.) ;
- communications générales (p. ex., affiches, intranet, brochures, etc.) ;
- rappels et soutien de la direction (p. ex., présentations, réunions, etc.).

Exigence E2 :

La formation doit porter sur les politiques, les contrôles d'accès et les procédures établis pour les *systèmes électroniques BES*, et inclure, au moins, les éléments nécessaires en fonction des rôles et responsabilités de chacun, selon le tableau E2. L'entité responsable a la liberté de définir son propre programme de formation, qui peut se composer de plusieurs modules et modes de prestation, mais un seul programme de formation pour toutes les personnes devant être formées est aussi acceptable. L'entité responsable peut, à sa guise, axer la formation sur les fonctions, les rôles ou les responsabilités.

L'ordonnance 706 de la FERC, paragraphe 434, intègre à la formation un nouvel élément qui concerne le matériel et les logiciels de mise en réseau ainsi que les autres éléments d'interconnectabilité électronique nécessaires à l'exploitation et au contrôle des *systèmes électroniques BES*. Cet élément n'exige pas que l'on donne une formation technique aux personnes responsables du matériel et des logiciels de mise en réseau, mais plutôt que l'on informe les utilisateurs de systèmes des risques posés à la cybersécurité par l'interconnectabilité de ces systèmes. Selon leurs fonctions, rôles ou responsabilités, les utilisateurs doivent avoir une connaissance de base des systèmes auxquels ils peuvent accéder à partir d'autres systèmes et des incidences de leurs actions sur la cybersécurité.

Chaque entité responsable doit s'assurer que tous les membres du personnel auxquels un accès électronique autorisé ou un accès physique autorisé sans accompagnement est accordé à ses *systèmes électroniques BES*, y compris les entrepreneurs et les fournisseurs de services, suivent une formation sur la cybersécurité avant de se voir accorder cet accès autorisé, sauf dans des *circonstances CIP exceptionnelles*. Pour conserver leur accès autorisé, les personnes doivent suivre la formation au moins une fois tous les 15 mois.

Exigence E3 :

Chaque entité responsable doit s'assurer qu'une évaluation des risques liés au personnel est menée pour tout le personnel auquel est accordé un accès électronique autorisé ou un accès physique autorisé sans accompagnement à ses *systèmes électroniques BES*, y compris les entrepreneurs et les fournisseurs de services, avant que leur soit accordé cet accès, exception faite des circonstances exceptionnelles qui ont une incidence sur la fiabilité du BES ou l'intervention d'urgence, qui sont précisées au programme et approuvées par le cadre supérieur désigné ou son délégué. Le contrôle de l'identité doit être réalisé en respectant les lois fédérales et provinciales et les ententes syndicales en vigueur. Ce contrôle n'est nécessaire qu'avant le premier accès à accorder, mais peut être répété périodiquement durant la période d'emploi, selon le processus suivi par l'entité, à l'identique ou d'une autre façon.

Une vérification des antécédents judiciaires sur les sept années précédentes doit être effectuée en tenant compte des endroits où a résidé la personne pendant au moins six mois consécutifs. Cette vérification doit aussi être effectuée en respect des lois fédérales, d'états, provinciales et locales, et est sujette aux conventions collectives en vigueur. S'il est impossible de mener une vérification complète des antécédents judiciaires sur les sept années précédentes, la portion qui a pu être vérifiée doit être documentée ainsi que les motifs pour lesquels la vérification complète sur cette période n'a pu se faire. Il peut s'agir, par exemple, de personnes âgées de moins de 25 ans dont les antécédents à titre de jeune contrevenant sont protégés en vertu de la loi, de personnes qui ont résidé à des endroits où il est impossible d'obtenir de vérifications des antécédents judiciaires ou des personnes dont l'emploi est régi par une convention collective qui l'interdit. Dans de tels cas, l'entité responsable doit tenir compte du fait que les renseignements sont incomplets lorsqu'elle évalue le risque d'accorder un accès. Chaque personne ayant un accès doit avoir fait l'objet d'une évaluation des risques liés au personnel au cours des sept années précédentes. Une nouvelle vérification des antécédents judiciaires doit être menée dans le cadre de cette nouvelle évaluation des risques. Les personnes auxquelles on a accordé un accès en vertu d'une version antérieure des présentes normes doivent faire l'objet d'une nouvelle évaluation des risques liés au personnel dans les sept ans suivant leur évaluation précédente. Dans la présente version de la norme, le processus de vérification des antécédents judiciaires sur les sept années précédentes a été clarifié de sorte qu'il ne soit pas nécessaire de mener une nouvelle évaluation des risques liés au personnel avant la date de mise en œuvre.

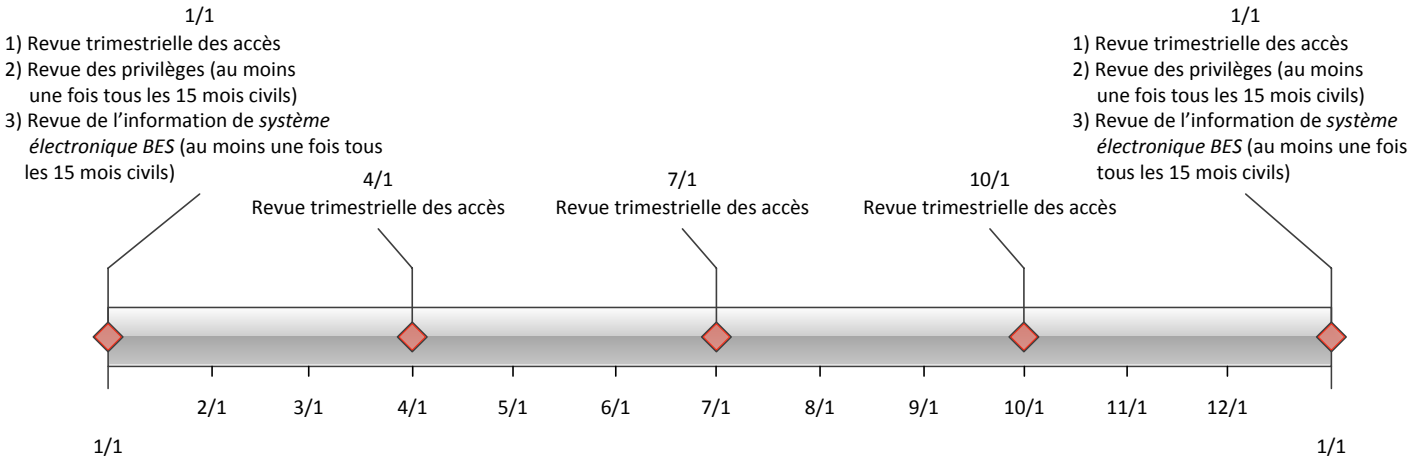
Exigence E4

L'autorisation d'accès électronique et physique sans accompagnement et d'accès à l'information de *système électronique BES* doit être accordée selon le principe du besoin de savoir suivant la fonction de chacun. Les documents attestant l'autorisation doivent comporter une justification des besoins d'affaires invoqués. Pour assurer une séparation adéquate des tâches, l'autorisation et la fourniture d'accès ne doivent pas être assumées par la même personne dans la mesure du possible.

Cette exigence prévoit des examens trimestriels ainsi que des examens au moins une fois tous les 15 mois civils. Les examens trimestriels servent à vérifier que l'accès aux *systèmes électroniques BES* n'a été accordé qu'aux utilisateurs autorisés. Pour ce faire, on compare la liste des personnes ayant reçu un accès à un *système électronique BES* avec le registre des personnes autorisées à accéder à ce *système électronique BES*. Cette exigence met l'accent sur l'intégrité du processus de fourniture d'accès plutôt que sur les comptes individuels de l'ensemble des *actifs électroniques BES*. La liste des personnes ayant reçu un accès peut être une liste de comptes générée automatiquement. Toutefois, dans un *système électronique BES* comptant plusieurs bases de données de comptes, la liste des personnes ayant reçu un accès peut provenir d'autres sources, comme des activités de fourniture d'accès ou d'une base de données de comptes utilisateurs qui sert habituellement de point de départ à la fourniture des accès.

L'examen des droits d'accès effectué au moins une fois tous les 15 mois civils est plus détaillé afin de s'assurer que seuls les droits d'accès nécessaires à un utilisateur dans l'exercice de ses

fonctions lui soient accordés (droit d'accès minimal). Les entités peuvent optimiser cet examen en mettant en place un accès basé sur les rôles. Ceci consiste à définir les rôles au sein du système (p. ex., répartiteur, technicien, récepteur de rapports, administrateur, etc.), puis à grouper les droits d'accès selon ces différents rôles, et à assigner leurs rôles aux utilisateurs. Ce système ne suppose aucun logiciel particulier et on peut le mettre en place en définissant des processus de fourniture d'accès particuliers pour chaque rôle ne permettant pas l'affectation de groupes d'accès. Le système d'autorisation d'accès axé sur les rôles élimine la nécessité d'un examen des droits d'accès des comptes individuels. Un calendrier type de tous les examens



énoncés à l'exigence E4 est illustré ci-dessous.

La séparation des tâches doit être prise en compte au moment de la réalisation des examens selon l'exigence E4. La personne chargée de l'examen ne doit pas être celle qui fournit les accès.

Si les résultats des examens de comptes trimestriels ou des examens de comptes aux 15 mois révèlent qu'il s'est produit une erreur administrative ou de transcription faisant en sorte qu'un accès n'a pas été réellement fourni, le SDT juge que cette erreur ne constitue pas une non-conformité.

Dans le cas de *systèmes électroniques BES* pour lesquels aucun compte utilisateur n'est défini, les contrôles indiqués à l'exigence E4 ne s'appliquent pas. L'entité responsable doit cependant documenter ces configurations.

Exigence E5 :

L'exigence de révoquer les accès au moment d'un départ prévoit des procédures démontrant que la révocation de l'accès se produit en même temps que le départ. On y admet que le moment où l'emploi prend fin peut varier selon les circonstances. Quelques scénarios courants et processus possibles en fonction du moment où cesse l'emploi sont présentés au tableau ci-dessous. Ces scénarios ne constituent pas une liste exhaustive de tous les scénarios possibles, mais ils sont représentatifs de plusieurs pratiques opérationnelles courantes.

Scénario	Processus possible
Départ involontaire immédiat	Un représentant des ressources humaines ou un agent de sécurité accompagne la personne hors du lieu de travail et le superviseur de celle-ci ou le personnel des ressources humaines demande au personnel compétent d'entamer le processus de révocation.
Départ involontaire prévu	Le personnel des ressources humaines est avisé du départ et collabore avec le personnel compétent pour que l'accès soit révoqué au moment du départ.
Départ volontaire	Le personnel des ressources humaines est avisé du départ et collabore avec le personnel compétent pour que l'accès soit révoqué au moment du départ.
Départ à la retraite, lorsque le dernier jour de travail est plusieurs semaines avant la date de cessation	Le personnel des ressources humaines s'entend avec le gestionnaire sur la date où l'accès ne sera plus nécessaire et planifie la révocation de l'accès pour cette date.
Décès	Le personnel des ressources humaines est avisé du décès et collabore avec le personnel compétent pour entamer le processus de révocation.

On entend par « révocation de l'accès électronique » un processus dont le résultat final est l'impossibilité d'obtenir un accès électronique aux *systèmes électroniques BES* en utilisant les identifiants de connexion attribués à ou connus de la personne dont les droits d'accès sont révoqués. Les mesures à prendre pour ce faire comprennent notamment la suppression ou la désactivation des comptes utilisés par cette personne ; aucune mesure précise n'est cependant prescrite dans la norme. Les entités doivent considérer les ramifications d'une suppression de compte, lesquelles peuvent inclure des entrées de journaux d'événements incomplets en raison d'un compte non reconnu ou de services de système utilisant le compte pour se connecter.

La révocation initiale prescrit à l'exigence E5.1 concerne aussi bien l'accès physique non accompagné que l'*accès distant interactif*. La révocation de ces deux accès doit empêcher tout accès de la personne après son départ. Si la personne détient toujours des comptes à accès local (c.-à-d. des comptes sur l'actif électronique même) sur les *actifs électroniques BES*, l'entité responsable dispose alors de 30 jours pour mener à bien le processus de révocation pour ces comptes. Toutefois, rien n'empêche l'entité responsable de révoquer tous les accès au moment du départ.

Dans le cas d'une personne mutée ou réaffectée, une révision des droits d'accès doit être effectuée. Cette révision peut impliquer une simple liste de toutes les autorisations associées à la personne et travailler en collaboration avec les gestionnaires respectifs pour déterminer de quels accès elle aura toujours besoin dans son nouveau poste. Dans le cas où la personne doit conserver un accès pour une période transitoire, l'entité doit prévoir une date d'examen de ces

droits d’accès ou les inclure dans l’examen de comptes trimestriel ou l’examen annuel des droits d’accès.

La révocation de l’accès aux comptes partagés est traitée séparément pour empêcher les situations où les mots de passe des équipements d’un poste ou d’une centrale changent constamment en raison du roulement du personnel.

L’exigence 5.5 précise que les mots de passe pour comptes partagés doivent être changés dans les 30 jours civils suivant la cessation de l’emploi ou lorsque l’entité responsable détermine qu’une personne n’a plus besoin d’avoir accès au compte en raison de sa réaffectation ou de sa mutation. Cette période de 30 jours est valable dans des conditions opérationnelles normales. Toutefois, certaines circonstances peuvent faire en sorte que ce ne soit pas possible. Il peut être nécessaire d’arrêter ou de redémarrer certains systèmes pour compléter le changement de mot de passe. En périodes de chaleur ou de froid extrême, plusieurs entités responsables pourraient interdire l’arrêt et le redémarrage de systèmes afin de maintenir la fiabilité du BES. Dans ce cas, l’entité responsable doit consigner ces circonstances et prévoir changer le mot de passe dans les 10 jours civils suivant la fin de ces circonstances. Les documents consignant ces activités doivent être conservés afin de démontrer que l’entité responsable a suivi le plan qu’elle a établi.

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 :

Faire en sorte que l'entité responsable avec du personnel ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *actifs électroniques BES* prenne des mesures pour que ce personnel avec de tels accès électroniques autorisés ou accès physiques autorisés sans accompagnement soit toujours au fait de ses pratiques de sécurité.

Sommaire des modifications : Restructuration sous forme de tableau.

Référence à une version précédente : (Partie 1.1) CIP-004-4, E1

Justification des modifications : (Partie 1.1)

Modifications visant à remplacer la nécessité de s'assurer ou de prouver que toutes les personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement « ont reçu » un rappel de façon continue énonçant que les pratiques de sécurité ont fait l'objet d'un rappel.

Déplacement des mécanismes de rappel dans les exemples.

Raisonnement pour E2 :

Faire en sorte que le programme de formation de l'entité responsable à l'intention du personnel ayant besoin d'un accès électronique autorisé ou d'un accès physique autorisé sans accompagnement à des *systèmes électroniques BES* traite des politiques, des contrôles d'accès et des procédures visant à protéger les *systèmes électroniques BES* et que ce personnel reçoive la formation avant de se voir accorder des accès.

Selon leur rôle, certains membres du personnel n'ont pas nécessairement à être formés sur tous les points.

Sommaire des modifications :

1. Ajout de formation axé sur les rôles pour :

- le programme de contrôle des visiteurs ;
- l'interconnectabilité électronique nécessaire à l'exploitation et au contrôle des *systèmes électroniques BES* ;
- les supports de stockage utilisés pour gérer l'information de *système électronique BES*.

2. Remplacement du terme « *actifs électroniques critiques* » par « *systèmes électroniques BES* ».

Référence une la version précédente : (Partie 2.1) CIP-004-4, E2.2.1

Justification des modifications : (Partie 2.1)

Retrait du concept d'« utilisation adéquate des *actifs électroniques critiques* » des versions antérieures pour mettre l'accent sur les questions de cybersécurité plutôt que sur la fonction administrative. La version précédente mettait l'accent sur l'utilisation administrative ou fonctionnelle des *systèmes électroniques BES*, qui sort du cadre de la cybersécurité. Le personnel qui administre le programme de contrôle des visiteurs ou qui accompagne les visiteurs doit recevoir une formation sur le programme. Formation de base sur la gestion de l'information de *système électronique BES* (et non d'*actif électronique critique*), et ajout du stockage ; ordonnance 706 de la FERC, paragraphe 413 et paragraphes 632 à 634, 688, 732 à 734 ; DHS 2.4.16. Formation de base sur la détection et la déclaration des incidents de cybersécurité ; ordonnance 706 de la FERC, paragraphe 413 ; se reporter à la norme CIP-008-5 et aux exigences de déclaration des incidents du Department of Homeland Security (DHS) pour les personnes ayant un rôle à jouer dans la déclaration des incidents. Formation de base sur les plans d'intervention et les procédures visant à rétablir les *systèmes électroniques BES* qui est donnée au personnel ayant un rôle à jouer dans le rétablissement ; ordonnance 706 de la FERC, paragraphe 413. Les programmes de formation de base sont destinés à englober le matériel et les logiciels de mise en réseau ainsi que sur les autres questions d'interconnectabilité électronique qui soutiennent l'exploitation et le contrôle des *systèmes électroniques BES* ; ordonnance 706 de la FERC, paragraphe 434.

Référence à une version précédente : (Partie 2.2) CIP-004-4, E2.1

Justification des modifications : (Partie 2.2)

L'ajout de critères relatifs aux circonstances exceptionnelles, conformément à l'ordonnance 706 de la FERC, paragraphe 431, est décrit en détail à la norme CIP-003-5.

Référence à une version précédente : (Partie 2.3) CIP-004-4, E2.3

Justification des modifications : (Partie 2.3)

Remplacement de la fréquence « annuelle » par « une fois tous les 15 mois civils ».

Raisonnement pour E3 :

Faire en sorte que les personnes qui ont besoin d'un accès électronique autorisé ou d'un accès physique autorisé sans accompagnement à des *systèmes électroniques BES* ont fait l'objet d'une évaluation des risques. Les personnes qui ont accès à ces systèmes doivent avoir fait l'objet d'une évaluation des risques liés au personnel au cours des sept dernières années, qu'il s'agisse d'une première autorisation d'accès ou du maintien de l'autorisation.

Sommaire des modifications : Précise que la vérification des antécédents criminels sur les sept années précédentes doit tenir compte de tous les endroits où a résidé la personne pendant au moins six mois consécutifs, y compris le lieu où elle réside actuellement, peu importe depuis combien de temps.

Référence à une version précédente : (Partie 3.1) CIP-004-4, E3.1

Justification des modifications : (Partie 3.1)

Prise en compte de la demande d'interprétation dans les exemples. Précise qu'il est nécessaire de disposer d'un processus de contrôle de l'identité. Le plan de mise en œuvre précise qu'un contrôle d'identité documenté mené en vertu d'une version antérieure des normes CIP est suffisant.

Référence à une version précédente : (Partie 3.2) CIP-004-4, E3.1

Justification des modifications : (Partie 3.2)

Précise que la vérification des antécédents judiciaires sur les sept années précédentes doit tenir compte de tous les endroits où a résidé la personne pendant au moins six mois, y compris le lieu où elle réside actuellement, peu importe depuis combien de temps. Ajout d'une formulation reposant sur la demande d'interprétation. Modalités pour le cas où il est impossible de mener une vérification complète sur les sept années précédentes.

Référence à une version précédente : (Partie 3.3) Nouvelle

Justification des modifications : (Partie 3.3)

Des critères ou des processus documentés doivent être en place pour permettre une évaluation des résultats des vérifications des antécédents judiciaires en vue d'autoriser un accès.

Référence à une version précédente : (Partie 3.4) CIP-004-4, E3.3

Justification des modifications : (Partie 3.4)

Migration de cette exigence dans sa propre partie d'exigences du tableau.

Référence à une version précédente : (Partie 3.5) CIP-004-3, E3, E3.3

Justification des modifications : (Partie 3.5)

Qu'il s'agisse d'une première autorisation d'accès ou du maintien de l'autorisation, établit que les personnes ayant un accès, doivent avoir fait l'objet d'une évaluation des risques liés au personnel au cours des sept dernières années. Ceci couvre l'initial et de le renouvellement. Le plan de mise en œuvre précise que cette exigence entre en vigueur sept ans après l'évaluation précédente des risques liés au personnel menée en vertu d'une version antérieure des normes CIP sur la cybersécurité. CIP-004-3, E3, E3.3

Raisonnement pour E4 :

Faire en sorte que les personnes ayant accès à des *systèmes électroniques BES* et à des emplacements physiques et électroniques où l'entité responsable stocke de l'information de *système électronique BES* sont dûment autorisées à avoir accès à ces systèmes et emplacements. L'« autorisation » est considérée comme étant un octroi de permission par une ou des personnes habilitées par l'entité responsable à autoriser cet octroi et faisant partie des délégations mentionnées à la norme CIP 003 5. La « fourniture » devrait être considérée comme étant les mesures prises pour donner un accès à une personne.

L'accès est constitué des accès physiques, logiques, et distant à des *actifs électroniques* qui composent le *système électronique BES* ou qui permettent l'accès au *système électronique BES*.

Au moment d'accorder, de réexaminer ou de révoquer un accès, l'entité responsable doit tenir compte de l'*actif électronique* en particulier de même que des systèmes utilisés pour permettre cet accès (p. ex., système de contrôle des accès physiques, système d'accès distant, services d'annuaire).

Les *circonstances CIP exceptionnelles* doivent être définies dans une politique de l'entité responsable conformément à la norme CIP 003 5 ; elles constituent une exception à l'exigence d'autorisation d'accès aux *systèmes électroniques BES* et à l'information de *système électronique BES*.

Les revues trimestrielles énoncées à la partie 4.5 servent à confirmer que l'accès aux *systèmes électroniques BES* n'a été accordé qu'aux utilisateurs autorisés. Pour ce faire, on compare la liste des personnes auxquelles on a réellement fourni un accès à un *système électronique BES* avec le registre des personnes autorisées à accéder à ce *système électronique BES*. Cette exigence met l'accent sur l'intégrité du processus de fourniture d'accès plutôt que sur les comptes individuels de l'ensemble des *actifs électroniques BES*. La liste des personnes auxquelles on a fourni un accès peut provenir d'une liste de comptes générée automatiquement. Toutefois, dans un *système électronique BES* comptant plusieurs bases de données de comptes, elle peut provenir d'autres sources, comme des activités de fourniture d'accès ou d'une base de données de comptes utilisateurs qui sert habituellement de point de départ à la fourniture des accès.

Si les résultats des examens de comptes trimestriels ou annuels révèlent qu'il s'est produit une erreur administrative ou de transcription faisant en sorte que l'accès n'a pas été réellement fourni, le SDT juge que cette erreur ne constitue pas une non-conformité.

Dans le cas de *systèmes électroniques BES* pour lesquels aucun compte utilisateur n'est défini, les contrôles indiqués à l'exigence E4 ne s'appliquent pas. L'entité responsable devrait cependant documenter ces configurations.

Sommaire des modifications : La principale modification consiste à rassembler les exigences sur la gestion des accès des normes CIP-003-4, CIP-004-4 et CIP-007-4 en une seule exigence. Les exigences de la version 4 restent pratiquement inchangées, sauf que certains termes ont été clarifiés. En combinant ces exigences, on cherche à ce qu'il n'y ait plus d'impression de redondance entre les processus d'autorisation et d'examen. L'obligation de tenir à jour une liste des employés autorisés, citée dans l'exigence E4 de la norme CIP 004-4, a été éliminée parce que cette liste ne représente qu'une forme de preuve parmi d'autres qui permet de démontrer que seules les personnes autorisées disposent d'un accès.

Références à une version précédente : (Partie 4.1) CIP-003-4, E5.1 et E5.2 ; CIP-006-4, E1.5 et E4 ; et CIP-007-4, E5.1 et E5.1.1

Justification des modifications : (Partie 4.1)

Combinaison des exigences des normes CIP-003-4, CIP-007-4 et CIP-006-4 en vue de clarifier et d'uniformiser le processus d'autorisation. Les normes CIP-003-4, CIP-004-4, CIP-006-4 et CIP-007-4 mentionnent toutes l'autorisation d'accès d'une façon ou d'une autre, et les normes CIP-003-4 et CIP-007-4 stipulent que l'autorisation doit être accordée selon le principe

du besoin de savoir ou selon les fonctions de chacun. Ces exigences ont été combinées afin d'uniformiser la formulation de l'exigence.

Référence à une version précédente : (Partie 4.2) CIP-004-4, E4.1

Justification des modifications : (Partie 4.2)

Les commentaires reçus des membres de l'équipe de rédaction, d'observateurs et d'auditeurs régionaux des normes CIP font état d'une certaine confusion, lors de mise en œuvre des mesures, quant au sens à donner au terme « revoir » à l'exigence E4.1 de la norme CIP-004-4. La présente exigence précise que l'examen doit comparer la fourniture de l'accès et l'autorisation de l'accès.

Référence à une version précédente : (Partie 4.3) CIP-007-4, E5.1.3

Justification des modifications : (Partie 4.3)

Déplacement des exigences pour assurer la cohérence et éliminer les renvois entre exigences. Précision sur les éléments à observer pour effectuer la vérification en indiquant que l'objectif est de confirmer que les droits d'accès sont correctement attribués et qu'ils se limitent au strict minimum.

Référence à la version précédente : (Partie 4.4) CIP-003-4, E5.1.2

Justification des modifications : (Partie 4.4)

Déplacement de l'exigence pour assurer la cohérence entre les examens des autorisations d'accès. Clarification du sens à donner au terme « annuel ». Précision sur les éléments à observer pour effectuer la vérification en indiquant que l'objectif est de confirmer que les droits d'accès sont correctement attribués et qu'ils correspondent au minimum nécessaire pour les tâches à accomplir.

Raisonnement pour E5 :

La révocation rapide de l'accès électronique aux *systèmes électroniques BES* constitue un élément essentiel de tout système de gestion des accès. Lorsque l'accès d'une personne à un *système électronique BES* n'est plus nécessaire dans le cadre de ses fonctions, il doit être révoqué. Ceci est particulièrement important dans les situations où des personnes sont licenciées ou réaffectées involontairement, puisqu'il y a un risque qu'elles réagissent de manière hostile ou destructrice.

En examinant la manière de répondre aux directives de l'ordonnance 706 de la FERC qui stipulent que l'accès doit être « immédiatement » révoqué en cas de départ involontaire, le SDT a choisi de ne pas préciser de délais précis dans l'exigence (p. ex., « révoquer l'accès dans l'heure suivant le départ »). Le moment où l'emploi d'une personne prend fin ne peut généralement pas être déterminé à l'heure près. Cependant, la plupart des organisations disposent d'un processus de cessation d'emploi en bonne et due forme, et la révocation de l'accès le plus rapide survient en même temps que les premières étapes de ce processus.

L'accès est constitué des accès physiques, logiques, et distant à des *actifs électroniques* qui composent le *système électronique BES* ou qui permettent l'accès au *système électronique BES*. Au moment d'accorder, de réexaminer ou de révoquer un accès, l'entité responsable doit tenir compte de l'*actif électronique* en particulier de même que des systèmes utilisés pour permettre cet accès (p. ex., système de contrôle des accès physiques, système d'accès distant, services d'annuaire).

Sommaire des modifications : L'ordonnance 706 de la FERC, paragraphes 460 et 461, énonce ce qui suit : « La Commission adopte la proposition réglementaire (Notice of Proposed Rulemaking ou NOPR) CIP pour demander à l'organisme de fiabilité du service d'électricité (ERO) d'apporter des modifications à la norme CIP 004 1 afin que soient immédiatement révoqués les droits d'accès d'un employé, d'un entrepreneur ou d'un fournisseur qui n'exerce plus une fonction exigeant un accès physique ou électronique à un *actif électronique critique*, pour quelque raison que ce soit (y compris les mesures disciplinaires, les mutations, les départs à la retraite ou les licenciements).

De façon générale, la Commission est d'avis que la révocation d'un accès dont l'employé n'a plus besoin, en raison d'un changement d'emploi ou d'une cessation d'emploi, doit être immédiate. »

Référence à une version précédente : (Partie 5.1) CIP-004-4, E4.2

Justification des modifications : (Partie 5.1)

L'ordonnance 706 de la FERC, paragraphes 460 et 461, prescrit des modifications aux normes **qui obligent la révocation immédiate** de l'accès de toute personne qui n'en a plus besoin. Pour tenir compte de cette directive, cette exigence stipule que la révocation doit se faire en même temps que la cessation d'emploi, plutôt que dans un délai de 24 heures.

Référence à une version précédente : (Partie 5.2) CIP-004-4, E4.2

Justification des modifications : (Partie 5.2)

L'ordonnance 706 de la FERC, paragraphes 460 et 461, prescrit des modifications aux normes qui obligent la révocation immédiate de l'accès de toute personne qui n'en a plus besoin, y compris les employés mutés. En examinant les modifications à apporter à cette exigence, le SDT a jugé que la date à laquelle une personne n'a plus besoin d'un accès après une mutation posait problème étant donné que les besoins peuvent varier avec le temps. Par conséquent, le SDT a adapté cette exigence à partir de la version 3 de la norme 800-53 du NIST de sorte que l'examen des autorisations d'accès soit fait à la date de mutation. Le SDT a estimé que cette mesure de contrôle permettait d'atteindre plus efficacement l'objectif d'empêcher une personne de cumuler des autorisations inutiles au fil des mutations.

Référence à une version précédente : (Partie 5.3) Nouvelle

Justification des modifications : (Partie 5.3)

L'ordonnance 706 de la FERC, paragraphe 386, prescrit des modifications aux normes qui obligent la révocation rapide de l'accès à l'information protégée. Pour tenir compte de cette directive, les entités responsables doivent révoquer l'accès aux emplacements destinés à

l'information de *système électronique BES.* Ceci pourrait comprendre les classeurs, les salles de commande de postes électriques, les systèmes de gestion des documents, les partages de fichiers ou autres emplacements physiques et logiques sous le contrôle de l'entité responsable.

Référence à une version précédente : (Partie 5.4) Nouvelle

Justification des modifications : (Partie 5.4)

L'ordonnance 706 de la FERC, paragraphes 460 et 461, prescrit des modifications aux normes pour exiger la révocation immédiate de l'accès de toute personne qui n'en a plus besoin. Afin de respecter ce délai immédiat, les entités responsables disposeront probablement de procédures de révocation initiale visant à bloquer l'accès distant et physique au *système électronique BES*. Dans certains cas, la coordination de la révocation d'accès à des *actifs électroniques* et applications individuels peut prendre plus de temps sans nuire à la fiabilité. Cette exigence accorde le délai supplémentaire pour examiner et compléter le processus de révocation. Bien que les mesures initiales empêchent déjà un accès ultérieur, cette étape offre une assurance supplémentaire dans le processus de révocation d'accès.

Référence à la version précédente : (Partie 5.5) CIP-007-4, E5.2.3

Justification des modifications : (Partie 5.5)

Fournir une clarification sur les mesures à prendre pour gérer les mots de passe.

Historique des versions

Version	Date	Modification apportée	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.
5.1	30 septembre 2013	Modification de deux VSL à E4.	Errata
5.1	22 novembre 2013	Émission d'une ordonnance de la FERC approuvant CIP-004-5.1	
5.1	9 juillet 2014	Émission d'une lettre d'ordonnance approuvant les révisions aux VRF et VSL	L'exigence 4 de CIP-004-5.1 est

		de certaines normes CIP.	passée de Faible à Moyen, et changement des VSL de l'exigence 4 à une gradation basé sur un pourcentage.

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

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe aura préséance.

A. Introduction

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

2. **Numéro :** CIP-004-5.1

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

Entités fonctionnelles

Aucune disposition particulière

Installations

La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

- Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur un réseau voisin.
- Postes élévateurs des installations de production identifiées au point précédent.

5. **Date d'entrée en vigueur au Québec :**

5.1. Adoption de la norme par la Régie de l'énergie : xx mois 201x

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

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

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

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

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

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

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

A. Introduction

1. Titre : Cybersécurité – Périmètres de sécurité électronique

2. Numéro : CIP-005-5

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

4. Applicabilité :

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

4.1.1 Responsable de l'équilibrage

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

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

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

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

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

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

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

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

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

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

4.2.1.1 Chaque système de DSF ou de DST qui :

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

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

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

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

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

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

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

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

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

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

5. Dates d'entrée en vigueur :

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

6. Contexte :

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

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

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

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

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

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

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

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

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

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

Colonnes « Systèmes visés » des tableaux :

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

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

B. Exigences et mesures

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

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

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

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

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

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

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

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

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

C. Conformité

1. Processus de surveillance de la conformité :

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

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

1.2. Conservation des pièces justificatives :

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

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

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

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

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

1.4. Autres informations sur la conformité :

- Aucune

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)	L'entité responsable n'avait pas documenté un ou plusieurs processus pour le *Tableau E1 (CIP-005-5) – Périmètre de sécurité électronique*. (R1) OU L'entité responsable n'avait pas tous les *actifs électroniques* 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) OU La *connectivité externe routable* à travers l'ESP n'était pas effectuée par l'intermédiaire d'un EAP identifié. (1.2) OU

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-005-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						L'entité responsable n'a pas exigé d'autorisations pour les accès entrants et sortants et refusé tout autre accès par défaut. (1.3) OU L'entité responsable n'a pas effectué l'authentification lors de l'établissement de la connectivité par lien commuté avec les *actifs électroniques* applicables, lorsque techniquement faisable. (1.4)
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)	

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

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe aura préséance.

A. Introduction

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

2. **Numéro :** CIP-005-5

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

   Entités fonctionnelles

   Aucune disposition particulière

   Installations

   La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

   Exemptions additionnelles

   Sont exemptés de l'application de la présente norme :

   - Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur un réseau voisin.
   - Postes élévateurs des installations de production identifiées au point précédent.

5. **Date d'entrée en vigueur au Québec :**

   5.1. Adoption de la norme par la Régie de l'énergie : xx mois 201x

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

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

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

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

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

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

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

A. Introduction

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

2. Numéro : CIP-006-5

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

4. Applicabilité :

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

4.1.1 Responsable de l'équilibrage

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

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

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

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

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

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

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

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

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

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

4.2.1.1 Chaque système de DSF ou de DST qui :

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

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

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

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

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

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

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

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

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

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

5. Dates d'entrée en vigueur

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

6. Contexte

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

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

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

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

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

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

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

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

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

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

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

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

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

Colonnes « Systèmes visés » des tableaux

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

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

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

B. Exigences et mesures

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Conformité

1. Processus de surveillance de la conformité

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

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

1.2. Conservation des pièces justificatives

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

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

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

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

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

1.4. Autres informations sur la conformité

- Aucune

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 « Responsabilité du contrôle de 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 :

- Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur un réseau voisin.
- Postes élévateurs des installations de production identifiées au point précédent.

5. **Date d'entrée en vigueur au Québec :**

5.1. Adoption de la norme par la Régie de l'énergie : xx mois 201x

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

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

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

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

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

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

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

A. Introduction

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

2. Numéro : CIP-007-5

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

4. Applicabilité :

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

4.1.1 Responsable de l'équilibrage

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

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

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

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

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

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

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

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

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

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

4.2.1.1 Chaque système de DSF ou de DST qui :

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

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

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

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

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

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

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

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

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

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

5. Dates d'entrée en vigueur

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

6. Contexte :

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

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

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

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

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

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

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

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

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

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

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

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

Colonnes « Systèmes visés » des tableaux

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

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

B. Exigences et mesures

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Tableau E4 (CIP-007-5) – Surveillance des événements de sécurité			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
4.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; 2. PACS associés ; 3. PCA associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; 2. PACS associés ; 3. PCA associés.	Journaliser les événements au niveau du *système électronique BES* (selon les capacités du *système électronique BES*) ou au niveau de l'*actif électronique* (selon les capacités de l'*actif électronique*) permettant la détection des *incidents de cybersécurité* – et les enquêtes subséquentes à leur sujet – qui comprennent au minimum chacun des types d'événements suivants : 4.1.1. toute tentative détectée d'ouverture de session ayant réussi ; 4.1.2. toute tentative détectée d'accès ou d'ouverture de session ayant échoué ; 4.1.3. tout programme malveillant détecté.	Exemples non limitatifs de pièces justificatives : liste des types d'événements que le *système électronique BES* est en mesure de détecter, générée manuellement ou par le système lui-même, et, le cas échéant, qu'il est configuré pour journaliser. Cette liste doit comprendre les types d'événements obligatoires.

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

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

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

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

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

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

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

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

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

C. Conformité

1. Processus de surveillance de la conformité

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

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

1.2. Conservation des pièces justificatives

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

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

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

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

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

1.4. Autres informations sur la conformité

- Aucune.

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

2. Tableau des éléments de conformité

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	**Exploitation du jour même**	**Moyen**	Sans objet	L'entité responsable a mis en œuvre et documenté des processus pour les ports et services, mais n'avait aucune méthode pour empêcher l'utilisation de ports d'entrée-sortie physiques non nécessaires utilisés pour la connectivité de réseau, les commandes pupitre ou les supports d'information amovibles, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (1.2) OU L'entité responsable a mis en œuvre et documenté des processus pour les ports et services mais	L'entité responsable a mis en œuvre et documenté des processus pour la détermination des ports et services nécessaires, mais lorsque techniquement faisable, un ou plusieurs ports logiques accessibles par le réseau non nécessaires étaient activés, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (1.1) OU L'entité responsable a mis en œuvre et documenté des processus pour la détermination des ports et services nécessaires, mais lorsque techniquement	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus qui comprenaient les éléments applicables du tableau E1 (CIP-007-5), et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (E1) OU L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus qui comprenaient les éléments applicables du tableau E1 (CIP-007-5), mais n'a pas identifié, évalué ou corrigé les lacunes. (E1)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				n'avait aucune méthode pour empêcher l'utilisation de ports d'entrée-sortie physiques non nécessaires utilisés pour la connectivité de réseau, les commandes pupitre ou les supports d'information amovibles, mais n'a pas identifié, évalué ou corrigé les lacunes. (1.2)	faisable, un ou plusieurs ports logiques accessibles par le réseau non nécessaires étaient activés, mais n'a pas identifié, évalué ou corrigé les lacunes. (1.1)	
E2	**Planification de l'exploitation**	**Moyen**	L'entité responsable a documenté et mise en œuvre un ou plusieurs processus pour évaluer l'applicabilité des rustines de sécurité non installées publiées, mais n'a pas évalué l'applicabilité des rustines de sécurité dans les 35 jours civils, mais dans les 50 jours civils après l'évaluation précédente pour la ou	L'entité responsable a documenté et mise en œuvre un ou plusieurs processus pour la gestion des rustines, mais n'a inclus aucun processus comprenant la désignation de la ou des sources pour le suivi ou l'évaluation des rustines de cybersécurité destinées aux *actifs électroniques* visés, et	L'entité responsable a documenté et mise en œuvre un ou plusieurs processus pour la gestion des rustines, mais n'a inclus aucun processus pour l'installation des rustines de cybersécurité destinées aux *actifs électroniques* visés, et a identifié les lacunes, mais n'a pas évalué ou	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus qui comprenaient les éléments applicables du tableau E2 (CIP-007-5), et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (E2) OU L'entité responsable

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			les sources indiquées, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (2.2) OU L'entité responsable a documenté et mise en œuvre un ou plusieurs processus pour évaluer l'applicabilité des rustines de sécurité non installées publiées, mais n'a pas évalué l'applicabilité des rustines de sécurité dans les 35 jours civils, mais dans les 50 jours civils après l'évaluation précédente pour la ou les sources indiquées, mais n'a pas identifié, évalué ou corrigé les lacunes. (2.2) OU L'entité responsable a un ou plusieurs	a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (2.1) OU L'entité responsable a documenté et mise en œuvre un ou plusieurs processus pour la gestion des rustines, mais n'a inclus aucun processus comprenant la désignation de la ou des sources pour le suivi ou l'évaluation des rustines de cybersécurité destinées aux *actifs électroniques* visés, mais n'a pas identifié, évalué ou corrigé les lacunes. (2.1) OU L'entité responsable a documenté et mise en œuvre un ou plusieurs processus pour évaluer	corrigé les lacunes. (2.1) OU L'entité responsable a documenté et mise en œuvre un ou plusieurs processus pour la gestion des rustines, mais n'a inclus aucun processus pour l'installation des rustines de cybersécurité destinées aux *actifs électroniques* visés, mais n'a pas identifié, évalué ou corrigé les lacunes. (2.1) OU L'entité responsable a documenté et mise en œuvre un ou plusieurs processus pour évaluer l'applicabilité des rustines de sécurité non installées publiées, mais n'a pas évalué	n'a pas mis en œuvre ou documenté un ou plusieurs processus qui comprenaient les éléments applicables du tableau E2 (CIP-007-5), mais n'a pas identifié, évalué ou corrigé les lacunes. (E2) OU L'entité responsable a documenté et mise en œuvre un ou plusieurs processus pour la gestion des rustines, mais n'a inclus aucun processus pour le suivi, l'évaluation ou l'installation des rustines de cybersécurité destinées aux *actifs électroniques* visés, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (2.1)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			processus documentés pour l'évaluation des rustines de cybersécurité, mais, afin de mitiger les vulnérabilités exposées par les rustines de sécurité applicables, n'a pas appliqué les rustines applicables, créé un plan de mitigation daté, ou révisé un plan de mitigation existant dans les 35 jours civils, mais dans les 50 jours civils après que l'évaluation soit terminée, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (2.3) OU L'entité responsable a un ou plusieurs processus documentés pour l'évaluation des rustines de	l'applicabilité des rustines de sécurité non installées publiées, mais n'a pas évalué l'applicabilité des rustines de sécurité dans les 50 jours civils, mais dans les 65 jours civils après l'évaluation précédente pour la ou les sources indiquées, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (2.2) OU L'entité responsable a documenté et mise en œuvre un ou plusieurs processus pour évaluer l'applicabilité des rustines de sécurité non installées publiées, mais n'a pas évalué l'applicabilité des rustines de sécurité dans les 50 jours civils, mais dans les 65 jours	l'applicabilité des rustines de sécurité dans les 65 jours civils après l'évaluation précédente pour la ou les sources indiquées, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (2.2) OU L'entité responsable a documenté et mise en œuvre un ou plusieurs processus pour évaluer l'applicabilité des rustines de sécurité non installées publiées, mais n'a pas évalué l'applicabilité des rustines de sécurité dans les 65 jours civils après l'évaluation précédente pour la ou les sources indiquées, mais n'a pas identifié, évalué ou corrigé les	OU L'entité responsable a documenté et mise en œuvre un ou plusieurs processus pour la gestion des rustines, mais n'a inclus aucun processus pour le suivi, l'évaluation ou l'installation des rustines de cybersécurité destinées aux *actifs électroniques* visés, mais n'a pas identifié, évalué ou corrigé les lacunes. (2.1) OU L'entité responsable a documenté un plan de mitigation pour une rustine de cybersécurité applicable et a documenté une révision ou un prolongement du délai,

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			cybersécurité, mais, afin de mitiger les vulnérabilités exposées par les rustines de sécurité applicables, n'a pas appliqué les rustines applicables, créé un plan de mitigation daté, ou révisé un plan de mitigation existant dans les 35 jours civils, mais dans les 50 jours civils après que l'évaluation soit terminée, mais n'a pas identifié, évalué ou corrigé les lacunes. (2.3)	civils après l'évaluation précédente pour la ou les sources indiquées, mais n'a pas identifié, évalué ou corrigé les lacunes. (2.2) OU L'entité responsable a un ou plusieurs processus documentés pour l'évaluation des rustines de cybersécurité, mais, afin de mitiger les vulnérabilités exposées par les rustines de sécurité applicables, n'a pas appliqué les rustines applicables, créé un plan de mitigation daté, ou révisé un plan de mitigation existant dans les 50 jours civils, mais dans les 65 jours civils après que l'évaluation soit terminée, et a identifié	lacunes. (2.2) OU L'entité responsable a un ou plusieurs processus documentés pour l'évaluation des rustines de cybersécurité, mais, afin de mitiger les vulnérabilités exposées par les rustines de sécurité applicables, n'a pas appliqué les rustines applicables, créé un plan de mitigation daté, ou révisé un plan de mitigation existant dans les 65 jours civils après que l'évaluation soit terminée, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (2.3) OU L'entité responsable a	mais n'a pas obtenu l'approbation du *cadre supérieur CIP* ou de son délégué, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (2.4) OU L'entité responsable a documenté un plan de mitigation pour une rustine de cybersécurité applicable et a documenté une révision ou un prolongement du délai, mais n'a pas obtenu l'approbation du *cadre supérieur CIP* ou de son délégué, mais n'a pas identifié, évalué ou corrigé les lacunes. (2.4) OU L'entité responsable a documenté un plan de

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				les lacunes, mais n'a pas évalué ou corrigé les lacunes. (2.3) OU L'entité responsable a un ou plusieurs processus documentés pour l'évaluation des rustines de cybersécurité, mais, afin de mitiger les vulnérabilités exposées par les rustines de sécurité applicables, n'a pas appliqué les rustines applicables, créé un plan de mitigation daté, ou révisé un plan de mitigation existant dans les 50 jours civils, mais dans les 65 jours civils après que l'évaluation soit terminée, mais n'a pas identifié, évalué ou corrigé les lacunes.	un ou plusieurs processus documentés pour l'évaluation des rustines de cybersécurité, mais, afin de mitiger les vulnérabilités exposées par les rustines de sécurité applicables, n'a pas appliqué les rustines applicables, créé un plan de mitigation daté, ou révisé un plan de mitigation existant dans les 65 jours civils après que l'évaluation soit terminée, mais n'a pas identifié, évalué ou corrigé les lacunes. (2.3)	mitigation pour une rustine de cybersécurité applicable, mais n'a pas mis en œuvre le plan tel que créé ou révisé dans le délai spécifié dans le plan, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (2.4) OU L'entité responsable a documenté un plan de mitigation pour une rustine de cybersécurité applicable, mais n'a pas mis en œuvre le plan tel que créé ou révisé dans le délai spécifié dans le plan, mais n'a pas identifié, évalué ou corrigé les lacunes. (2.4)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				(2.3)		
E3	**Exploitation du jour même**	**Moyen**		L'entité responsable a mis en œuvre un ou plusieurs processus, mais, dans les cas où des signatures ou des séquences de code sont utilisées, l'entité responsable n'a pas traité de l'essai des signatures et des séquences de code, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (3.3) OU L'entité responsable a mis en œuvre un ou plusieurs processus, mais, dans les cas où des signatures ou des séquences de code sont utilisées, l'entité responsable n'a pas traité de l'essai des signatures et des	L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour la protection contre les programmes malveillants, mais n'a pas mitigé la menace des programmes malveillants détectés, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (3.2) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour la protection contre les programmes malveillants, mais n'a pas mitigé la menace des programmes malveillants détectés, mais n'a pas identifié,	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus qui comprenaient les éléments applicables du tableau E3 (CIP-007-5), et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (E3) OU L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus qui comprenaient les éléments applicables du tableau E3 (CIP-007-5), mais n'a pas identifié, évalué ou corrigé les lacunes. (E3) OU L'entité responsable a mis en œuvre un ou

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				séquences de code, mais n'a pas identifié, évalué ou corrigé les lacunes. (3.3)	évalué ou corrigé les lacunes. (3.2) OU L'entité responsable a mis en œuvre un ou plusieurs processus, mais, dans les cas où des signatures ou des séquences de code sont utilisées, l'entité responsable n'a pas mis à jour les protections contre les programme malveillants, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (3.3) OU L'entité responsable a mis en œuvre un ou plusieurs processus, mais, dans les cas où des signatures ou des séquences de code sont utilisées, l'entité	plusieurs processus documentés pour la protection contre les programmes malveillants, mais n'a pas déployé de méthodes pour bloquer, détecter ou prévenir les programmes malveillants, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (3.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour la protection contre les programmes malveillants, mais n'a pas déployé de méthodes pour bloquer, détecter ou prévenir les programmes

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					responsable n'a pas mis à jour les protections contre les programme malveillants, mais n'a pas identifié, évalué ou corrigé les lacunes. (3.3)	malveillants, mais n'a pas identifié, évalué ou corrigé les lacunes. (3.1)
E4	**Exploitation du jour même et Évaluation de l'exploitation**	**Moyen**	L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour repérer les *incidents de cybersécurité* non détectés en passant en revue un résumé ou un échantillon des événements journalisés défini par l'entité, au moins tous les 15 jours civils, mais a manqué un intervalle et complété la revue dans les 22 jours civils après la revue précédente, et a identifié les lacunes, mais n'a pas évalué ou	L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour repérer les *incidents de cybersécurité* non détectés en passant en revue un résumé ou un échantillon des événements journalisés défini par l'entité, au moins tous les 15 jours civils, mais a manqué un intervalle et complété la revue dans les 30 jours civils après la revue précédente, et a identifié les lacunes, mais n'a pas évalué ou	L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour générer des alertes pour les événements de sécurité nécessaires (tel que déterminé par l'entité responsable) pour les systèmes applicables (par fonction de dispositif ou de système), mais n'a pas généré d'alertes pour tous les types d'événements indiqués en 4.2.1 à 4.2.2, et a identifié les lacunes, mais n'a pas évalué ou corrigé les	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus qui comprenaient les éléments applicables du tableau E4 (CIP-007-5), et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (E4) OU L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus qui comprenaient les éléments applicables du tableau E4

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			corrigé les lacunes. (4.4) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour repérer les *incidents de cybersécurité* non détectés en passant en revue un résumé ou un échantillon des événements journalisés défini par l'entité, au moins tous les 15 jours civils, mais a manqué un intervalle et complété la revue dans les 22 jours civils après la revue précédente, mais n'a pas identifié, évalué ou corrigé les lacunes. (4.4)	corrigé les lacunes. (4.4) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour repérer les *incidents de cybersécurité* non détectés en passant en revue un résumé ou un échantillon des événements journalisés défini par l'entité, au moins tous les 15 jours civils, mais a manqué un intervalle et complété la revue dans les 30 jours civils après la revue précédente, mais n'a pas identifié, évalué ou corrigé les lacunes. (4.4)	lacunes. (4.2) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour générer des alertes pour les événements de sécurité nécessaires (tel que déterminé par l'entité responsable) pour les systèmes applicables (par fonction de dispositif ou de système), mais n'a pas généré d'alertes pour tous les types d'événements indiqués en 4.2.1 à 4.2.2, mais n'a pas identifié, évalué ou corrigé les lacunes. (4.2) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs	(CIP-007-5), mais n'a pas identifié, évalué ou corrigé les lacunes. (E4) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour journaliser les événements pour les systèmes applicables (par fonction de dispositif ou de système), mais n'a pas journalisé tous les types d'événements requis indiqués en 4.1.1 à 4.1.3, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (4.1) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					processus pour journaliser les événements applicables indiqués en 4.1 (lorsque techniquement faisable et sauf dans des *circonstances CIP exceptionnelles*), mais n'a pas conservé les journaux d'événements applicables pendant au moins les 90 derniers jours consécutifs, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (4.3) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour journaliser les événements applicables indiqués en 4.1 (lorsque	journaliser les événements pour les systèmes applicables (par fonction de dispositif ou de système), mais n'a pas journalisé tous les types d'événements requis indiqués en 4.1.1 à 4.1.3, mais n'a pas identifié, évalué ou corrigé les lacunes. (4.1)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					techniquement faisable et sauf dans des *circonstances CIP exceptionnelles*), mais n'a pas conservé les journaux d'événements applicables pendant au moins les 90 derniers jours consécutifs, mais n'a pas identifié, évalué ou corrigé les lacunes. (4.3) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour repérer les *incidents de cybersécurité* non détectés en passant en revue un résumé ou un échantillon des événements journalisés défini par l'entité, au moins tous les 15 jours civils, mais a manqué deux	

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					intervalles ou plus, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (4.4) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour repérer les *incidents de cybersécurité* non détectés en passant en revue un résumé ou un échantillon des événements journalisés défini par l'entité, au moins tous les 15 jours civils, mais a manqué deux intervalles ou plus, mais n'a pas identifié, évalué ou corrigé les lacunes. (4.4)	
E5	**Planification de l'exploitation**	**Moyen**	L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour	L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour	L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus qui

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			l'authentification par mot de passe uniquement de l'accès utilisateur interactif, mais n'a pas imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe dans les 15 mois civils, mais en moins de 16 mois civils après le dernier changement de mot de passe, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (5.6) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification par mot de passe uniquement de l'accès	l'authentification par mot de passe uniquement de l'accès utilisateur interactif, mais n'a pas imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe dans les 16 mois civils, mais en moins de 17 mois civils après le dernier changement de mot de passe, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (5.6) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification par mot de passe uniquement de l'accès	contrôle des accès aux systèmes, mais n'a pas inclus l'identification ou l'inventaire de tous les comptes par défaut ou autres types de comptes génériques qui sont connus et activés, soit par système, par groupe de systèmes, par emplacement ou par type de système, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (5.2) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais n'a pas inclus l'identification ou l'inventaire de tous les comptes par défaut ou autres types de	comprenaient les éléments applicables du tableau E5 (CIP-007-5), et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (E5) OU L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus qui comprenaient les éléments applicables du tableau E5 (CIP-007-5), mais n'a pas identifié, évalué ou corrigé les lacunes. (E5) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais, lorsque techniquement faisable, n'a pas de

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			utilisateur interactif, mais n'a pas imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe dans les 15 mois civils, mais en moins de 16 mois civils après le dernier changement de mot de passe, mais n'a pas identifié, évalué ou corrigé les lacunes. (5.6)	utilisateur interactif, mais n'a pas imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe dans les 16 mois civils, mais en moins de 17 mois civils après le dernier changement de mot de passe, mais n'a pas identifié, évalué ou corrigé les lacunes. (5.6)	comptes génériques qui sont connus et activés, soit par système, par groupe de systèmes, par emplacement ou par type de système, mais n'a pas identifié, évalué ou corrigé les lacunes. (5.2) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais n'a pas inclus l'identification des personnes ayant un accès autorisé à des comptes partagés, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (5.3) OU L'entité responsable a	méthodes pour imposer l'authentification de l'accès utilisateur interactif, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (5.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais, lorsque techniquement faisable, n'a pas de méthodes pour imposer l'authentification de l'accès utilisateur interactif, mais n'a pas identifié, évalué ou corrigé les lacunes. (5.1) OU L'entité responsable a

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais n'a pas inclus l'identification des personnes ayant un accès autorisé à des comptes partagés, mais n'a pas identifié, évalué ou corrigé les lacunes. (5.3) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification par mot de passe uniquement de l'accès utilisateur interactif qui n'imposait pas, par des moyens techniques ou procéduraux, un des deux paramètres de mot de passe indiqués en 5.5.1 et 5.5.2, et a identifié les lacunes,	mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais n'a pas, par fonction de dispositif, changé les mots de passe par défaut connus, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (5.4) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais n'a pas, par fonction de dispositif, changé les mots de passe par défaut connus, mais n'a pas identifié, évalué ou corrigé les lacunes. (5.4)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					mais n'a pas évalué ou corrigé les lacunes. (5.5) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification par mot de passe uniquement de l'accès utilisateur interactif qui n'imposait pas, par des moyens techniques ou procéduraux, un des deux paramètres de mot de passe indiqués en 5.5.1 et 5.5.2, mais n'a pas identifié, évalué ou corrigé les lacunes. (5.5) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification par	OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification par mot de passe uniquement de l'accès utilisateur interactif qui n'imposait pas, par des moyens techniques ou procéduraux, tous les paramètres de mot de passe indiqués en 5.5.1 et 5.5.2, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (5.5) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification par mot de passe uniquement de l'accès utilisateur interactif qui

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					mot de passe uniquement de l’accès utilisateur interactif, mais n'a pas imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l’obligation de changer le mot de passe dans les 17 mois civils, mais en moins de 18 mois civils après le dernier changement de mot de passe, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (5.6) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l’authentification par mot de passe uniquement de l’accès utilisateur interactif,	n'imposait pas, par des moyens techniques ou procéduraux, tous les paramètres de mot de passe indiqués en 5.5.1 et 5.5.2, mais n'a pas identifié, évalué ou corrigé les lacunes. (5.5) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l’authentification par mot de passe uniquement de l’accès utilisateur interactif, mais n'a pas imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l’obligation de changer le mot de passe dans les 18 mois civils après le dernier changement

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					mais n'a pas imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe dans les 17 mois civils, mais en moins de 18 mois civils après le dernier changement de mot de passe, mais n'a pas identifié, évalué ou corrigé les lacunes. (5.6)	de mot de passe, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (5.6) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification par mot de passe uniquement de l'accès utilisateur interactif, mais n'a pas imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe dans les 18 mois civils après le dernier changement de mot de passe, mais n'a pas identifié, évalué ou corrigé les

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						lacunes. (5.6) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais, lorsque techniquement faisable, n'a pas soit limité le nombre de tentatives d'authentification échouées ou soit généré des alertes après un certain nombre de tentatives d'authentification échouées, et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (5.7) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						contrôle des accès aux systèmes, mais, lorsque techniquement faisable, n'a pas soit limité le nombre de tentatives d'authentification échouées ou soit généré des alertes après un certain nombre de tentatives d'authentification échouées, mais n'a pas identifié, évalué ou corrigé les lacunes. (5.7)

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 a pour but de réduire la surface d'attaque des *actifs électroniques* en obligeant les entités à désactiver les ports non nécessaires. L'intention du SDT est de faire en sorte que l'entité sache quels ports et services connexes sont accessibles (« ports à l'écoute ») sur ses actifs et systèmes et s'ils sont nécessaires au fonctionnement de l'*actif électronique*, et qu'elle désactive tous les autres ports ou limite l'accès à ceux-ci.

1.1. Le plus souvent, il est possible de respecter cette exigence en désactivant le service ou programme à l'écoute sur le port, ou les paramètres de configuration dans l'*actif électronique*. Il est aussi possible d'utiliser des ordinateurs pare-feu, des enveloppeurs TCP ou d'autres moyens sur l'*actif électronique* afin de restreindre l'accès. À noter : cette exigence s'applique aux *actifs électroniques*, qui constituent les *systèmes électroniques BES* pertinents et les *actifs électroniques* qui leur sont associés. Ce contrôle constitue une autre couche de défense contre les attaques provenant du réseau et, par conséquent, le SDT souhaite que le contrôle soit installé sur le dispositif lui-même ou y soit raccordé directement, sans possibilité de contournement. Le verrouillage de ports à la frontière de l'ESP ne se substitue pas à cette exigence touchant le dispositif. Si un dispositif ne permet pas que l'on en désactive ou restreigne les ports logiques (par exemple, un dispositif spécialement conçu et commandé par

micrologiciel, sans configuration de port possible), les ports ouverts sont alors jugés « nécessaires ».

1.2. Les ports d'entrée-sortie physiques sont par exemple les ports réseau, série et USB à l'extérieur du boîtier du dispositif. Puisque les *systèmes électroniques BES* doivent se trouver à l'intérieur d'un *périmètre de sécurité physique*, les ports d'entrée-sortie physiques sont protégés contre les accès non autorisés. Une utilisation accidentelle est cependant possible, par exemple le branchement d'un modem ou d'un câble reliant des réseaux, ou l'insertion d'une clé USB. Les ports utilisés pour les « commandes pupitre » sont principalement des ports série sur des *actifs électroniques* qui fournissent une interface de gestion.

La protection de ces ports peut être assurée par plusieurs moyens, notamment les suivants :

- désactivation de tous les ports physiques non nécessaires dans la configuration de l'*actif électronique* ;
- signalisation bien en évidence, ruban inviolable ou tout autre moyen servant à signaler que les ports ne doivent pas être utilisés sans autorisation appropriée ;
- obstruction des ports physiques au moyen de verrous amovibles.

Il s'agit d'un contrôle faisant partie d'une démarche de « défense en profondeur » et qui tient compte du fait qu'il existe d'autres niveaux de contrôle, dont le PSP, qui empêchent le personnel non autorisé d'avoir un accès physique à ces ports. Même avec l'accès physique, il a été souligné qu'il y avait d'autres moyens de contourner le contrôle. Ce type de contrôle, qui comprend notamment la signalisation, ne se veut pas un moyen de prévention contre les intrusions. En effet, la signalisation est un contrôle directif plus qu'un contrôle préventif. Toutefois, dans une approche de défense en profondeur, différents niveaux et types de contrôles sont exigés d'un bout à l'autre de la norme, ce qui renforce la sécurité dans l'environnement des *centres de contrôle*. Une fois que le personnel autorisé a accédé physiquement après être avoir satisfait aux autres mesures de prévention et de détection, il est opportun de prévoir comme dernière ligne de défense dans ces secteurs à très haut risque un contrôle directif décrivant le comportement approprié. Essentiellement, la signalisation sert à rappeler aux utilisateurs autorisés de réfléchir avant de brancher quoi que ce soit sur un de ces systèmes : c'est exactement ce que vise cette exigence. Ce contrôle n'est pas conçu principalement pour empêcher les intrusions, mais plutôt à l'intention d'un employé autorisé, par exemple, qui voudrait brancher son téléphone intelligent peut-être infecté sur le port USB du pupitre d'un répartiteur afin d'en recharger la pile.

Exigence E2

L'intention du SDT en produisant l'exigence E2 est d'obliger les entités à se tenir au courant des vulnérabilités logicielles connues qui sont associées à leurs *actifs électroniques BES*, à en faire le suivi et à en mitiger les effets. Il ne s'agit pas de leur imposer l'installation de chaque rustine de sécurité, mais plutôt d'exiger qu'ils se tiennent au courant de toutes les vulnérabilités connues et de les gérer en temps opportun.

La gestion des rustines de sécurité s'impose pour les *systèmes électroniques BES* qui sont accessibles à distance et pour les systèmes autonomes. Ces derniers sont vulnérables à l'introduction intentionnelle ou involontaire de programmes malveillants. Une solide stratégie de défense en profondeur emploie des mesures supplémentaires telles que la sécurité physique, un logiciel de protection contre les programmes malveillants et la gestion des rustines pour restreindre l'introduction de programmes malveillants ou l'exploitation de vulnérabilités connues.

Un ou plusieurs processus peuvent être utilisés. Par exemple, un processus d'évaluation global peut être abordé dans un document principal, des documents secondaires établissant le processus plus détaillé à suivre pour chacun des systèmes. Ces documents secondaires peuvent notamment aborder les caractéristiques particulières des *systèmes électroniques BES*.

2.1. L'entité responsable doit disposer d'un programme de gestion des rustines qui aborde le suivi, l'évaluation et l'installation des rustines de cybersécurité. Cette exigence s'applique uniquement aux rustines de sécurité, c'est-à-dire aux correctifs publiés pour corriger une vulnérabilité particulière dans un produit matériel ou logiciel. Ainsi, elle ne concerne que les rustines permettant de corriger des problèmes de cybersécurité et exclut les rustines uniquement liées à la fonctionnalité sans répercussions sur la cybersécurité. Le suivi comprend des processus par lesquels l'entité est avisée de la disponibilité de nouvelles rustines de cybersécurité pertinentes pour les *actifs électroniques*. La documentation de la source de rustines est exigée à l'étape de suivi pour déterminer à quel moment commence la période d'évaluation. Cette exigence tient compte des situations où une rustine de sécurité peut provenir d'une première source (telle qu'un fournisseur de systèmes d'exploitation), mais qu'elle doit être approuvée ou certifiée par une autre source (telle qu'un fournisseur de systèmes de contrôle) avant de pouvoir être évaluée et appliquée sans compromettre la disponibilité ou l'intégrité du système de contrôle. La source peut prendre plusieurs formes : la « National Vulnerability Database » du NIST et les fournisseurs de systèmes d'exploitation ou de systèmes de contrôle peuvent tous être des sources pour le suivi de la publication de rustines de sécurité, de correctifs et de mises à jour. Une source de rustines n'est pas obligatoire pour les *actifs électroniques* qui n'ont pas de logiciel ou de micrologiciel actualisable (les utilisateurs ne peuvent pas mettre à jour le logiciel interne ou un micrologiciel s'exécutant sur l'*actif électronique*) ou pour lesquels il n'existe pas de source de rustines, par exemple quand le fournisseur n'existe plus. La détermination de ces sources n'est nécessaire qu'une seule fois, à moins qu'un logiciel change ou qu'il soit ajouté à la configuration de référence de l'*actif électronique*.

2.2. Les entités responsables doivent effectuer une évaluation des rustines de sécurité dans les 35 jours civils suivant leur publication par la source suivie. L'évaluation doit consister à déterminer l'applicabilité de chaque rustine à l'environnement et aux systèmes propres à l'entité. Cela consiste principalement à vérifier si la rustine s'applique à une composante logicielle ou à un composant matériel en particulier que l'entité a installé dans un *actif électronique* visé. Une rustine conçue pour un service ou un composant qui n'est pas installé dans l'environnement de l'entité n'est pas pertinente. Si l'entité détermine que la rustine est non pertinente, il lui suffit de le documenter et de le justifier pour être conforme. Si la rustine est pertinente, l'évaluation peut comprendre une détermination du risque couru, la façon de

remédier à la vulnérabilité, l'urgence et le délai de mise en œuvre de la mesure corrective, de même que les démarches déjà entreprises par l'entité ou qu'elle compte entreprendre. Lorsque des *systèmes électroniques BES* ou des *actifs électroniques BES* ne sont plus pris en charge par leurs fournisseurs, il faut faire très attention avant d'y appliquer des rustines de sécurité, des correctifs ou des mises à jour ou des mesures de neutralisation. Il est en effet possible que des rustines, des correctifs et des mises à jour réduisent la fiabilité du système, et les entités doivent en tenir compte en choisissant les mesures de neutralisation à prendre. Les entités responsables peuvent utiliser l'information fournie dans le document *Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems* du Department of Homeland Security (DHS). Le document *Recommended Practice for Patch Management of Control Systems* du DHS fournit des lignes directrices relatives au processus d'évaluation. Ce document propose des niveaux de gravité déterminés au moyen du « Common Vulnerability Scoring System » (version 2). Une exception liée à la faisabilité technique (TFE) n'est pas indiquée lorsqu'il est déterminé qu'une rustine, un correctif ou une mise à jour représente un trop grand risque pour un système ou n'est pas pertinent en raison de la configuration du système.

Au moment de documenter les mesures correctives, il n'est peut-être pas nécessaire de les consigner une par une. Le plan de mesures correctives peut être cumulatif. Par exemple, pour s'attaquer à une vulnérabilité d'un logiciel, l'entité peut choisir de désactiver un service particulier. Or, comme ce service peut être ciblé pour exploiter d'autres vulnérabilités du logiciel, sa désactivation permet de neutraliser plusieurs vulnérabilités.

2.3. Cette exigence tient compte des situations où le déploiement d'une rustine visant une vulnérabilité représente un plus grand risque pour la fiabilité d'un système en exploitation que la vulnérabilité elle-même. Dans tous les cas, l'entité a le choix soit d'installer la rustine, soit de documenter, au moyen d'un nouveau plan de mitigation ou de la mise à jour d'un plan existant, ce qu'elle entend faire pour mitiger la vulnérabilité et à quel moment elle compte le faire. Il est parfois plus judicieux, pour protéger la fiabilité, de ne pas installer une rustine, auquel cas l'entité peut consigner les mesures qu'elle a prises pour mitiger la vulnérabilité. Lorsque des rustines de sécurité sont jugées pertinentes, l'entité responsable doit, dans les 35 jours civils, les installer, créer un plan de mitigation daté qui décrit les mesures à prendre ou celles qu'elle a déjà prises pour mitiger les vulnérabilités visées par la rustine de sécurité, ou réviser un plan de mitigation existant. Le délai fixé ne doit pas nécessairement être un jour civil en particulier, mais peut être désigné par un événement comme « le prochain arrêt planifié d'au moins deux jours ». Les plans de mitigation dont il est question dans la présente norme désignent des documents internes et ne doivent pas être confondus avec les plans de mitigation soumis aux entités régionales en réponse aux non-conformités.

2.4. L'entité a été avisée d'un risque connu, l'a évalué, a mis au point un plan pour y remédier et doit ensuite mettre en œuvre ce plan. Un plan de remédiation qui comprend seulement des mesures déjà mises en œuvre est considéré comme ayant été mis en œuvre dès que la documentation du plan est terminée. Un plan de remédiation comportant des mesures à prendre pour remédier à la vulnérabilité doit être mis en œuvre selon l'échéance que l'entité a indiquée dans le plan. L'exigence ne prescrit pas de délai maximal, car l'application de correctifs et la modification des systèmes comportent leurs propres risques pour la disponibilité et l'intégrité des systèmes et peuvent devoir être reportées jusqu'au moment d'un arrêt planifié.

Lors des périodes de forte demande ou de conditions météorologiques menaçantes, la modification des systèmes peut être réduite ou refusée à cause du risque pour la fiabilité.

Exigence E3

3.1. Étant donné la vaste gamme d'équipements composant les *systèmes électroniques BES*, la grande variété des fonctions de ces équipements et de leurs vulnérabilités aux maliciels, ainsi que l'évolution constante des menaces et des outils et contrôles créés pour y faire face, il n'est pas pratique de prescrire dans la norme la façon de protéger chaque *actif électronique* contre les logiciels malveillants. L'entité responsable détermine plutôt, pour chaque *système électronique BES*, quels *actifs électroniques* sont susceptibles de subir l'intrusion de maliciels, puis documente ses plans et processus de gestion de ces risques et fournit la preuve qu'elle suit ces plans et processus. Il existe de nombreuses options : solutions antivirus habituelles pour les systèmes d'exploitation courants, listes blanches, techniques d'isolement de réseau, politiques relatives aux supports de stockage portatifs, solutions de détection et de prévention des intrusions, etc. Si une entité détient de nombreux *systèmes électroniques BES* ou *actifs électroniques* d'une architecture identique, elle peut établir un seul processus décrivant le mode de protection de tous les *actifs électroniques* semblables. Si un *actif électronique* particulier n'a pas de logiciel actualisable et que son code exécutable ne peut être modifié, cet *actif électronique* est considéré comme doté de sa propre méthode interne de protection contre les programmes malveillants.

3.2. Lorsqu'un programme malveillant est détecté sur un *actif électronique* dans le cadre de l'application de cette exigence, la menace posée par ce programme doit être mitigée. Dans les situations où les programmes antivirus habituels sont utilisés, ceux-ci peuvent être configurés de manière à supprimer automatiquement ou à mettre en quarantaine les programmes malveillants. Dans les cas où des listes blanches sont utilisées, l'outil lui-même peut mitiger la menace en empêchant le programme de s'exécuter, mais d'autres mesures doivent être prises pour supprimer le programme malveillant de l'*actif électronique*. Dans certains cas, il est préférable, pour protéger la fiabilité, de ne pas supprimer ou mettre en quarantaine immédiatement le programme malveillant, par exemple si la disponibilité du système risque d'être compromise lorsque le programme malveillant est supprimé pendant que le système fonctionne et qu'il faut planifier une reconstruction du système. Il est alors possible d'accroître la surveillance et de prendre des mesures pour s'assurer que le programme malveillant ne puisse communiquer avec d'autres systèmes. Dans d'autres cas, l'entité peut collaborer avec la police ou d'autres organisations gouvernementales pour surveiller étroitement le programme et dépister l'intrus. C'est pour ces raisons qu'il n'y a pas de délai maximal ou de méthode prescrite en vue de la suppression d'un programme malveillant ; l'exigence est plutôt de mitiger la menace posée par le programme malveillant qui a été identifié.

3.3. Lorsque les technologies de détection de maliciels dépendent de signatures ou de séquences de code connues, leur efficacité pour protéger les systèmes contre des nouvelles menaces est liée à la capacité de tenir ces signatures et séquences à jour. L'entité doit disposer d'un processus documenté qui prévoit la vérification et l'installation des mises à jour des signatures ou des séquences de code. Dans un *système électronique BES*, certains *actifs électroniques* pourraient bénéficier de l'installation plus rapide des mises à jour, la disponibilité

de ces actifs ne compromettant pas la disponibilité ou le fonctionnement du système électronique BES. Par exemple, certains postes de travail disposant d'une interface personne-machine faisant appel à des supports portatifs pourraient bénéficier des plus récentes mises à jour en tout temps, avec un minimum de vérification. Sur d'autres *actifs électroniques*, les mises à jour devraient être vérifiées intégralement avant la mise en œuvre, car un résultat « faux positif » pourrait nuire à la disponibilité du *système électronique BES*. La vérification ne doit pas avoir un impact négatif sur la fiabilité du BES. Elle doit être axée sur la mise à jour elle-même et sur le risque qu'elle nuise au *système électronique BES*. La vérification n'implique en aucun cas qu'une entité doive s'assurer qu'un logiciel malveillant est détecté s'il est introduit dans le système. Elle vise uniquement à faire en sorte que l'entité s'assure, avant d'installer une mise à jour, qu'elle n'aura pas d'incidence négative sur le *système électronique BES*.

Exigence E4

Consulter les publications NIST 800-92 et 800-137 pour des directives supplémentaires sur la surveillance des événements de sécurité.

4.1. Dans le contexte d'environnements informatiques complexes confrontés à des menaces et à des vulnérabilités qui ne cessent d'évoluer, il n'est pas pratique que la norme énumère tous les événements de sécurité justifiant une alerte ou une intervention en cas d'incident. L'entité responsable détermine plutôt quels événements informatiques doivent être journalisés et doivent faire l'objet d'alertes et d'un suivi compte tenu de leur *système électronique BES* particulier.

Les événements de sécurité précis déjà visés par la version 4 des normes CIP sont reportés dans cette version. Ils comprennent les tentatives d'accès aux *points d'accès électroniques* qui auraient été répertoriées pour un *système électronique BES*, par exemple : (i) tentatives bloquées d'accès au réseau, (ii) tentatives d'accès d'utilisateurs distants, qu'elles aient réussi ou échoué, (iii) tentatives bloquées d'accès au réseau à partir d'un VPN distant et (iv) tentatives réussies d'accès au réseau ou d'obtention d'information sur les flux dans le réseau.

Les événements associés aux accès et aux activités des utilisateurs sont notamment générés par les *actifs électroniques* situés à l'intérieur du *périmètre de sécurité électronique* et ayant la capacité de contrôler les accès. Ces types d'événements comprennent : (i) l'authentification ayant réussi ou échoué, (ii) la gestion des comptes, (iii) l'accès aux objets et (iv) les processus entrepris et interrompus.

L'intention du SDT n'est pas qu'une TFE soit générée si un dispositif ne peut journaliser un événement en particulier. Son intention est plutôt que l'entité journalise tous les éléments de la liste à puces (fermeture de session par les utilisateurs, par exemple) que le dispositif est en mesure de journaliser. Si le dispositif n'a pas la capacité de journaliser un événement, l'entité demeure conforme.

4.2. Les alertes en temps réel permettent au système électronique de communiquer automatiquement des événements importants aux intervenants désignés. Cela nécessite la configuration d'un mécanisme de communication et l'établissement de règles d'analyse des journaux. Les alertes peuvent être configurées sous forme de courriels, de messages texte ou d'affichages et d'alarmes directement sur le système. Les règles d'analyse des journaux peuvent

exister à l'intérieur du système d'exploitation, d'une application spécifique ou d'un système centralisé de surveillance des événements de sécurité. À un bout du spectre, une alerte en temps réel peut être un simple réglage sur une station terminale en cas d'échec d'ouverture de session et, à l'autre bout, un système de surveillance des événements de sécurité proposant de multiples options de communication d'alertes déclenchées par des règles complexes de corrélation des journaux.

Les événements déclencheurs d'alertes en temps réel peuvent être modifiés avec le temps à mesure que les administrateurs de système et les intervenants en cas d'incident apprennent à mieux reconnaître les types d'événements pouvant signaler un incident de cybersécurité. Il faut configurer les alertes en tenant compte de la nécessité de prévenir les intervenants quand un événement se produit tout en évitant un accroissement indu du nombre des fausses alertes. La liste suivante comprend des exemples d'événements dont une entité responsable doit tenir compte lors de la configuration des alertes en temps réel :

- détection de maliciels ou d'activités malveillantes connus ou potentiels ;
- défaillance des mécanismes de journalisation des événements de sécurité ;
- échecs d'ouverture de session pour des comptes critiques ;
- ouverture de session interactive sur des comptes système ;
- activation de comptes ;
- utilisation de comptes nouvellement attribués ;
- tâches de gestion ou de modification de système effectuées par un utilisateur non autorisé ;
- tentatives d'authentification sur certains comptes en dehors des heures ouvrables ;
- changements de configuration non autorisés ;
- insertion d'un support amovible en infraction à une politique.

4.3 Les journaux créés conformément à la partie 4.1 doivent être conservés sur les *actifs électroniques* ou les *systèmes électroniques BES* visés pendant au moins 90 jours. Cette période est différente de la période de conservation des pièces justificatives exigée dans les normes CIP afin de prouver la conformité historique d'une entité. Pour les fins d'audit, l'entité doit conserver une pièce justificative indiquant qu'elle a conservé les journaux portant sur 90 jours (par exemple, des preuves de l'élimination de journaux d'événements datant de plus de 90 jours avant la période de conservation des pièces justificatives).

4.4. L'examen des journaux au moins tous les 15 jours (environ toutes les deux semaines) peut consister dans l'analyse d'un résumé ou d'un échantillon d'événements journalisés. La publication spéciale SP800-92 du NIST contient beaucoup de conseils sur l'analyse périodique des journaux. Si un système centralisé de surveillance des événements de sécurité est employé, l'analyse des journaux peut être une analyse descendante commençant par un examen des tendances tirées des rapports sommaires. L'examen des journaux peut aussi être un prolongement de l'exercice consistant à repérer les événements nécessitant des alertes en temps réel selon lequel on analyserait les événements qui ne sont pas parfaitement compris ou qui pourraient provoquer d'innombrables alertes en temps réel.

Exigence E5

Les types de comptes dont il est question dans cette exigence comprennent les suivants :

- Compte utilisateur partagé : compte employé par plusieurs utilisateurs – employés ou des entrepreneurs – dans le cours normal des activités. Il se trouve habituellement sur un dispositif qui ne prend pas en charge les comptes d'utilisateurs individuels.
- Compte d'utilisateur individuel : compte employé par un seul utilisateur.
- Compte administratif : compte comportant des droits d'accès élargis permettant d'exécuter des fonctions administratives ou d'autres fonctions spécialisées. Le compte peut être individuel ou commun.
- Compte système : compte utilisé pour exécuter des services sur un système (Web, DNS, courriel, etc.). Aucun utilisateur n'a accès à ce type de compte.
- Compte d'application : compte système particulier comportant des droits d'accès accordés au niveau de l'application, souvent utilisé pour accéder à une base de données.
- Compte d'invité : compte d'utilisateur individuel qui n'est pas habituellement utilisé par des employés ou des entrepreneurs pour l'exécution de leurs tâches normales et qui n'est pas associé à un utilisateur particulier. Peut être partagé ou non par plusieurs utilisateurs.
- Compte d'accès distant : compte d'utilisateur individuel utilisé uniquement pour obtenir un accès distant interactif au *système électronique BES*.
- Compte générique : compte de groupe établi par le système d'exploitation ou par l'application pour la réalisation de certaines tâches. Diffère d'un compte utilisateur commun en ce que les utilisateurs individuels ne reçoivent pas l'autorisation d'accéder à ce type de compte.

5.1 Voir la justification de l'exigence.

5.2 Dans la mesure du possible, les comptes par défaut et autres comptes génériques définis par un fournisseur doivent être retirés, renommés ou désactivés avant la mise en service de l'*actif électronique* ou du *système électronique BES*. Si ce n'est pas possible, les mots de passe par défaut doivent être changés. Tout compte par défaut ou autre compte générique qui demeure activé doit être documenté. Pour les configurations courantes, on peut procéder à cette documentation au niveau du *système électronique BES* ou à un niveau plus général.

5.3 Les entités peuvent choisir de désigner des personnes ayant accès aux comptes communs par l'entremise du processus d'autorisation et de fourniture d'accès, auquel cas les registres d'autorisations individuelles suffisent pour assurer la conformité à cette partie de l'exigence. Les entités peuvent aussi choisir de tenir une liste distincte pour les comptes communs. Les deux formes de preuves sont conformes au résultat visé, soit conserver le contrôle des comptes communs.

5.4. Les mots de passe par défaut sont souvent publiés dans la documentation que les fournisseurs offrent à tous les clients utilisant ce type d'équipement et qu'ils diffusent parfois en ligne.

La possibilité de mots de passe exclusifs est précisée dans l'exigence pour les cas où l'*actif électronique* génère ou attribue des mots de passe par défaut pseudo-aléatoires au moment de la mise en service ou de l'installation. Il n'est alors pas nécessaire de changer le mot de passe par défaut parce que le système ou le fabricant l'a créé exclusivement pour l'*actif électronique*.

5.5. L'accès utilisateur interactif exclut l'accès à de l'information en lecture seule pour lequel la configuration de l'*actif électronique* ne peut être changée (afficheur intégré, rapports Web, etc.). Si un dispositif n'est pas en mesure d'assurer l'authentification, pour des raisons techniques ou opérationnelles, l'entité doit démontrer que tous les chemins d'accès utilisateur interactif distants et locaux sont configurés de manière à assurer l'authentification. La sécurité physique est suffisante comme configuration des accès locaux si elle est en mesure d'enregistrer l'identité des personnes qui se trouvent dans le *périmètre de sécurité physique* à tout moment.

Les moyens techniques ou procéduraux sont requis pour imposer les paramètres de mot de passe lorsque le mot de passe est le seul justificatif d'authentification des personnes. Les moyens techniques s'appliquent aux *actifs électroniques* qui vérifient que le mot de passe choisi par une personne est conforme aux paramètres obligatoires avant de permettre l'authentification au moyen de ce mot de passe. Ils devraient être employés dans la plupart des cas où l'*actif électronique* le permet. Quant aux moyens procéduraux, il s'agit de procédures exigeant le respect des paramètres obligatoires ; ainsi, les personnes choisissant un mot de passe ont l'obligation de s'assurer qu'il est conforme aux paramètres obligatoires.

La complexité des mots de passe désigne la politique selon laquelle un *actif électronique* exige qu'un mot de passe comporte un ou plusieurs des types de caractères suivants : (1) lettres minuscules, (2) lettres majuscules, (3) caractères numériques et (4) caractères non alphanumériques ou spéciaux (#, $, @, &, etc.), selon diverses combinaisons.

5.6 Les moyens techniques ou procéduraux sont requis pour imposer le changement de mot de passe lorsque le mot de passe est le seul justificatif d'authentification des personnes. Les moyens techniques s'appliquent aux *actifs électroniques* qui exigent le changement du mot de passe après une période donnée avant d'autoriser l'accès. Dans ce cas, il n'est pas nécessaire de changer le mot de passe avant la fin de cette période pourvu que l'*actif électronique* exige le changement du mot de passe après la première authentification réussie du compte au-delà de cette période. Les moyens procéduraux signifient le changement manuel des mots de passe servant à l'accès utilisateur interactif à une fréquence donnée.

5.7 Le blocage des comptes ou la génération d'alertes après un certain nombre d'échecs d'authentification sert à prévenir les accès non autorisés au moyen d'une attaque de craquage de mots de passe perpétrée en ligne. Le seuil du nom re d'échecs doit être assez haut pour éviter les faux positifs imputables à des utilisateurs autorisés qui ne réussissent pas à s'authentifier, mais assez bas pour contrer les attaques s'étendant sur une longue période. Il

peut être ajusté à l'environnement d'exploitation au fil du temps afin d'éviter les blocages de compte non nécessaires.

Les entités doivent faire attention, en configurant le blocage de comptes, d'éviter de bloquer les comptes nécessaires au *système électronique BES* pour une tâche assurant la fiabilité du BES. Dans un tel cas, il faut plutôt configurer la génération d'alertes en cas d'échec d'authentification.

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 :

Cette exigence a pour but une réduction au minimum de la surface d'attaque des *systèmes électroniques BES* soit par la désactivation des ports d'entrée-sortie physiques et des services et ports logiques non nécessaires accessibles par le réseau, soit par une restriction de l'accès à ces ports et services.

Sommaire des modifications : La formulation « nécessaires aux activités normales et aux activités d'urgence » a été remplacée par « les ports nécessaires ». La mention des ports d'entrée-sortie physiques a été ajoutée en réponse à une ordonnance de la FERC. Les ports physiques non nécessaires dans les *centres de contrôle*, soit les zones présentant le risque le plus élevé et ayant le plus grand impact, doivent aussi être protégés.

Référence à une version précédente : (Partie 1.1) CIP-007-4, E2.1 et E2.2

Justification de la modification : (Partie 1.1)

Cette exigence est axée sur le fait que l'entité sait quels ports sont nécessaires et n'active que ceux-ci. La classification supplémentaire « activités normales ou activités d'urgence » n'ajoutait aucune valeur et a été supprimée.

Référence à une version précédente : (Partie 1.2) Nouveau

Justification de la modification : (Partie 1.2)

Le 18 mars 2010, la FERC a publié une ordonnance approuvant l'interprétation par la NERC de l'exigence E2 de la norme CIP-007-2. Dans cette ordonnance, la FERC admettait que le terme « ports » dans « ports et services » désigne les ports de communication logiques (p. ex. ports TCP-IP), mais encourageait aussi l'équipe de rédaction à se pencher sur le sujet des ports physiques inutilisés.

Raisonnement pour E2 :

La gestion des rustines de sécurité est un moyen proactif utilisé pour faire le suivi des vulnérabilités connues en matière de sécurité et pour corriger celles-ci avant qu'elles ne puissent être exploitées de manière malveillante en vue de prendre le contrôle d'un *actif électronique BES* ou d'un *système électronique BES* ou de le rendre hors d'état de fonctionner.

Pour le maintien de la fiabilité du BES, le plan de mesures correctives peut être mis à jour au besoin, y compris une explication de tout changement à la planification des mesures.

Sommaire des modifications : Les exigences E3, E3.1 et E3.2 de la version précédente de la norme CIP-007 ont été séparées en exigences individuelles pour une plus grande granularité ou

précision. La documentation des sources pour le suivi des rustines de sécurité, des correctifs et des mises à jour des *systèmes électroniques BES* ou *actifs électroniques BES* a été ajoutée comme contexte relatif à la date de publication. La formulation « consigner dans les 30 jours civils suivant leur disponibilité, l'évaluation des rustines de sécurité et des mises à jour de sécurité pour déterminer si elles doivent être déployées » prêtait à confusion quant à la date de disponibilité. Étant donné les enjeux possibles concernant les ententes de service et les accords de licence des fournisseurs des systèmes de contrôle, les entités responsables doivent disposer d'une marge de manœuvre afin de définir les sources à utiliser pour le suivi relatif aux *actifs électroniques BES*.

Référence à une version précédente : (Partie 2.1) CIP-007, E3

Justification des modifications : (Partie 2.1)

Cette exigence découle des versions précédentes des normes CIP, auxquelles s'ajoute la définition de la ou des sources qu'une entité responsable utilise pour faire le suivi de la publication de rustines de sécurité. La documentation des sources est utile pour déterminer à quel moment commence la période d'évaluation. Cette exigence tient également compte des situations où des rustines de sécurité peuvent provenir d'une source originale (telle que le fournisseur d'un système d'exploitation), mais doivent être approuvées ou certifiées par une autre source (telle que le fournisseur d'un système de contrôle) avant de pouvoir être évaluées et appliquées sans compromettre la disponibilité ou l'intégrité du système de contrôle.

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

Justification des modifications : (Partie 2.2)

Libellé semblable au libellé actuel, mais comportant en outre « par la ou les sources indiquées à la partie 2.1 » afin de clarifier le délai de 35 jours.

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

Justification des modifications : (Partie 2.3)

Cette exigence a été modifiée pour tenir compte des situations où la correction d'une vulnérabilité représente un plus grand risque pour la fiabilité d'un système en exploitation que la vulnérabilité elle-même. Dans tous les cas, l'entité documente, soit par la création d'un nouveau plan de neutralisation, soit par la mise à jour d'un plan existant, ce qu'elle entend faire pour neutraliser la vulnérabilité et à quel moment elle le fera. Le plan de neutralisation peut simplement consister à installer la rustine. Cependant, il est parfois plus judicieux, pour protéger la fiabilité, de ne pas installer une rustine, auquel cas l'entité peut consigner les mesures qu'elle a prises pour neutraliser la vulnérabilité.

Référence à une version précédente : (Partie 2.4) CIP-007, E3.2

Justification des modifications : (Partie 2.4)

Libellé semblable au libellé actuel, comportant en outre la mention que le plan doit être mis en œuvre dans le délai précisé dans le plan ou dans un plan révisé approuvé par le *cadre supérieur CIP* ou son délégué.

Raisonnement pour E3 :

La protection contre les programmes malveillants consiste à détecter et à limiter l'ajout de programmes malveillants aux *actifs électroniques* visés d'un *système électronique BES*. Ces programmes (virus, vers, réseaux de zombies, code ciblé tel que Stuxnet, etc.) peuvent compromettre la disponibilité ou l'intégrité d'un *système électronique BES*.

Sommaire des modifications : Dans les versions précédentes, cette exigence a probablement produit le plus grand nombre d'exceptions liées à la faisabilité technique (TFE), car elle prescrivait l'utilisation d'une technologie particulière sur tous les CCA, peu importe la vulnérabilité de cet actif ou sa capacité à utiliser la technologie en question. Comme la portée des *actifs électroniques* visés par ces normes s'étend à un plus grand nombre d'actifs sur le terrain, cet enjeu ne fera que croître de façon exponentielle. L'équipe de rédaction a décidé de fonder cette exigence sur les compétences, c'est-à-dire que l'entité doit documenter le mode de gestion des risques liés aux programmes malveillants pour chaque *système électronique BES* ; toutefois, l'équipe ne prescrit pas une méthode technique particulière ni l'obligation de l'utiliser sur chaque *actif électronique*. Ce sont les *systèmes électroniques BES* qui font l'objet de la protection.

Dans l'ordonnance 706 de la FERC, paragraphes 619 à 622, plus particulièrement au paragraphe 621, la FERC admet que la norme « ne prescrit pas une seule méthode… Toutefois, la méthode utilisée par l'entité responsable devrait être détaillée dans sa politique sur la cybersécurité afin qu'elle puisse faire l'objet d'un audit de conformité…»

Au paragraphe 622, la FERC ordonne de modifier l'exigence en ajoutant des mesures de protection contre l'introduction malveillante ou accidentelle par le personnel de virus ou d'autres programmes malveillants par l'intermédiaire de l'accès à distance, de supports électroniques ou d'autres moyens. L'équipe de rédaction est d'avis que l'examen de cette question à un niveau global, c'est-à-dire au niveau des *systèmes électroniques BES* et indépendamment de la technologie, ainsi que les exigences accrues en matière de gestion du changement, respecte cette directive.

Référence à une version précédente : (Partie 3.1) CIP-007-4, E4 ; CIP-007-4, E4.1

Justification des modifications : (Partie 3.1)

Voir le sommaire des modifications apportées. L'ordonnance 706 de la FERC, paragraphe 621, établit que le processus d'élaboration des normes devrait déterminer le degré de description de la protection des *systèmes électroniques BES* contre l'introduction de programmes malveillants par le personnel.

Référence à une version précédente : (Partie 3.2) CIP-007-4, E4 ; CIP-007-4, E4.1

Justification des modifications : (Partie 3.2)

Voir le sommaire des modifications.

Référence à une version précédente : (Partie 3.3) CIP-007-4, E4 ; CIP-007-4, E4.2

Justification des modifications : (Partie 3.3)

Ces exigences demeurent essentiellement inchangées par rapport aux versions précédentes ; la mise à jour a pour but de faire référence aux parties antérieures du tableau des exigences.

Raisonnement pour E4 :

La surveillance des événements de sécurité a pour but la détection des accès non autorisés, des activités de reconnaissance et d'autres actes malveillants ciblant les *systèmes électroniques BES*. Elle comprend les activités liées à la constitution, au traitement et à la conservation des journaux de sécurité ainsi que les alertes. Ces journaux peuvent à la fois (1) permettre la détection d'un incident et (2) fournir une preuve utile à l'enquête sur un incident. La conservation des journaux de sécurité est destinée à étayer l'analyse des données post-événement.

Cette exigence ne pénalise pas les échecs de journalisation ; elle précise plutôt les processus à mettre en place pour surveiller les échecs de journalisation et en aviser le personnel.

Sommaire des modifications : À partir des paragraphes 525 et 628 de son ordonnance 706, la FERC demande que l'examen manuel des journaux d'événements de sécurité soit effectué plus régulièrement. La présente exigence combine l'exigence E5 de la norme CIP 005-4 et l'exigence E6 de la norme CIP 007-4 dans une perspective globale. Le principal commentaire reçu à propos de cette exigence au cours de la période de consultation informelle portait sur l'imprécision des termes « événement de sécurité » et « surveillance ».

Les termes « événement de sécurité » et « événements touchant la cybersécurité » sont problématiques parce qu'ils ne s'appliquent pas systématiquement à l'ensemble des plateformes et des applications. Pour clarifier ce terme, le libellé de l'exigence est semblable à celui de la publication 800 53 du NIST, en ce que l'entité doit définir les événements de sécurité pertinents pour le système. Pour quelques événements, il est indiqué explicitement que si un *actif électronique* ou un *système électronique BES* peut les journaliser, alors il doit le faire.

En outre, cette exigence établit des paramètres de surveillance et d'examen des processus. Il est rarement faisable ou productif d'examiner chaque journal des événements de sécurité d'un système. Cette réalité est prise en considération dans le paragraphe 629 de l'ordonnance 706 de la FERC, où un examen manuel des journaux est prescrit. Par conséquent, selon cette exigence, l'examen manuel peut consister en un échantillonnage ou en un résumé des événements de sécurité survenus depuis le dernier examen.

Référence à une version précédente : (Partie 4.1) CIP-005-4, E3 ; CIP-007-4, E5, E5.1.2, E6.1 et E6.3

Justification de la modification : (Partie 4.1)

Cette exigence est dérivée de l'alinéa AU-2 de la publication 800-53, version 3, du NIST, qui oblige les organisations à déterminer quels événements systèmes journaliser à des fins d'intervention en cas d'incident. Selon les commentaires officieux reçus au sujet de la norme CIP-011, l'industrie a indiqué une certaine confusion face au terme « événements systèmes touchant la cybersécurité ». Les journaux des accès de l'ESP prescrits à l'exigence E3 de la

norme CIP-005-4 et les journaux des accès et des activités des utilisateurs prescrits à l'exigence E5 de la norme CIP-007-5 sont également visés ici.

Référence à une version précédente : (Partie 4.2) CIP-005-4, E3.2 ; CIP-007-4, E6.2

Justification de la modification : (Partie 4.2)

Cette exigence est dérivée des exigences relatives aux alertes, soit l'exigence E3.2 de la norme CIP-005-4 et l'exigence E6.2 de la norme CIP-007-4, en plus de l'alinéa AU-6 de la publication 800-53, version 3, de la NIST. Les versions antérieures des normes CIP exigeaient des alertes en cas de tentatives d'accès non autorisé et de détection d'*incidents de cybersécurité*, qui peuvent être très nombreux et difficiles à déterminer au jour le jour. Les modifications à cette exigence permettent à l'entité de déterminer quels événements nécessitent une intervention.

Référence à une version précédente : (Partie 4.3) CIP-005-4, E3.2 ; CIP-007-4, E6.4

Justification des modifications : (Partie 4.3)

Aucune modification importante.

Référence à une version précédente : (Partie 4.4) CIP-005-4, E3.2 ; CIP-007-4, E6.5

Justification de la modification : (Partie 4.4)

À partir des paragraphes 525 et 628 de son ordonnance 706, la FERC demande que l'examen manuel des journaux des événements de sécurité soit effectué plus régulièrement et suggère un examen hebdomadaire. Dans cette ordonnance, la FERC reconnaît qu'il est rarement faisable d'examiner tous les journaux systèmes. En effet, l'examen des journaux est un processus dynamique qui doit s'améliorer avec le temps et à la lumière de nouveaux renseignements sur les menaces. Selon les modifications à la présente exigence, un examen d'un résumé ou d'un échantillon des journaux peut être effectué environ toutes les deux semaines.

Raisonnement pour E5 :

Faire en sorte qu'aucune personne autorisée ne puisse obtenir un accès électronique à un *système électronique BES* à moins d'être authentifiée, c'est-à-dire sans que ses renseignements d'authentification n'aient été validés. L'exigence E5 cherche aussi à réduire le risque que des mots de passe statiques utilisés comme facteur d'authentification soient compromis.

L'exigence 5.1 vise à assurer que tout *système électronique BES* et tout *actif électronique* authentifie les personnes pouvant modifier l'information de configuration. Cette exigence porte notamment sur la configuration de l'authentification. L'autorisation des personnes est aussi abordée ailleurs dans les normes CIP sur la cybersécurité. L'accès utilisateur interactif exclut l'accès à de l'Information en lecture seule pour lequel la configuration de l'*actif électronique* ne peut être changée (afficheur intégré, rapports Web, etc.). Si un dispositif n'est pas en mesure d'assurer l'authentification, pour des raisons techniques ou opérationnelles, l'entité doit démontrer que tous les chemins d'accès utilisateur interactif distants et locaux sont configurés

de manière à assurer l'authentification. La sécurité physique est suffisante comme configuration des accès locaux si elle est en mesure d'enregistrer l'identité des personnes qui se trouvent dans le *périmètre de sécurité physique* à tout moment.

L'exigence 5.2 porte sur les comptes par défaut et autres comptes génériques. Le fait que l'entité consigne quelle l'utilisation est faite des comptes par défaut et autres comptes génériques pouvant causer des vulnérabilités a l'avantage de faire en sorte qu'elle comprenne le risque éventuel représenté par ces comptes pour le *système électronique BES*. Cette partie d'exigence évite de prescrire une intervention sur ces comptes parce que la solution la plus efficace dépend de chaque situation et que la suppression ou la désactivation du compte pourrait nuire à la fiabilité.

L'exigence 5.3 porte sur les personnes ayant accès aux comptes communs. L'objectif est de neutraliser le risque d'accès non autorisé par l'intermédiaire de comptes communs. Cette exigence est différente de celles d'autres normes CIP sur la cybersécurité visant l'autorisation de l'accès. Une entité peut autoriser l'accès sans savoir qui a accès à un compte partagé. L'entité qui n'aurait pas la liste des personnes ayant accès aux comptes communs pourrait difficilement retirer ces droits d'accès à quiconque n'en a plus besoin. Le terme « autorisé » est employé dans l'exigence pour préciser que le fait qu'une personne enregistre ou perde un mot de passe ou qu'elle le partage sans autorisation ne constitue pas une non-conformité en vertu de cette exigence.

L'exigence 5.4 porte sur les mots de passe par défaut. Leur modification élimine une vulnérabilité facilement exploitable de nombreux systèmes et applications. Les mots de passe pseudo-aléatoires générés par le système ne sont pas considérés comme des mots de passe par défaut.

En ce qui concerne l'authentification des utilisateurs par mot de passe, l'utilisation de mots de passe forts et leur modification périodique contribuent à atténuer le risque de réussite des attaques de craquage de mots de passe ainsi que le risque de divulgation accidentelle de mots de passe à des personnes non autorisées. L'équipe de rédaction a envisagé plusieurs approches pour rendre cette exigence assez efficace et flexible pour permettre aux entités responsables de prendre les bonnes décisions en matière de sécurité. L'une des approches envisagées consistait à exiger une entropie minimale pour les mots de passe ; or, le calcul de la véritable entropie d'information est beaucoup plus complexe et se fonde sur plusieurs hypothèses concernant le choix de mots de passe par les utilisateurs. Ces derniers peuvent choisir des mots de passe faibles dont l'entropie est nettement inférieure au minimum calculé.

L'équipe de rédaction a aussi choisi de ne pas exiger d'exceptions liées à la faisabilité technique pour les dispositifs qui ne respectent pas les paramètres de longueur et de complexité des mots de passe. L'objectif de cette exigence est d'appliquer une politique de mot de passe mesurable afin de prévenir les tentatives de craquage ; le remplacement de dispositifs simplement pour respecter une politique précise sur les mots de passe n'atteint pas cet objectif. Cependant, l'exigence a été renforcée de manière à exiger le verrouillage de comptes ou la génération d'alertes en cas d'échec d'ouverture de session, ce qui permet généralement de mieux atteindre l'objectif visé.

L'exigence de changement des mots de passe permet de contrer la situation où une tentative de craquage aurait réussi à déceler un mot de passe chiffré, ainsi que de remplacer tout rafraîchir tous les mots de passe qui auraient été divulgués accidentellement au fil du temps. L'exigence donne à l'entité le loisir de préciser quelle fréquence de changement des mots de passe permet d'atteindre l'objectif. En particulier, l'équipe de rédaction a jugé plus efficace que la fréquence soit déterminée en fonction de plusieurs facteurs plutôt que d'être fixée pour tous les *systèmes électroniques BES* visés par la norme. En général, les mots de passe servant à l'authentification des utilisateurs doivent être changés au moins une fois par année. Cette fréquence peut parfois être réduite : ainsi, des mots de passe d'applications longs et pseudo-aléatoires pourraient être changés très peu fréquemment. Par ailleurs, les mots de passe employés uniquement comme méthode d'authentification faible d'une application (par exemple, l'accès à la configuration d'un relais) pourraient n'être changés que dans le cadre de l'entretien de routine.

L'*actif électronique* doit appliquer automatiquement la politique sur les mots de passe aux comptes d'utilisateurs individuels. Toutefois, dans le cas des comptes communs pour lesquels il n'existe aucun mécanisme d'application de la politique sur les mots de passe, l'entité responsable peut recourir à des procédures ainsi qu'à une évaluation interne et à un audit.

L'exigence 5.7 aide à prévenir les attaques perpétrées en ligne visant les mots de passe en limitant le nombre de tentatives possible. Il s'agit soit de limiter le nombre de tentatives d'authentification, soit de générer une alerte après un certain nombre d'échecs. Les entités doivent user de prudence avant de limiter le nombre de tentatives d'authentification pour tous les comptes, car cela peut ouvrir la possibilité d'une attaque par déni de service visant le *système électronique BES*.

Sommaire des modifications (par rapport à E5) :

L'exigence E5.3 de la norme CIP 007-4 prescrit l'utilisation de mots de passe et précise une politique d'au moins six caractères combinant caractères alphanumériques et autres. Le niveau de détail dans ces exigences peut par contre limiter le recours à des mesures de sécurité plus efficaces. Ainsi, plusieurs l'ont interprété comme s'appliquant aux mots de passe de jetons ou de systèmes biométriques, ce qui a pu empêcher le recours à ces formes d'authentification plus fortes. En outre, l'utilisation de mots de passe plus longs peut réduire la nécessité d'imposer des règles de complexité. Les exigences relatives aux mots de passe ont été modifiées afin de permettre à l'entité de préciser les paramètres les plus efficaces en fonction de l'impact du *système électronique BES*, du mode d'utilisation des mots de passe et de leur importance pour restreindre l'accès au système. Le SDT croit que ces modifications renforcent le mécanisme d'authentification en obligeant les entités à se pencher sur la façon d'utiliser les mots de passe qui soit la plus efficace dans leur environnement. En effet, l'imposition d'une politique stricte relative aux mots de passe peut limiter l'efficacité des mécanismes de sécurité et empêcher la mise en place de meilleurs mécanismes à l'avenir.

Référence à une version précédente : (Partie 5.1) CIP-007-4, E5

Justification des modifications : (Partie 5.1)

L’exigence d’imposer l’authentification pour tout accès par un utilisateur est incluse ici. L’exigence d’établir, de mettre en œuvre et de documenter les contrôles est incluse dans cette exigence d’introduction. L’exigence d’avoir des contrôles techniques et procéduraux a été supprimée parce que les contrôles techniques sont suffisants lorsqu’une documentation des procédures est déjà exigée. L’expression « qui minimisent les risques d’un accès non autorisé » a été supprimée et est rendue plus adéquatement dans la justification de l’exigence E5.

Référence à une version précédente : (Partie 5.2) CIP-007-4, E5.2 et E5.2.1

Justification des modifications : (Partie 5.2)

La norme CIP-007-4 oblige les entités à limiter l’étendue et à encadrer l'utilisation admise des droits attachés aux comptes. L’exigence de limiter les droits attachés aux comptes a été supprimée parce que la mise en œuvre d’une telle politique est difficile à mesurer.

Référence à une version précédente : (Partie 5.3) CIP-007-4, E5.2.2

Justification des modifications apportées : (Partie 5.3)

Aucune modification importante. Le mot « autorisés » a été ajouté à « accès » pour préciser clairement que le fait qu’une personne enregistre ou perde un mot de passe ou qu’elle le partage sans autorisation ne constitue pas une non-conformité en vertu de cette exigence.

Référence à une version précédente : (Partie 5.4) CIP-007-4, E5.2.1

Justification des modifications : (Partie 5.4)

L’exigence portant sur « le retrait, la désactivation ou le changement de nom des comptes, lorsque cela est possible » a été supprimée et intégrée à une directive sur l’utilisation acceptable des types de comptes. Cette exigence a été supprimée parce que ces actions ne conviennent pas à tous les types de comptes. Ajout de la possibilité de mots de passe par défaut exclusifs pour les cas où un système a généré un mot de passe par défaut ou les cas où un mot de passe par défaut fixe a été figé dans le code au moment de la fabrication du *système électronique BES*.

Référence à une version précédente : (Partie 5.5) CIP-007-4, E5.3

Justification des modifications : (Partie 5.5)

L’exigence E5.3 de la norme CIP-007-4 prescrit l’utilisation de mots de passe et une politique d’une combinaison d’au moins six caractères alphanumériques et spéciaux. Le niveau de détail dans ces exigences peut par contre limiter le recours à des mesures de sécurité plus efficaces. Les exigences relatives aux mots de passe ont été modifiées afin d’autoriser le maximum alloué par le dispositif dans les cas où les paramètres de mot de passe ne permettent pas d’observer une politique plus stricte. Grâce à cette modification, il est tout de même possible d’atteindre l’objectif de l’exigence – réduire le risque de divulgation non autorisée des justificatifs d’identité des mots de passe – tout en reconnaissant que les paramètres de mot de passe seuls ne sont pas suffisants pour y parvenir. L’équipe de rédaction était convaincue que le fait de laisser à l’entité responsable la possibilité d’appliquer la politique de mot de passe la plus stricte permise par un dispositif surpassait la nécessité de surveiller un contrôle plus ou moins efficace au moyen du recours aux TFE.

Référence à une version précédente : (Partie 5.6) CIP-007-4, E5.3.3

Justification des modifications : (Partie 5.6)

*Initialement l'exigence E5.5.3, elle a été déplacée pour permettre l'ajout de « à connectivité externe routable » après « à impact moyen » en réponse aux commentaires. Cette exigence a une portée limitée parce que le risque d'une attaque sur les mots de passe en provenance du réseau est amoindri par l'absence de connectivité externe routable. Le changement fréquent du mot de passe des actifs sur le terrain peut nécessiter un effort important tout en ne réduisant pas beaucoup le risque.

Référence à une version précédente : (Partie 5.7) Nouvelle exigence

Justification des modifications : (Partie 5.7)

La réduction au minimum du nombre des tentatives d'ouverture de session diminue considérablement le risque lié aux tentatives de craquage en temps réel des mots de passe. Dans de telles situations, ce contrôle est plus efficace que les paramètres de mot de passe.

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 suveillance 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	Modifications visant à ajouter des critères spécifiques 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-007-5 (L'ordonnance entre en vigueur le 3 février 2014)	

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

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe aura préséance.

A. Introduction

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

   Entités fonctionnelles

   Aucune disposition particulière

   Installations

   La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

   Exemptions additionnelles

   Sont exemptés de l'application de la présente norme :

   - Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur un réseau voisin.
   - Postes élévateurs des installations de production identifiées au point précédent.

5. **Date d'entrée en vigueur au Québec :**

   5.1. Adoption de la norme par la Régie de l'énergie : xx mois 201x

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

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

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

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

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

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

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

A. Introduction

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

2. Numéro : CIP-008-5

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

4. Applicabilité :

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

4.1.1 Responsable de l'équilibrage

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

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

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

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

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

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

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

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

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

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

4.2.1.1 Chaque système de DSF ou de DST qui :

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

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

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

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

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

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

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

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

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

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

5. Dates d'entrée en vigueur

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

6. Contexte :

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

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

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

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

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

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

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

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

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

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

Colonnes « Systèmes visés » des tableaux

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

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

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

B. Exigences et mesures

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Conformité

1. Processus de surveillance de la conformité

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

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

1.2. Conservation des pièces justificatives

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

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

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

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

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

1.4. Autres informations sur la conformité

- Aucune

2. Tableau des éléments de conformité

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

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

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

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

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

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

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 :

Les directives suivantes servent de guide pour les éléments que doit comporter un plan d'intervention en cas d'*incident de cybersécurité* :

- Department of Homeland Security, Control Systems Security Program, Developing an Industrial Control Systems Cyber Security Incident Response Capability, 2009, en ligne à l'adresse http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, Computer Security Incident Handling Guide, Special Publication 800-61 revision 1, March 2008, en ligne à l'adresse http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

À la partie 1.2, un *incident de cybersécurité à déclarer* est un *incident de cybersécurité* qui a compromis ou perturbé une ou plusieurs tâches de fiabilité d'une entité fonctionnelle. Il est à noter que les *incidents de cybersécurité à déclarer* sont ceux qui doivent faire l'objet d'une mesure d'intervention, laquelle peut s'inscrire dans l'une de deux catégories : nécessaire ou facultative. Celles-ci se distinguent par la réponse ou non à un événement. Les mesures de précaution qui ne sont pas adoptées en réponse à des dommages ou à des effets persistants peuvent être classées comme facultatives. Toutes les autres mesures d'intervention prises pour

éviter des dommages persistants ou des effets néfastes, y compris l'activation de systèmes redondants, sont désignées comme requises.

Selon les obligations de déclaration des *incidents de cybersécurité à déclarer*, un avis au moins préliminaire doit être transmis à l'ES-ISAC dans l'heure qui suit la détermination qu'un *incident de cybersécurité* doit être déclaré (et non dans l'heure qui suit l'*incident de cybersécurité*, une distinction importante). Cet ajout vient répondre à la directive traitant de cette question à l'ordonnance 706 de la FERC, paragraphes 673 et 676, qui stipule que la déclaration (au moins préliminaire) doit être faite dans un délai d'au plus une heure. La présente norme n'exige pas la transmission d'un rapport complet dans l'heure qui suit la détermination qu'un *incident de cybersécurité* doit être déclaré, mais d'un avis au moins préliminaire (par exemple, un appel téléphonique, un courriel ou un avis envoyé via le Web). La norme ne précise pas de délai particulier pour achever le rapport.

Exigence E2 :

L'exigence E2 prescrit la mise à l'épreuve périodique du plan d'intervention en cas d'*incident de cybersécurité* par les entités. Ceci comprend l'exigence à la partie 2.2, qui stipule que le plan doit être suivi pendant la mise à l'épreuve. Les exigences de mise à l'épreuve concernent expressément les *incidents de cybersécurité à déclarer*.

Les entités peuvent remplacer la mise à l'épreuve annuelle du plan par une intervention à l'occasion d'un *incident de cybersécurité à déclarer* réel. Autrement, elles doivent mettre le plan à l'épreuve au moyen d'un exercice sur papier, d'un exercice sur table ou d'un exercice opérationnel complet. Le programme Homeland Security Exercise and Evaluation Program (HSEEP) de la Federal Emergency Management Agency (FEMA) présente d'autres types d'exercices, dont les quatre types suivants d'exercices axés sur les discussions : séminaires, ateliers, exercices sur table et jeux. Il définit, en particulier, l'exercice sur table, à savoir « un exercice où des membres clés du personnel se réunissent pour discuter de scénarios de simulation dans un contexte informel. On peut avoir recours à des exercices sur table pour évaluer des plans, des politiques ou des procédures. »

Le programme HSEEP énumère les trois types suivants d'exercices axés sur les opérations : exercice d'entraînement, exercice fonctionnel et exercice à grand déploiement. Il définit, en particulier, l'exercice à grand déploiement, à savoir « un exercice multidisciplinaire, intergouvernemental et multi-agences qui donne lieu à des interventions fonctionnelles (p. ex., bureaux locaux conjoints, centres des opérations d'urgence, etc.) et sur le terrain (p. ex., pompiers décontaminant des mannequins). »

Outre les exigences de mise en œuvre du plan d'intervention, la partie 3.2 stipule que les entités doivent conserver les dossiers des *incidents de cybersécurité à déclarer*. La colonne « Mesures » énumère plusieurs exemples de types de preuve. Les entités devraient consulter leurs procédures de gestion pour déterminer les types de preuve à conserver et la façon de les transporter et de les stocker. Pour plus d'information relativement à la conservation des dossiers sur les incidents, consulter le guide SP800-86 du NIST, *Guide to Integrating Forensic Techniques into Incident Response*. Celui-ci comprend une section (3.1.2) sur l'acquisition de données dans le cadre d'une analyse judiciaire.

Exigence E3 :

Cette exigence prescrit la tenue à jour par les entités de leurs plans d'intervention en cas d'*incident de cybersécurité*. Deux parties dans les exigences requièrent la mise à jour d'un plan : (1) les leçons apprises, à la partie 3.1, et (2) les changements organisationnels ou technologiques, à la partie 3.2.

La documentation des leçons apprises, à la partie 3.1, concerne les *incidents de cybersécurité à déclarer* et les activités illustrées à la figure 1 ci-dessous. Elle doit débuter à la fin de l'incident, en reconnaissant que les mesures d'intervention peuvent prendre des jours sinon des semaines à être mises en place dans le cas d'incidents complexes mettant en jeu des systèmes complexes. Durant le processus d'intégration des leçons apprises, l'équipe d'intervention peut être amenée à discuter de l'incident en vue de déterminer les lacunes ou les points à améliorer dans le plan. Tout écart documenté au plan, mentionné à la partie 2.2, peut faire partie des leçons apprises. Il est possible qu'aucune leçon apprise documentée ne soit associée à un *incident de cybersécurité à déclarer*. Dans un tel cas, l'entité doit conserver les documents attestant l'absence de leçons apprises associées à cet incident.

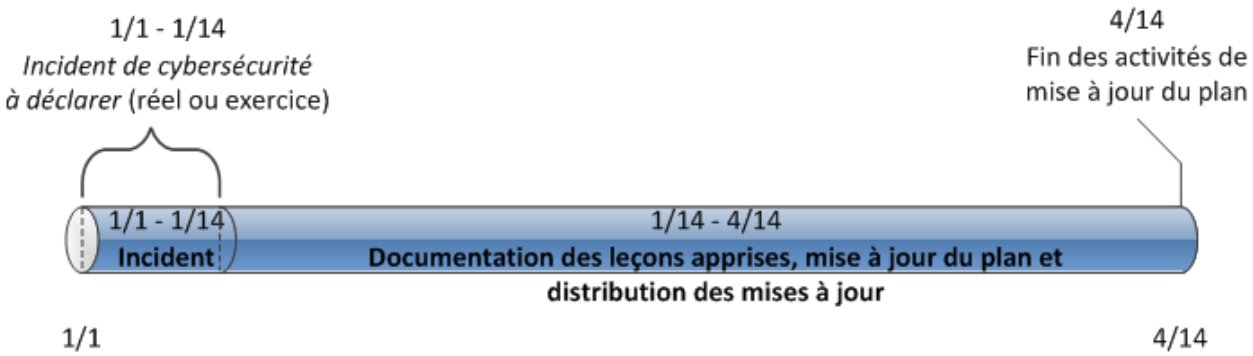


Figure 1 : Calendrier de CIP-008-5 E3 pour les incidents de cybersécurité à déclarer

Les activités nécessaires pour intégrer les leçons apprises au plan comprennent notamment la mise à jour du plan et la distribution de ces mises à jour. Les entités doivent envisager de rencontrer toutes les personnes concernées par l'incident et de documenter les leçons apprises aussitôt que possible après qu'il se produit. On disposera ainsi d'un plus long délai pour mettre à jour le plan, obtenir les approbations requises et distribuer ces mises à jour à l'équipe d'intervention en cas d'incident.

L'exigence de la partie 3.2 portant sur la révision du plan concerne les changements organisationnels et technologiques aux éléments touchés par le plan et vise les activités illustrées à la figure 2 ci-dessous. Parmi les changements organisationnels, on compte les changements apportés aux rôles et responsabilités des personnes définies dans le plan ou aux groupes ou personnes chargés de l'intervention. Il peut s'agir de changements apportés à des noms ou à des coordonnées cités dans le plan. Les changements technologiques qui ont une incidence sur le plan peuvent être des changements apportés à des sources d'information, à des systèmes de communication ou à des systèmes d'établissement de tickets.

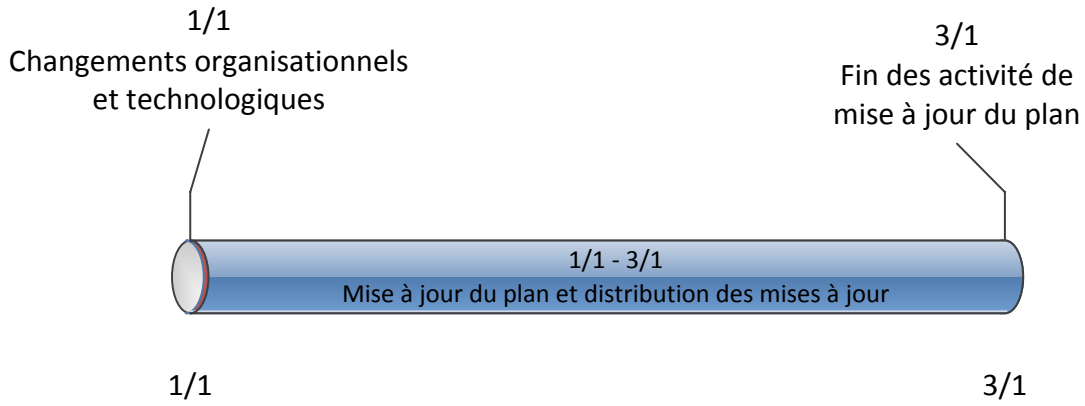


Figure 2 : Calendrier de révision du plan de 3.2.

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 :

La mise en œuvre d'un plan d'intervention efficace en cas d'*incident de cybersécurité* réduit les risques posés au fonctionnement fiable du BES par un *incident de cybersécurité* et procure aux entités responsables une rétroaction qui leur permet d'améliorer les mesures de sécurité relatives aux *systèmes électroniques BES*. Les activités de prévention peuvent limiter le nombre d'incidents, sans toutefois tous les éliminer. Il est donc essentiel de se doter d'une stratégie préétablie d'intervention en cas d'incident en vue de détecter rapidement les incidents, de limiter les pertes et la destruction, de combler les lacunes exploitées et de rétablir les services informatiques. Cette exigence peut être remplie au moyen d'un plan d'entreprise ou d'un seul plan d'intervention pour l'ensemble des *systèmes électroniques BES*. Une organisation peut disposer d'un plan commun pour de multiples entités visées qu'elle détient.

Sommaire des modifications : Des modifications, tenant compte essentiellement des commentaires formulés par l'industrie, ont été apportées au libellé pour décrire plus précisément les mesures à suivre.

Référence à une version précédente : (Partie 1.1) CIP-008, E1.1

Description et justification des modifications : (Partie 1.1)

Remplacement de « caractériser » par « identifier » et de « mesures d'intervention » par « répondre » aux fins de clarification.

Référence à une version précédente : (Partie 1.2) CIP-008, E1.1

Description et justification des modifications : (Partie 1.2)

Prise en compte des exigences de déclaration des versions antérieures de la norme CIP-008. La seule obligation à laquelle doivent se plier les entités, selon la présente partie des exigences, est de disposer d'un processus pour déterminer les *incidents de cybersécurité à déclarer*. Cette partie tient compte aussi de la directive établie dans l'ordonnance 706 de la FERC, aux paragraphes 673 et 676, qui stipule que la déclaration doit être faite dans un délai d'au plus une heure (au moins de façon préliminaire).

Référence à une version précédente : (Partie 1.3) CIP-008, E1.2

Description et justification des modifications : (Partie 1.3)

Remplacement des « équipes d'intervention en cas d'incident » par les « groupes ou personnes » chargés de l'intervention pour éviter l'interprétation selon laquelle les sections portant sur les rôles et responsabilités doivent faire référence à des équipes en particulier.

Référence à une version précédente : (Partie 1.4) CIP-008, E1.2

Description et justification des modifications : (Partie 1.4)

Modification apportée aux fins de conformité pour refléter la redéfinition du terme « *incident de cybersécurité* ».

Raisonnement pour E2 :

La mise en œuvre d'un plan d'intervention efficace en cas d'*incident de cybersécurité* réduit les risques posés à la fiabilité du BES par un tel incident et procure aux entités responsables une rétroaction qui leur permet d'améliorer les mesures de sécurité relatives aux *systèmes électroniques BES*. Cette exigence encadre la mise en œuvre des plans d'intervention. La partie 2.3 de l'exigence prescrit la conservation des documents relatifs à chaque incident aux fins d'analyse ultérieure.

Cette exigence oblige les entités à suivre le plan d'intervention en cas d'*incident de cybersécurité* lorsque se produit un incident ou lors des essais, mais ne les empêche pas de s'écarter du plan en cas de besoin. Elle fait en sorte que le plan représente l'intervention réelle et qu'il n'existe pas aux seules fins de documentation. Si le plan est rédigé de façon assez générale, chaque mesure prise durant l'intervention ne devrait pas être sujette à examen. Le plan devrait tenir compte des différences pertinentes dans les décisions tactiques prises par les personnes ou groupes chargés de l'intervention en cas d'incident. Les écarts par rapport au plan peuvent être documentés durant l'intervention ou après coup, dans le cadre de l'examen.

Sommaire des modifications : Ajout d'exigences de vérification de l'efficacité et de l'application cohérente du plan d'intervention de l'entité responsable en réponse à un ou des *incidents de cybersécurité* ayant un impact sur un *système électronique BES*.

Référence à une version précédente : (Partie 2.1) CIP-008, E1.6

Description et justification des modifications : (Partie 2.1)

Reformulations mineures ; libellé resté pratiquement inchangé.

Référence à une version précédente : (Partie 2.2) CIP-008, E1.6

Description et justification des modifications : (Partie 2.2)

Autorisation des écarts entre le ou les plans et les mesures prises durant des situations réelles ou des épreuves, si ces écarts sont consignés aux fins d'examen.

Référence à une version précédente : (Partie 2.3) CIP-008, E2

Description et justification des modifications : (Partie 2.3)

Suppression des références faites à la période de conservation étant donné que la norme traite de la conservation des données dans la section « Conformité ».

Raisonnement pour E3 :

Effectuer suffisamment d'examens, de mises à jour et de communications pour confirmer l'efficacité et l'application cohérente du plan d'intervention de l'entité responsable en réponse à un ou des *incidents de cybersécurité* ayant un impact sur un *système électronique BES*. Il n'est pas nécessaire de disposer d'un plan distinct pour les parties de l'exigence du tableau s'appliquant aux *systèmes électroniques BES* à impact élevé ou moyen. Si une entité dispose d'un seul plan d'intervention en cas d'*incident de cybersécurité* et détient des *systèmes électroniques BES* à impact élevé et moyen, les exigences supplémentaires s'appliquent à ce plan.

Sommaire des modifications : Les modifications apportées tiennent comptent de l'ordonnance 706 de la FERC, paragraphe 686, qui inclut une directive imposant un examen après intervention dans le cadre d'épreuves ou d'incidents réels ainsi qu'une mise à jour du plan tenant compte des leçons apprises. La norme a aussi été modifiée pour préciser ce que sous-entend un examen du plan et les changements qui nécessiteraient une mise à jour du plan.

Référence à une version précédente : (Partie 3.1) CIP-008, E1.5

Description et justification des modifications : (Partie 3.1)

Prise en compte de l'ordonnance 706 de la FERC, paragraphe 686, qui prescrit la documentation des vérifications ou incidents réels et des leçons apprises.

Référence à une version précédente : (Partie 3.2) CIP-008, E1.4

Description et justification des modifications : (Partie 3.2)

Précisions sur les activités nécessaires pour tenir le plan à jour. La version précédente demandait aux entités de mettre le plan à jour après tout changement. Les modifications clarifient les changements qui nécessitent une mise à jour.

Historique des versions

Version	Date	Modification apportée	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 raisonnables. 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		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.	Mise à jour
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

Version	Date	Modification apportée	Suivi des modifications
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-008-5.	
5	9 juillet 2014	Émission d'une lettre d'ordonnance de la FERC approuvant les révisions aux VRF et VSL de certaines normes CIP.	Exigence E2 de la CIP-008-5, tableau des VSL sous Critique, changé de 19 à 18 mois civils.

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

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe aura préséance.

A. Introduction

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

2. **Numéro :** CIP-008-5

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

   Entités fonctionnelles

   Aucune disposition particulière

   Installations

   La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

   Exemptions additionnelles

   Sont exemptés de l'application de la présente norme :

   - Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur un réseau voisin.
   - Postes élévateurs des installations de production identifiées au point précédent.

5. **Date d'entrée en vigueur au Québec :**

   5.1. Adoption de la norme par la Régie de l'énergie : xx mois 201x

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

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

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

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

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

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

A. Introduction

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

2. Numéro : CIP-009-5

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

4. Applicabilité :

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

4.1.1 Responsable de l'équilibrage

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

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

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

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

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

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

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

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

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

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

4.2.1.1 Chaque système de DSF ou de DST qui :

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

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

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

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

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

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

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

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

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

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

5. Dates d'entrée en vigueur

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

6. Contexte :

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

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

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

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

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

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

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

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

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

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

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

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

Colonnes « Systèmes visés » des tableaux

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

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

B. Exigences et mesures

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

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

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

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

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

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

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

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

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

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

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

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

C. Conformité

1. Processus de surveillance de la conformité :

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

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

1.2. Conservation des pièces justificatives :

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

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

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

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

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

1.4. Autres informations sur la conformité :

- Aucune

2. Tableau des éléments de conformité

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

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

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

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

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

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

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

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

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 :

Les directives suivantes servent de guide pour les éléments que doit comporter un plan de rétablissement :

- North American Electric Reliability Corporation (NERC). Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions. September 2011. En ligne au http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology (NIST). Contingency Planning Guide for Federal Information Systems. Special Publication 800-34 revision 1, May 2010. En ligne au http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Le terme plan de rétablissement est utilisé dans la présente norme pour désigner un ensemble documenté d'instructions et de ressources nécessaires au rétablissement des fonctions de fiabilité exercées par les *systèmes électroniques BES*. Le plan de rétablissement peut s'inscrire dans un plan global de continuité des activités ou de reprise après sinistre, mais ce terme n'implique pas d'autres obligations associées aux disciplines non visées par les exigences.

Un plan de rétablissement documenté peut ne pas être nécessaire pour chaque *système électronique BES* visé. Par exemple, le plan de rétablissement à court terme d'un *système électronique BES* situé dans un poste électrique donné peut être géré quotidiennement à l'aide d'applications avancées pour les réseaux électriques, telles que l'estimation d'état, les contingences et les mesures correctives ainsi que la gestion prévisionnelle des retraits. Un seul plan de rétablissement de *systèmes électroniques BES* devrait être suffisant pour plusieurs installations similaires, comme celles qu'on retrouve dans les postes électriques ou les centrales.

À la partie 1.1, les conditions de déclenchement du plan de rétablissement doivent tenir compte de menaces viables pour le *système électronique BES*, comme une catastrophe naturelle, une panne de matériel ou d'environnement informatique ou un *incident de cybersécurité*. Une analyse des incidences opérationnelles pour le *système électronique BES* peut s'avérer utile en vue de déterminer ces conditions.

À la partie 1.2, les entités doivent identifier les personnes chargées des mesures de rétablissement du *système électronique BES* visé.

À la partie 1.3, les entités doivent tenir compte des types d'information suivants lors du rétablissement des *systèmes électroniques BES* :

1. fichiers et supports d'installation ;
2. bandes de sauvegarde courantes et autres paramètres de configuration documentés ;
3. procédures documentées d'assemblage ou de restauration ; et
4. stockage de duplication entre les sites.

À la partie 1.4, les processus de vérification du bon déroulement des processus de sauvegarde doivent comprendre notamment : (1) la vérification de l'intégrité des supports de sauvegarde, (2) la vérification des journaux ou une inspection attestant que l'information du système de production courant peut être lue, et (3) la vérification des journaux ou une inspection attestant que l'information a été écrite sur le support de sauvegarde. Cette partie de l'exigence n'impose pas la réalisation d'essais de restauration. Les scénarios de sauvegarde suivants donnent des exemples de processus efficaces pour vérifier le bon déroulement des sauvegardes et déceler les échecs de sauvegarde :

- Processus de sauvegarde périodique (p. ex., quotidienne ou hebdomadaire) – Examen des journaux générés ou des rapports d'état des travaux et mise en place d'avis d'échec de sauvegarde.
- Processus de sauvegarde non périodique – Essai initial et essais périodiques (tous les 15 mois) seulement si une sauvegarde unique est fournie durant la mise en service du système. Essais supplémentaires effectués au besoin, par exemple dans le cadre du programme de gestion des changements de configuration.

- Écriture de données miroir – Configuration d'alertes en cas d'échec de transfert de données pendant un délai précisé par l'entité (p. ex., 15 minutes), après lequel l'information miroir n'est peut-être plus utile aux fins de rétablissement.
- Données de configuration manuelle – Inspection initiale et périodique (tous les 15 mois) des données utilisées pour le rétablissement avant leur stockage. Inspections supplémentaires effectuées au besoin, par exemple dans le cadre du programme de gestion des changements de configuration.

Le plan doit aussi inclure des processus de prise en compte des échecs de sauvegarde, qui précisent les mesures à prendre en cas d'avis d'échec ou de toute autre indication d'un échec.

À la partie 1.5, le plan de rétablissement doit inclure des modalités de conservation des données permettant de déterminer la cause d'un *incident de cybersécurité*. Puisqu'il n'est pas toujours possible de savoir initialement si un *incident de cybersécurité* est ce qui a entraîné le déclenchement du plan de rétablissement, les procédures de conservation des données doivent être suivies tant et aussi longtemps que la possibilité d'un *incident de cybersécurité* n'est pas écartée. La norme CIP-008 traite de la conservation des données associées à ce type d'incident.

Exigence E2 :

Une entité responsable doit tester chaque plan de rétablissement des *systèmes électroniques BES* tous les 15 mois. Toutefois, cela ne veut pas nécessairement dire que l'entité doit mettre à l'essai chaque plan individuel. Les *systèmes électroniques BES* qui sont répartis et en grand nombre, comme ceux qu'on retrouve dans les postes électriques, peuvent ne pas nécessiter un plan de rétablissement individuel et les installations redondantes connexes si les mesures à prendre en cas d'événement grave consistent généralement à reconfigurer et à reconstruire ces systèmes. Inversement, chaque zone de production-transport d'électricité comporte habituellement un centre de contrôle nécessitant une installation redondante ou de repli. Étant donné ces différences, les plans de rétablissement associés aux centres de contrôle diffèrent grandement de ceux qui sont associés aux centrales et aux postes électriques.

Le test d'un plan de rétablissement ne porte pas nécessairement sur tous les aspects du plan ou des scénarios de panne, mais il doit suffire pour s'assurer que le plan est à jour et il doit porter sur au moins un processus de restauration des systèmes électroniques visés.

Les entités peuvent remplacer un test du plan aux 15 mois par un rétablissement suivant un incident réel. Autrement, elles doivent mettre à l'essai le plan au moyen d'un exercice sur papier, d'un exercice sur table ou d'un exercice opérationnel. Le programme Homeland Security Exercise and Evaluation Program (HSEEP) de la Federal Emergency Management Agency (FEMA) présente d'autres types d'exercices, dont les quatre types suivants d'exercices axés sur les discussions : séminaires, ateliers, exercices sur table et jeux. Il définit, en particulier, l'exercice sur table, à savoir « un exercice où des membres clés du personnel se réunissent pour discuter de scénarios de simulation dans un contexte informel. On peut avoir recours à des exercices sur table pour évaluer des plans, des politiques ou des procédures. »

Le programme HSEEP énumère les trois types suivants d'exercices axés sur les opérations : exercice d'entraînement, exercice fonctionnel et exercice à grand déploiement. Il définit, en

particulier, l'exercice à grand déploiement, à savoir « un exercice multidisciplinaire, intergouvernemental et multi-agences qui donne lieu à des interventions fonctionnelles (p. ex., bureaux locaux conjoints, centres des opérations d'urgence, etc.) et sur le terrain (p. ex., pompiers décontaminant des mannequins). »

À la partie 2.2, les entités doivent se reporter aux exigences de sauvegarde et de stockage de l'information nécessaire au rétablissement des *systèmes électroniques BES* précisées à la partie 1.3. Cela permet d'offrir une assurance supplémentaire que cette information permettra effectivement de rétablir le *système électronique BES*, le cas échéant. Dans le cas d'équipement informatique complexe, un essai complet de l'information est irréaliste. Les entités doivent alors déterminer l'échantillon représentatif de l'information qui offre une assurance dans les processus mentionnés à la partie 1.3. Cet essai doit comprendre les étapes nécessaires pour s'assurer que l'information est à la fois accessible et courante. Dans le cas des supports de sauvegarde, il peut s'agir d'en mettre à l'essai un échantillon représentatif pour s'assurer que l'information peut être chargée et d'en vérifier le contenu pour s'assurer que l'information reflète la configuration courante des *actifs électroniques* visés.

Exigence E3 :

Cette exigence prescrit la tenue à jour par les entités de leurs plans de rétablissement. Deux parties d'exigence déclenchent la mise à jour d'un plan : (1) les leçons apprises, et (2) les changements organisationnels ou technologiques.

La documentation des leçons apprises concerne chaque déclenchement de plan de rétablissement, et comprend les activités illustrées à la figure 1 ci-dessous. Elle débute à la fin des activités de rétablissement, en reconnaissance du fait que les activités de rétablissement complexes peuvent prendre des jours sinon des semaines à réaliser. Durant le processus d'intégration des leçons apprises, l'équipe de rétablissement peut être amenée à discuter de l'incident en vue de déterminer les lacunes ou les points à améliorer dans le plan. Il est possible qu'aucune leçon apprise documentée ne soit associée à un déclenchement de plan de rétablissement. Dans un tel cas, l'entité doit conserver les documents attestant l'absence de leçons apprises associées à ce déclenchement.

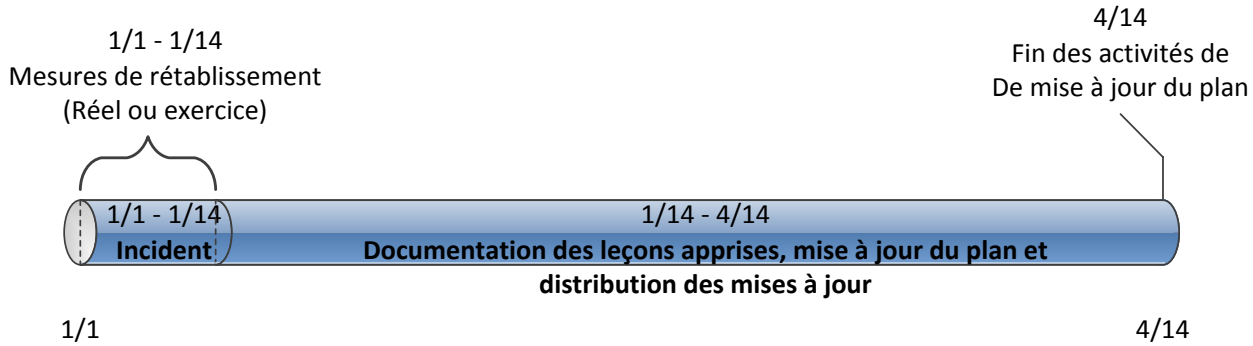


Figure 1 : Calendrier pour E3 CIP-009-5

Les activités nécessaires pour intégrer les leçons apprises au plan comprennent notamment la mise à jour du plan et la distribution de ces mises à jour. Les entités doivent envisager de

rencontrer toutes les personnes concernées par le plan de rétablissement et de documenter les leçons apprises aussitôt que possible après qu'il a été déclenché. On disposera ainsi d'un plus long délai pour mettre à jour le plan, obtenir les approbations requises et distribuer ces mises à jour à l'équipe de rétablissement.

L'exigence portant sur la révision du plan concerne les changements organisationnels et technologiques aux éléments touchés par le plan et vise les activités illustrées à la figure 2 ci-dessous. Parmi les changements organisationnels, on compte les changements apportés aux rôles et responsabilités des personnes définis dans le plan et aux groupes ou personnes chargés de l'intervention. Il peut s'agir de changements apportés à des noms ou à des coordonnées cités dans le plan. Les changements technologiques qui ont une incidence sur le plan peuvent être des changements apportés à des sources d'information, à des systèmes de communication ou à des systèmes d'établissement de tickets.

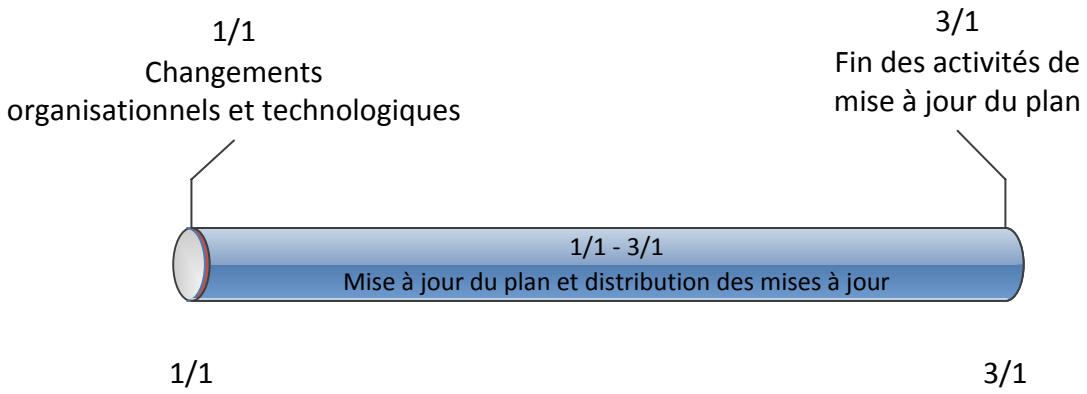


Figure 2 : Calendrier pour les changements au plan de 3.2.

Au moment d'aviser les personnes de changements apportés au plan d'intervention, les entités doivent garder à l'esprit que les plans de rétablissement peuvent être considérés comme de l'information de *système électronique BES*. Elles doivent donc prendre les mesures qui s'imposent pour empêcher la divulgation non autorisée de l'information contenue dans ces plans. Par exemple, le plan de rétablissement lui-même et toute autre information sensible concernant le plan doivent être retranchés des courriels et autres communications non chiffrées.

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 :

Les activités de prévention peuvent limiter le nombre d'incidents, sans toutefois les prévenir tous. Il est donc nécessaire de se doter de moyens pour assurer un rétablissement rapide après les incidents, limiter les pertes et la destruction, combler les lacunes exploitées et rétablir les services informatiques afin que la restauration des fonctionnalités des *systèmes électroniques BES* se fasse de manière cohérente et organisée.

Sommaire des modifications : Ajout de modalités visant la protection des données pouvant être utiles dans le cadre d'une enquête sur un événement qui nécessite le déclenchement d'un plan de rétablissement de systèmes électroniques.

Référence à une version précédente : (Partie 1.1) CIP-009, E1.1

Description et justification des modifications : (Partie 1.1)

Reformulations mineures ; libellé pratiquement inchangé.

Référence à une version précédente : (Partie 1.2) CIP-009, E1.2

Description et justification des modifications : (Partie 1.2)

Reformulations mineures ; libellé pratiquement inchangé.

Référence à une version précédente : (Partie 1.3) CIP-009, E4

Description et justification des modifications : (Partie 1.3)

Prise en compte de l'ordonnance de la FERC, paragraphes 739 et 748. Le texte modifié résume le paragraphe 744.

Référence à une version précédente : (Partie 1.4) Nouvelle exigence

Description et justification des modifications : (Partie 1.4)

Prise en compte de l'ordonnance de la FERC, paragraphes 739 et 748.

Référence à une version précédente : (Partie 1.5) Nouvelle exigence

Description et justification des modifications : (Partie 1.5)

Ajout de l'exigence pour tenir compte de l'ordonnance 706 de la FERC, paragraphe 706.

Raisonnement pour E2 :

La mise en œuvre d'un plan de rétablissement efficace réduit les risques posés fonctionnement fiable du BES en réduisant le délai de rétablissement après différents types d'incidents nuisibles

pour les *systèmes électroniques BES*. Cette exigence encadre la mise en œuvre continue des plans d'intervention.

La partie d'exigence 2.2 offre une assurance supplémentaire quant à l'information (p. ex., bandes de sauvegarde, centres miroir, etc.) nécessaire au rétablissement des *systèmes électroniques BES*. Dans la plupart des cas, une mise à l'épreuve complète du plan est irréaliste en raison de la grande quantité d'information nécessaire au rétablissement. L'entité responsable doit donc déterminer un échantillonnage qui offre l'assurance que l'information est utilisable.

Sommaire des modifications : Ajout d'essais opérationnels du plan de rétablissement des *systèmes électroniques BES*.

Référence à une version précédente : (Partie 2.1) CIP-009, E2

Description et justification des modifications : (Partie 2.1)

Reformulations mineures ; libellé pratiquement inchangé.

Référence à une version précédente : (Partie 2.2) CIP-009, E5

Description et justification des modifications : (Partie 2.2)

Précisions sur ce qui doit être mis à l'essai et clarification du fait qu'un échantillonnage représentatif suffit. Ces modifications, ainsi que l'exigence de la partie 1.4, tiennent compte de l'ordonnance 706 de la FERC, paragraphes 739 et 748, qui porte sur la mise à l'essai des sauvegardes, en offrant un haut degré de confiance que l'information permettra effectivement de rétablir le système au besoin.

Référence à une version précédente : (Partie 2.3) CIP-009, E2

Description et justification des modifications : (Partie 2.3)

Prise en compte de l'ordonnance 706 de la FERC, paragraphe 725, stipulant que le plan de rétablissement doit faire l'objet d'un essai opérationnel complet tous les trois ans.

Raisonnement pour E3 :

Améliorer l'efficacité du ou des plans de rétablissement des systèmes électroniques BES après un essai et assurer la tenue à jour et la distribution de ces plans. Pour ce faire, les entités responsables doivent (i) passer en revue les leçons apprises, à la partie 3.1, et (ii) réviser le plan, selon la partie 3.2, à la suite de changements organisationnels ou technologiques spécifiques qui pourraient avoir un impact sur l'exécution du plan. Dans les deux cas, l'entité responsable doit mettre à jour et distribuer le plan si ce dernier nécessite des modifications.

Sommaire des modifications :

Clarification du moment où les leçons apprises du plan doivent être passées en revue et précision du délai de mise à jour du plan de rétablissement.

Référence à une version précédente : (Partie 3.1) CIP-009, E1 et E3

Description et justification des modifications : (Partie 3.1)

Ajout des délais de documentation des leçons apprises et de mise à jour du plan. Cette exigence regroupe les trois activités en un seul endroit. Tandis que les versions antérieures précisaient un délai de 30 jours civils pour documenter les leçons apprises, suivi d'un autre délai pour mettre à jour les plans de rétablissement et transmettre l'avis, cette exigence regroupe ces activités en une seule période.

Référence à une version précédente : (Partie 3.2) Nouvelle exigence

Description et justification des modifications : (Partie 3.2)

Précisions sur les activités nécessaires pour tenir le plan à jour. La version précédente demandait aux entités de mettre le plan à jour après tout changement. Les modifications clarifient les changements qui nécessitent une mise à jour.

Historique des versions

Version	Date	Modification apportée	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 ».	

Version	Date	Modification apportée	Suivi des modifications
3		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.	Mise à jour
3	31 mars 2010	Approbation par la FERC.	
4	30 décembre 2010	Ajout de critères précis sur l'identification des *actifs critiques*.	Mise à jour
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 format selon le gabarit RBS.
5	22 novembre 2013	Émission d'une ordonnance de la FERC approuvant CIP-009-5.	
5	9 juillet 2014	Émission d'une lettre d'ordonnance de la FERC approuvant les révisions aux VRF et VSL de certaines normes CIP	Révision des délais contenus dans les VSL de 90-210 jours à 90-120 jours.

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

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe aura préséance.

A. Introduction

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

2. **Numéro :** CIP-009-5

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

Entités fonctionnelles

Aucune disposition particulière

Installations

La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

- Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur un réseau voisin.
- Postes élévateurs des installations de production identifiées au point précédent.

5. **Date d'entrée en vigueur au Québec :**

5.1. Adoption de la norme par la Régie de l'énergie : xx mois 201x

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

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

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

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

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

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

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

A. Introduction

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

2. Numéro : CIP-010-1

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

4. Applicabilité :

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

4.1.1 Responsable de l'équilibrage

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

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

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

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

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

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

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

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

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

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

4.2.1.1 Chaque système de DSF ou de DST qui :

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

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

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

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

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

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

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

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

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

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

5. Dates de mise en vigueur

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

6. Contexte :

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

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

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

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

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

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

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

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

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

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

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

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

Colonnes « Systèmes visés » des tableaux

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

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

B. Exigences et mesures

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Conformité

1. Processus de surveillance de la conformité :

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

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

1.2. Conservation des pièces justificatives :

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

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

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

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

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

1.4. Autres informations sur la conformité :

- Aucun

2. Tableau des éléments de conformité

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

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

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

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

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

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

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

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

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

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

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

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-1)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						chacun de ses *systèmes électroniques BES* visés, mais elle n'a pas effectué l'analyse de vulnérabilité active d'une manière qui simule une configuration de référence existante de ses *systèmes électroniques BES* visés. (3.3) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses *systèmes électroniques BES* visés, mais elle n'a pas documenté les résultats des analyses de vulnérabilité, les plans d'action pour remédier ou mitiger les vulnérabilités relevées

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

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

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 :

Configuration de référence

L'idée d'établir une configuration de référence pour un *actif électronique* vise à clarifier la formulation des exigences énoncées dans les versions précédentes des normes CIP. Tout changement apporté à un élément de la configuration de référence d'un *actif électronique* visé constitue le déclencheur du processus de gestion des changements par l'entité concernée.

Les configurations de référence dans la norme CIP-010 comportent cinq éléments : le système d'exploitation ou le système embarqué ; les logiciels commerciaux ou les logiciels libres ; les logiciels personnalisés ; les ports logiques accessibles par le réseau ; et les rustines de sécurité. L'information sur le système d'exploitation précise le nom et la version du logiciel en cours d'utilisation dans l'*actif électronique*. En l'absence de système d'exploitation indépendant (par exemple pour un relais de protection), l'information sur le système embarqué devrait être précisé. Les logiciels commerciaux ou les logiciels libres sont ceux qui ont été installés intentionnellement dans l'actif électronique. L'utilisation du mot « intentionnellement » vise à préciser que seuls les logiciels jugés nécessaires pour les *actifs électroniques* doivent être inclus dans la configuration de référence. Le SDT ne souhaite pas que soient inclus dans cette configuration les calepins, calculettes, les DLL, les pilotes de périphérique ou d'autres

applications compris dans un système d'exploitation du commerce ou distribués à titre de logiciel ouvert. Les logiciels personnalisés installés peuvent comprendre des scripts programmés pour des fonctions locales de l'entité ou d'autres programmes créés en vue d'une tâche ou fonction spécifique à l'entité. Dans le cas d'un logiciel supplémentaire qui a été installé intentionnellement et qui n'est ni un logiciel du commerce ni un logiciel libre, ce logiciel pourrait être considéré comme un logiciel personnalisé. Si un dispositif a besoin de communiquer avec un autre dispositif à l'extérieur du réseau, les communications doivent être limitées aux seuls dispositifs qui doivent communiquer, conformément à la norme CIP-007-5. Les ports accessibles doivent être indiqués dans la configuration de référence. Les rustines de sécurité appliquées doivent comprendre toutes les rustines antérieures et courantes appliquées sur l'actif électronique. Alors que l'exigence E2.1 de la norme CIP-007-5 stipule que les entités doivent se tenir informées des rustines de sécurité, les évaluer et les appliquer, l'exigence E1.1.5 de la norme CIP-010 stipule que les entités doivent consigner toutes les rustines appliquées, antérieures et courantes.

Afin d'aider la compréhension, voici un exemple qui décrit la configuration de référence d'un relais à microprocesseur série seulement :

Actif n^{o} 051028 au poste électrique Alpha

- E1.1.1 – Système embarqué : [FABRICANT]-[MODÈLE]-XYZ-1234567890-ABC
- E1.1.2 – Sans objet
- E1.1.3 – Sans objet
- E1.1.4 – Sans objet
- E1.1.5 – Rustine 12345, Rustine 67890, Rustine 34567 et Rustine 437823

En outre, pour un système informatique type, la configuration de référence pourrait renvoyer à une norme informatique qui précise les détails de la configuration. L'entité devrait alors présenter cette norme informatique à titre de preuve de conformité.

Mécanismes de cybersécurité

Les mécanismes de cybersécurité dont il est question dans cette exigence renvoient spécifiquement aux mécanismes des normes CIP-005 et CIP-007. Les parties pertinentes de l'exigence E1 de la norme CIP-010 stipulent que l'entité doit déterminer et analyser les mécanismes des normes CIP-005 et CIP-007 qui pourraient être touchés par un changement par rapport à la configuration de référence existante. Le SDT ne souhaite pas obliger l'entité responsable à passer en revue tous les mécanismes de cybersécurité des normes CIP-005 et CIP-007 pour chaque changement, mais seulement le ou les mécanismes susceptibles d'être touchés par le changement en question. Par exemple, les changements relatifs aux ports logiques concernent seulement l'exigence E1 de la norme CIP-007 (ports et services), tandis que

les changements relatifs aux rustines de sécurité concernent seulement l'exigence E2 de la norme CIP-007 (gestion des rustines de sécurité). Le SDT a choisi de ne pas préciser les exigences des normes CIP-005 et CIP-007 dans le texte de la norme CIP-010, étant donné que n'importe quel des mécanismes de cybersécurité de ces normes peut être touché par suite d'un changement dans la configuration de référence. L'équipe de rédaction considère qu'il est possible que toutes les exigences des normes CIP-005 et CIP-007 soient touchées par un changement important dans la configuration de référence, et c'est pourquoi les normes CIP-005 et CIP-007 sont citées dans leur globalité plutôt qu'à l'échelon de leurs exigences individuelles.

Environnement d'essai

L'environnement d'essai du *centre de contrôle* (ou l'environnement de production dans lequel l'essai est effectué d'une manière qui réduit au minimum les effets dommageables) doit simuler la configuration de référence, mais peut le faire au moyen de composants différents. Par exemple, un *système électronique BES* peut comporter une base de données sur un composant et un serveur Web sur un autre ; cependant, dans l'environnement d'essai, la base de données et le serveur Web peuvent résider sur un même composant pourvu que le système d'exploitation, les rustines de sécurité, les ports accessibles par le réseau et les logiciels soient identiques.

En outre, l'entité responsable doit prendre note que, lorsqu'il est question d'un environnement d'essai (ou d'un environnement de production dans lequel l'essai est effectué d'une manière qui réduit au minimum les effets dommageables), il s'agit bien de « simuler » la configuration de référence, et non de la reproduire à l'identique. Cette formulation a été choisie expressément pour les cas où il serait impossible de dupliquer certains éléments de *système électronique BES* d'un *centre de contrôle* ; par exemple, un modèle ancien de pilote de tableau de visualisation, ou encore les nombreuses liaisons d'échange de données à partir des installations sur le terrain ou vers d'autres *centres de contrôle* (comme les liaisons ICCP).

Exigence E2 :

L'idée maîtresse de cette exigence est la surveillance automatisée du *système électronique BES*. Cependant, le SDT reconnaît que certains *actifs électroniques* se prêtent mal à une surveillance automatisée (par exemple une horloge GPS). C'est pourquoi une surveillance technique automatisée n'est pas exigée explicitement ; l'entité responsable peut choisir de satisfaire à cette exigence par des procédures manuelles.

Exigence E3 :

L'entité responsable doit prendre note que l'exigence d'analyse de vulnérabilité fait une distinction entre analyse sur papier et analyse active. Cette distinction s'appuie sur l'ordonnance 706 de la FERC et la proposition réglementaire (*Notice of Proposed Rulemaking*) connexe. Dans l'élaboration de son processus d'analyse de vulnérabilité, l'entité responsable

est fortement encouragée à inclure à tout le moins les éléments suivants, dont plusieurs sont mentionnés dans les normes CIP-005 et CIP-007 :

Analyse de vulnérabilité sur papier :

1. Recherche de réseau – Examen de la connectivité réseau visant à inventorier tous les *points d'accès électronique* au *périmètre de sécurité électronique*.
2. Inventaire des ports et des services réseau – Examen permettant de vérifier que tous les ports et services activés ont une justification fonctionnelle.
3. Examen des vulnérabilités – Examen des règles et des configurations de sécurité, y compris les mesures de sécurité pour les comptes par défaut, les mots de passe et les chaînes de communauté pour la gestion du réseau.
4. Examen des réseaux sans fil – Inventaire des types courants de réseaux sans fil (par exemple 802.11a, b, g et n) et examen de leurs mesures de sécurité si ces réseaux sont utilisés d'une manière quelconque pour les communications du *système électronique BES*.

Analyse de vulnérabilité active :

1. Recherche de réseau – Recours à des outils de détection active pour inventorier les dispositifs actifs et les trajets de communication afin de confirmer que l'architecture réseau constatée correspond bien à l'architecture documentée.
2. Inventaire des ports et des services réseau – Recours à des outils de détection active (par exemple Nmap) pour déterminer les ports ouverts et les services actifs.
3. Balayage des vulnérabilités – Recours à un outil de balayage des vulnérabilités pour inventorier les ports et les services accessibles par le réseau et pour repérer les vulnérabilités connues associées aux services qui exploitent ces ports.
4. Balayage des réseaux sans fil – Recours à un outil de balayage pour inventorier les signaux et les réseaux sans fil dans le périmètre physique d'un *système électronique BES*. Permet de repérer les appareils sans fil non autorisés situés dans la portée de l'outil de balayage.

En outre, les entités responsables sont fortement encouragées à consulter la publication SP800-115 du NIST pour de plus amples renseignements sur la manière d'effectuer une analyse de vulnérabilité.

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 :

Les processus de gestion des changements de configuration visent à empêcher les modifications non autorisées aux *systèmes électroniques BES*.

Référence à une version précédente : (Partie 1.1) Nouvelle exigence

Justification des modifications : (Partie 1.1)

L'exigence de configuration de référence provient du Catalog of Control Systems Security du Department of Homeland Security. Cette exigence vise aussi à préciser dans quel contexte un processus de gestion des changements est exigé et quels éléments de configuration doivent être examinés.

Référence à une version précédente : (Partie 1.2) CIP-007-3, E9 ; CIP-003-3, E6

Justification des modifications : (Partie 1.2)

Le SDT a ajouté l'exigence d'une autorisation explicite des changements. Cette exigence était auparavant implicite dans l'exigence E6 de la norme CIP-003-3.

Référence à une version précédente : (Partie 1.3) CIP-007-3, E9 ; CIP-005-3, E5

Justification des modifications : (Partie 1.3)

L'exigence de tenue à jour de la documentation selon les changements apportés à un *système électronique BES* est équivalente aux exigences des versions précédentes des normes CIP.

Référence à une version précédente : (Partie 1.4) CIP-007-3, E1

Justification des modifications : (Partie 1.4)

Le SDT a voulu préciser à quel moment les essais doivent être effectués et a retiré la prescription de procédures d'essai particulières, celle-ci étant implicite dans la mise en œuvre de l'exigence.

Référence à une version précédente : (Partie 1.5) CIP-007-3, E1

Justification des modifications : (Partie 1.5)

Cette exigence précise quand des essais doivent avoir lieu et prescrit des essais supplémentaires pour gérer adéquatement les conséquences accidentelles des changements planifiés.

Ce changement tient compte de l'ordonnance 706 de la FERC, paragraphes 397, 609, 610 et 611.

Raisonnement pour E2 :

Le processus de surveillance de la configuration vise à détecter les modifications non autorisées aux *systèmes électroniques BES*.

Référence à une version précédente : (Partie 2.1) Nouvelle exigence

Justification des modifications : (Partie 2.1)

L'exigence de surveillance de la configuration des *systèmes électroniques BES* vient affirmer qu'il faut tenir compte des actions malveillantes autant que des changements intentionnels.

Cette exigence a été ajoutée après consultation du Catalog of Control Systems Security du Department of Homeland Security et pour tenir compte de l'ordonnance 706 de la FERC, paragraphe 397.

Le délai de 35 jours civils permet d'établir une fréquence mensuelle, avec une certaine souplesse pour tenir compte des mois de 31 jours ou des mois qui commencent ou se terminent pendant une fin de semaine.

Raisonnement pour E3 :

Les processus d'analyse de vulnérabilité doivent être intégrés à un programme général visant un contrôle périodique de la bonne mise en œuvre des mécanismes de cybersécurité et l'amélioration continue de la posture de sécurité des *systèmes électroniques BES*.

Les analyses de vulnérabilité effectuées dans le contexte de cette exigence peuvent faire partie d'un programme de détection, d'évaluation et de correction des déficiences.

Référence à une version précédente : (Partie 3.1) CIP-005-4, E4 ; CIP-007-4, E8

Justification des modifications : (Partie 3.1)

Comme le suggère l'ordonnance 706 de la FERC, paragraphe 644, les détails sur lesquels doit porter l'analyse sont laissés à discrétion.

Référence à une version précédente : (Partie 3.2) Nouvelle exigence

Justification des modifications : (Partie 3.2)

Ordonnance 706 de la FERC, paragraphes 541, 542, 543, 544, 545 et 547.

Comme le suggère l'ordonnance 706 de la FERC, paragraphe 644, les détails sur lesquels doit porter l'analyse sont laissés à discrétion.

Référence à une version précédente : (Partie 3.3) Nouvelle exigence

Justification des modifications : (Partie 3.3)

Ordonnance 706 de la FERC, paragraphes 541, 542, 543, 544, 545 et 547.

Référence à une version précédente : (Partie 3.4) CIP-005-3, E4.5 ; CIP-007-3, E8.4

Justification des modifications : (Partie 3.4)

Ajout d'une exigence quant à la date prévue d'achèvement par l'entité, conformément à l'ordonnance 706 de la FERC, paragraphe 643.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	26 novembre 2012	Adoption par le conseil d'administration de la NERC.	Cette norme encadre la gestion des changements de configuration et des analyses de vulnérabilité en coordination avec d'autres normes CIP et met en œuvre certaines dispositions de l'ordonnance 706 de la FERC.
1	22 novembre 2013	Émission d'une ordonnance de la FERC approuvant CIP-010-1 (L'ordonnance entre en vigueur le 3 février 2014)	

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

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe aura préséance.

A. Introduction

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

2. **Numéro :** CIP-010-1

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

   Entités fonctionnelles

   Aucune disposition particulière

   Installations

   La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

   Exemptions additionnelles

   Sont exemptés de l'application de la présente norme :

   - Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur un réseau voisin.
   - Postes élévateurs des installations de production identifiées au point précédent.

5. **Date d'entrée en vigueur au Québec :**

   5.1. Adoption de la norme par la Régie de l'énergie : xx mois 201x

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

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

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

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

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

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

A. Introduction

1. Titre : Cybersécurité — Protection de l'information

2. Numéro : CIP-011-1

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

4. Applicabilité :

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

4.1.1 Responsable de l'équilibrage

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

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

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

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

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

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

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

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

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

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

4.2.1.1 Chaque système de DSF ou de DST qui :

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

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

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

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

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

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

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

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

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

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

5. Dates de mise en vigueur

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

6. Contexte :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B. Exigences et mesures

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

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

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

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

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

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

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

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

C. Conformité

1. Processus de surveillance de la conformité

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

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

1.2. Conservation des pièces justificatives

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

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

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

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

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

1.4. Autres informations sur la conformité

- Aucune

2. Tableau des éléments de conformité

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

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

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

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

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

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 :

Les entités responsables sont libres d'utiliser les systèmes existants de gestion des changements et des actifs. Cependant, l'information que contiennent ces systèmes doit être évaluée, car les exigences de protection de l'information s'appliquent toujours.

La justification de cette exigence est déjà présente dans les versions précédentes des normes CIP, ainsi que dans l'ordonnance 706 de la FERC et la proposition réglementaire (*Notice of Proposed Rulemaking*) connexe.

Cette exigence stipule qu'il faut désigner l'*information de système électronique BES*. L'entité responsable dispose d'une certaine latitude quant à la mise en œuvre de cette exigence. L'entité responsable devrait expliquer par quels moyens l'*information de système électronique BES* est désignée dans son programme de protection de l'information. Par exemple, l'entité peut décider de marquer ou d'étiqueter les documents. Il n'est pas exigé d'établir des classes distinctes d'*information de système électronique BES*. Cependant, l'entité responsable est libre de le faire si elle le souhaite. Pour autant que le programme de protection de l'information englobe tous les éléments pertinents, l'entité peut aller plus loin et créer des niveaux de classification (public, confidentiel, usage interne, etc.). Si l'entité responsable choisit d'utiliser

un système de classification, elle doit documenter les classes de ce système et tout étiquetage connexe dans son programme d'*information de système électronique BES*.

L'entité responsable peut stocker toute l'information concernant les *systèmes électroniques BES* dans une archive ou un emplacement séparé (physique ou électronique) protégé par un contrôle d'accès. Par exemple, le programme de l'entité responsable pourrait spécifier que toute l'information stockée dans une archive particulière est une *information de système électronique BES*, ou que toute l'information stockée dans telle section d'une archive particulière est une *information de système électronique BES*, ou encore que toutes les copies papier de cette information sont stockées dans une partie sécurisée du bâtiment. D'autres méthodes pour la mise en œuvre de cette exigence sont suggérées à la section Mesures. Cependant, ces méthodes ne forment pas une liste exhaustive, et l'entité responsable peut recourir à d'autres moyens pour désigner l'*information de système électronique BES*.

Le SDT souhaite préciser que cette exigence ne s'applique pas à l'information accessible au public, comme les manuels de fournisseurs consultables sur des sites Web publics, non plus qu'à toute information considérée comme divulgable au grand public.

La protection de l'information englobe les versions électronique et papier. L'exigence E1.2 prescrit une ou plusieurs procédures pour la protection et la manipulation sécuritaire de l'*information de système électronique BES*, notamment le stockage, le transport et l'utilisation.

Le programme écrit de protection de l'information de l'entité doit expliquer comment celle-ci gère divers aspects de la protection de l'*information de système électronique BES*, notamment pendant le transport, afin de prévenir tout accès non autorisé, toute mauvaise utilisation ou toute corruption, et aussi pour protéger la confidentialité de l'information transmise. Par exemple, le recours à un fournisseur de service de télécommunications tiers plutôt qu'à une infrastructure détenue par l'organisation peut justifier le cryptage de l'information. L'entité peut choisir d'établir un trajet de communication de confiance pour le transport de l'*information de système électronique BES* ; ce trajet de confiance utiliserait un mécanisme d'authentification ou d'autres mesures pour assurer la sécurité pendant le transport. L'entité peut adopter d'autres mesures de protection physique, comme le transport par messager ou l'utilisation d'un contenant de transport verrouillé. La présente norme ne cherche pas à imposer un moyen particulier de sécuriser l'information pendant son transport.

Un bon programme de protection de l'information spécifie par écrit les circonstances dans lesquelles l'*information de système électronique BES* peut être partagée avec des tiers ou être utilisée par ceux-ci. L'entité ne doit diffuser ou partager l'information que selon le principe de l'accès sélectif. Par exemple, l'entité peut spécifier qu'un accord de confidentialité, une entente de non-divulgation, un contrat ou toute autre convention écrite concernant l'utilisation de l'information doit être en place entre l'entité et le tiers. Le programme de protection de l'information de l'entité doit spécifier les modalités de partage de l'*information de système électronique BES* avec des tiers ou de son utilisation par ceux-ci, par exemple une entente de non-divulgation. L'entité doit ensuite respecter son programme documenté. Ces exigences n'imposent pas un type particulier d'arrangement.

Exigence E2 :

Cette exigence permet le retrait du service des *systèmes électroniques BES* et leur analyse avec leur support intact, car cela ne constitue pas une autorisation de réutilisation. Cependant, si après analyse le support doit être réutilisé à l'extérieur d'un *système électronique BES* ou doit être éliminé, l'entité doit prendre des mesures pour empêcher la récupération non autorisée de l'*information de système électronique BES* présente sur le support.

La justification de cette exigence est déjà présente dans les versions précédentes des normes CIP, ainsi que dans l'ordonnance 706 de la FERC et la proposition réglementaire (*Notice of Proposed Rulemaking*) connexe.

Si un *actif électronique* visé est retiré du périmètre de sécurité physique avant que des mesures aient été prises pour empêcher la récupération non autorisée de l'*information de système électronique BES* ou avant que le support d'information ait été détruit, l'entité responsable doit tenir un dossier indiquant le détenteur du support d'information pendant que ce dernier se trouve hors du *périmètre de sécurité physique* avant l'application par l'entité des mesures prescrites à l'exigence E2.

On appelle « expurgation » le procédé qui consiste à éliminer l'information d'un support de données de manière à assurer raisonnablement que l'information ne pourra pas être récupérée ou reconstituée. Les moyens d'expurgation sont généralement divisés en quatre catégories : la mise au rebut, l'écrasement, la purge et la destruction. Aux fins de la présente exigence, la mise au rebut en elle-même – sauf dans certaines circonstances spéciales, comme le recours à un cryptage fort pour un disque utilisé dans un réseau de stockage (SAN) ou un autre support – ne doit jamais être jugée acceptable. Les techniques d'écrasement peuvent constituer un moyen d'expurgation adéquat pour les supports destinés à être réutilisés, tandis que les techniques de purge peuvent mieux convenir pour les supports destinés à l'élimination.

L'information suivante, tirée de la publication spéciale 800-88 du NIST, donne des précisions supplémentaires sur les types de mesures que l'entité pourrait prendre pour empêcher la récupération non autorisée de l'*information de système électronique BES* à partir de ses supports d'information :

> Écrasement : Cette méthode d'expurgation consiste à écrire des données non sensibles à la place des données existantes du support, au moyen d'un logiciel ou d'un appareil spécial. Ce procédé peut écraser ainsi non seulement l'emplacement logique du ou des fichiers en cause (par exemple, la table d'allocation de fichiers), mais aussi tous les emplacements mémoire adressables. Cette opération a pour objet de remplacer les données existantes par des données quelconques. L'écrasement n'est pas possible dans le cas d'un support endommagé ou non réinscriptible. Le type et la taille du support peuvent aussi déterminer si l'écrasement est une méthode d'expurgation convenable [800-36].
>
> Purge : La démagnétisation et l'exécution de la commande d'effacement sécurisé du microprogramme (pour les disques ATA seulement) sont des méthodes de purge

acceptables. La démagnétisation consiste à exposer le support magnétique à un fort champ magnétique afin de perturber les domaines magnétiques d'enregistrement ; ce champ magnétique est produit par un démagnétiseur. Il existe différents types de démagnétiseur (à faible puissance, à grande puissance, etc.) selon le type de support magnétique qu'ils peuvent traiter. Les démagnétiseurs comportent un aimant permanent puissant ou une bobine électromagnétique. La démagnétisation convient particulièrement pour purger un support endommagé, inopérant ou de très grande capacité, ou pour effacer rapidement des disquettes. [800-36]
La commande d'effacement sécurisé (disques ATA) et la démagnétisation sont des exemples de méthodes de purge acceptables. La démagnétisation d'un disque dur détruit habituellement celui-ci, car elle efface aussi le microprogramme qui commande le disque.

Destruction : Il existe de nombreux moyens pour détruire un support d'information. La désintégration, la pulvérisation, la fusion et l'incinération sont des procédés d'expurgation conçus pour détruire complètement le support. On les confie généralement à une entreprise agréée de destruction de produits métalliques ou d'incinération disposant des moyens techniques appropriés pour effectuer cette opération de manière efficace, sécurisée et sécuritaire. Les supports optiques, notamment les cédéroms (réinscriptibles ou non), les disques optiques (DVD) et les disques magnéto-optiques, doivent être détruits par pulvérisation, par déchiquetage transversal ou par combustion.

Dans certains cas, notamment pour de l'équipement réseau, il peut être nécessaire de consulter le fabricant pour connaître la méthode d'expurgation appropriée.

Il est de la plus grande importance que l'organisation tienne un dossier de ses activités d'expurgation afin d'empêcher la récupération non autorisée d'*information de système électronique BES*. Les entités sont fortement invitées à consulter la publication spéciale 800-88 du NIST pour de plus amples renseignements sur l'élaboration de procédés d'expurgation des supports.

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 :

L'exigence d'un programme de protection de l'information vise à empêcher tout accès non autorisé à l'*information de système électronique BES*.

Sommaire des modifications : Les exigences E4, E4.2 et E4.3 de la norme CIP 003 4 ont été transférées à l'exigence E1 de la norme CIP 011. L'exigence E4.1 de la norme CIP 003 4 a été transférée à la définition du terme « information de système électronique BES ».

Référence à une version précédente : (Partie 1.1) CIP-003-3, E4 ; CIP-003-3, E4.2

Justification des modifications : (Partie 1.1)

Le SDT a éliminé l'exigence explicite de classification, car il n'est pas nécessaire d'avoir plusieurs niveaux de protection (public, confidentiel, usage interne, etc.). Cette modification n'interdit pas pour autant les niveaux de classification, ce qui offre une plus grande souplesse pour l'intégration par l'entité du programme CIP de protection de l'information à ses activités normales.

Référence à une version précédente : (Partie 1.2) CIP-003-3, E4

Justification des modifications : (Partie 1.2)

Le SDT a remplacé la formulation « protéger les informations » par « procédures visant la protection et la manipulation sécuritaire de l'information » afin de préciser la protection requise.

Raisonnement pour E2 :

Le processus de réutilisation et d'élimination des *actifs électroniques BES* vise à empêcher toute diffusion non autorisée d'*information de système électronique BES* en cas de réutilisation ou d'élimination de ces actifs.

Référence à une version précédente : (Partie 2.1) CIP-007-3, E7.2

Justification des modifications : (Partie 2.1)

Conformément à l'ordonnance 706 de la FERC, paragraphe 631, le SDT précise qu'il s'agit d'empêcher toute récupération non autorisée d'information à partir du support. Le mot « effacer » n'est plus utilisé puisque, selon le support utilisé, l'effacement peut ne pas être un moyen suffisant pour atteindre le but visé.

Référence à une version précédente : (Partie 2.2) CIP-007-3, E7.1

Justification des modifications : (Partie 2.2)

Conformément à l'ordonnance 706 de la FERC, paragraphe 631, le SDT précise qu'il s'agit d'empêcher toute récupération non autorisée d'information à partir du support. Le mot « effacer » n'est plus utilisé puisque, selon le support utilisé, l'effacement peut ne pas être un moyen suffisant pour atteindre le but visé.

Le SDT a aussi éliminé l'exigence concernant la tenue de registres de retrait ou de redéploiement, de tels registres étant considérés comme une mesure d'attestation de l'exigence en vigueur, et non comme une exigence à proprement parler.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	26 novembre 2012	Adoption par le conseil d'administration de la NERC	Cette norme définit les exigences de protection de l'information en coordination avec d'autres normes CIP et met en œuvre certaines dispositions de l'ordonnance 706 de la FERC.
1	22 novembre 2013	Émission d'une ordonnance de la FERC approuvant CIP-010-1 (L'ordonnance entre en vigueur le 3 février 2014)	

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

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe aura préséance.

A. Introduction

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

2. **Numéro :** CIP-011-1

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

   Entités fonctionnelles

   Aucune disposition particulière

   Installations

   La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

   Exemptions additionnelles

   Sont exemptés de l'application de la présente norme :

   - Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur un réseau voisin.
   - Postes élévateurs des installations de production identifiées au point précédent.

5. **Date d'entrée en vigueur au Québec :**

   5.1. Adoption de la norme par la Régie de l'énergie : xx mois 201x

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

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

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

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

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

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

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