NORMES DE FIABILITÉ DE LA NERC

(VERSION FRANÇAISE)

A. Introduction

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

2. Numéro : CIP-003-6

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 *système de production-transport d'électricité* (*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* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale ; et

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

4.1.2.2 Chaque *automatisme de réseau* (SPS) ou *plan de défense* (RAS) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

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

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

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

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

4.1.5 ***Coordonnateur des échanges* ou *responsable des échanges***

4.1.6 ***Coordonnateur de la fiabilité***

4.1.7 ***Exploitant de réseau de transport***

4.1.8 ***Propriétaire d'installation de transport***

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

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

4.2.1.1 Chaque système de DSF ou de DST qui :

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

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

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les *distributeurs* :

Toutes les *installations* du *BES*.

4.2.3 Exemptions : Sont exemptés de la norme CIP-003-6 :

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

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

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

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

5. Dates d'entrée en vigueur :

Voir le plan de mise en œuvre de la norme CIP-003-6.

6. Contexte :

La norme CIP-003 fait partie d'une série de normes CIP sur la cybersécurité qui exigent la détermination et la catégorisation initiales des *systèmes électroniques BES*. Ces normes exigent aussi un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.

Le mot « politique » désigne un ou plusieurs documents écrits qui servent à communiquer les buts, objectifs et attentes de gestion de l'entité responsable quant à la manière dont celle-ci entend protéger ses systèmes électroniques BES. L'adoption de politiques permet aussi d'établir un cadre de gouvernance global qui favorise le développement d'une culture de sécurité et de conformité aux lois, règlements et normes.

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité doit inclure tout ce qu'elle juge nécessaire dans ses processus documentés, en s'assurant de bien couvrir les exigences pertinentes.

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

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont des exemples qui figurent dans les normes. La mise en œuvre complète des normes de fiabilité 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, moyen et faible. Par exemple, un même programme de sensibilisation à la cybersécurité pourrait répondre aux exigences en formation du personnel concernant plusieurs *systèmes électroniques BES*.

Les mesures présentent des exemples de pièces justificatives attestant 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 doivent 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 *BES*. Un examen des tolérances des 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 doit réexaminer 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 non-conformité : moyen] [Horizon : planification de l'exploitation]*

1.1 Pour ses systèmes électroniques BES à impact élevé ou moyen, le cas échéant :

1.1.1. personnel et formation (CIP-004) ;

1.1.2. *périmètres de sécurité électronique* (CIP-005), y compris l'*accès distant interactif ;*

1.1.3. sécurité physique des *systèmes électroniques BES* (CIP-006) ;

1.1.4. gestion de la sécurité des systèmes (CIP-007) ;

1.1.5. déclaration des incidents et planification des mesures d'intervention (CIP-008) ;

1.1.6. plans de rétablissement des *systèmes électroniques BES* (CIP-009) ;

1.1.7. gestion des changements de configuration et analyses de vulnérabilité (CIP-010) ;

1.1.8. protection de l'information (CIP-011) ; et

1.1.9. déclaration et réponse aux *circonstances CIP exceptionnelles*.

1.2 Pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, le cas échéant :

1.2.1. sensibilisation à la cybersécurité ;

1.2.2. mesures de sécurité physique ;

1.2.3. contrôle des accès électroniques pour toute *connectivité externe routable à impact faible* (*LERC*) et la *connectivité par lien commuté* ; et

1.2.4. intervention en cas d'*incident de cybersécurité*.

M1. Exemples non limitatifs de pièces justificatives : documents de politique ; historique de révisions, dossiers d'examen ou preuves de flux de travail provenant d'un système de gestion documentaire qui attestent le réexamen de chaque politique de cybersécurité au moins une fois tous les 15 mois civils ; et approbation documentée de chaque politique de cybersécurité par le *cadre supérieur CIP*.

E2. Chaque entité responsable qui détient au moins un actif comportant des *systèmes électroniques BES* à impact faible, selon les critères de la norme CIP-002, doit mettre en œuvre pour ses *systèmes électroniques BES* à impact faible un ou plusieurs plans de

cybersécurité documentés conformes à toutes les sections de l'annexe 1. *[Facteur de risque de non-conformité : faible] [Horizon : planification de l'exploitation]*

Remarque : 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. Des listes d'utilisateurs autorisés ne sont pas exigées.

M2. Les pièces justificatives doivent comporter chacun des plans de cybersécurité qui, collectivement, couvrent toutes les sections de l'annexe 1 ; d'autres pièces justificatives doivent attester la mise en œuvre des plans de cybersécurité. L'annexe 2 présente d'autres exemples de pièces justificatives pour chacune des sections de l'annexe 1.

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

M3. Exemple non limitatif de pièce justificative : 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 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 délégataires. Ces délégations doivent être documentées, et comprendre notamment le nom ou le titre du délégataire, les actes délégués et la date de la délégation ; être approuvées par le *cadre supérieur CIP* ; et être 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 non-conformité : faible] [Horizon : planification de l'exploitation]*

M4. Exemple non limitatif de pièce justificative : 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 des mesures pour assurer la conformité

Selon la définition des règles de procédure de la NERC, le terme « *responsable des mesures pour assurer la conformité* » (CEA) désigne la NERC ou l'entité régionale dans leurs rôles respectifs de surveillance de la conformité aux normes de fiabilité de la NERC.

1.2. Conservation des pièces justificatives

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

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

- Chaque entité 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 de conformité

Déclarations de non-conformité

Plaintes

1.4. Autres informations sur la conformité

Aucune.

2. Tableau des éléments de conformité

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-6)			
			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 moyen, mais il n'a pas traité de l'un des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant le réexamen précédent. (E1.1) OU L'entité responsable a fait approuver par le *cadre supérieur CIP* sa ou ses politiques de cybersécurité	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais en omettant deux des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant le réexamen précédent. (E1.1) OU L'entité responsable a fait approuver par le *cadre supérieur CIP* sa ou ses politiques de cybersécurité	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais en omettant trois des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable a terminé le réexamen de sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant le réexamen précédent. (E1.1) OU L'entité responsable a fait approuver par le *cadre supérieur CIP* sa ou ses politiques de cybersécurité	L'entité responsable a documenté et mis en œuvre une ou plusieurs politiques de cybersécurité pour ses *systèmes électroniques BES* à impact élevé et moyen, mais en omettant au moins quatre des neuf thèmes indiqués à l'exigence E1. (E1.1) OU L'entité responsable n'avait aucune politique de cybersécurité documentée pour ses *systèmes électroniques BES* à impact élevé et moyen, comme le prescrit l'exigence E1. (E1.1) OU L'entité responsable n'a pas terminé le réexamen de sa ou ses politiques de cybersécurité selon l'exigence E1 dans un délai de 18 mois civils suivant le réexamen précédent. (E1) OU

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant l'approbation précédente. (E1.1) OU L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant un des quatre thèmes indiqués à l'exigence E1. (E1.2) OU L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques*	documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant l'approbation précédente. (E1.1) OU L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant deux des quatre thèmes indiqués à l'exigence E1. (E1.2) OU L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques*	documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant l'approbation précédente. (E1) OU L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant trois des quatre thèmes indiqués à l'exigence E1. (E1.2) OU L'entité responsable a terminé le réexamen, selon l'exigence E1, de sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques*	L'entité responsable n'a pas fait approuver par le *cadre supérieur CIP* sa ou ses politiques de cybersécurité documentées pour ses *systèmes électroniques BES* à impact élevé et moyen selon l'exigence E1 dans un délai de 18 mois civils suivant l'approbation précédente. (E1.1) OU L'entité responsable a documenté une ou plusieurs politiques de cybersécurité pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais en omettant les quatre thèmes indiqués à l'exigence E1. (E1.2) OU L'entité responsable n'avait aucune politique de cybersécurité documentée, selon l'exigence E1, pour ses actifs qui comportent des

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			BES à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant le réexamen précédent. (E1.2) OU L'entité responsable a fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant l'approbation précédente. (E1.2)	*BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant le réexamen précédent. (E1.2) OU L'entité responsable a fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant l'approbation précédente. (E1.2)	*BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant le réexamen précédent. (E1.2) OU L'entité responsable a fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant l'approbation précédente. (E1.2)	*systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002. (E1.2) OU L'entité responsable n'a pas fait approuver par le *cadre supérieur CIP*, selon l'exigence E1, sa ou ses politiques de cybersécurité documentées pour ses actifs qui comportent des *systèmes électroniques BES* à impact faible selon les critères de la norme CIP-002, dans un délai de 18 mois civils suivant l'approbation précédente. (E1.2)
E2	**Planification de l'exploitation**	**Faible**	L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques* BES à impact faible, mais n'a pas documenté son plan de sensibilisation à la cybersécurité	L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas fait de rappel des pratiques de cybersécurité au moins une fois tous les 15 mois	L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas	L'entité responsable n'a pas documenté ou mis en œuvre un ou plusieurs plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible conformément à l'annexe 1 portant sur l'exigence E2 de

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			conformément à la section 1 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* conformément à la section 4 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2) OU L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas mis à jour chaque plan d'intervention en cas d'*incident de cybersécurité*	civils conformément à la section 1 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2) OU L'entité responsable a documenté un ou plusieurs plans d'intervention en cas d'incident dans le cadre de son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas inclus le processus de détection, de classement et d'intervention en cas d'*incident de cybersécurité* conformément à la section 4 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté le processus consistant à déterminer si	mis à l'essai chaque plan d'intervention en cas d'*incident de cybersécurité* au moins une fois tous les 36 mois civils conformément à la section 4 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2) OU L'entité responsable a documenté le processus consistant à déterminer si un *incident de cybersécurité* constaté est un *incident de cybersécurité à déclarer*, mais n'a pas avisé l'Electricity Sector Information Sharing and Analysis Center (ES-ISAC) conformément à la section 4 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2) OU L'entité responsable a documenté et mis en œuvre un contrôle des accès électroniques pour les *LERC*, mais n'a pas mis en place un *LEAP* ou géré les	la norme CIP-003-6. (E2)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			dans un délai de 180 jours conformément à la section 4 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)	un *incident de cybersécurité* constaté est un *incident de cybersécurité à déclarer*, puis à en aviser l'Electricity Sector Information Sharing and Analysis Center (ES-ISAC) conformément à la section 4 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté de mesures de sécurité physique conformément à la section 2 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2) OU L'entité responsable a documenté son ou ses plans de cybersécurité pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté le contrôle des	accès entrants et sortants conformément à la section 3 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2) OU L'entité responsable a documenté et mis en œuvre un contrôle des accès électroniques pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas documenté et mis en place une authentification pour toutes les *connectivités par lien commuté* (s'il en existe) qui donnent accès à des *systèmes électroniques BES* à impact faible, conformément à la section 3 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2) OU L'entité responsable a documenté le contrôle des accès physiques pour ses actifs comportant des *systèmes électroniques BES* à impact faible, mais n'a pas	

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				accès électroniques conformément à la section 3 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)	mis en œuvre les mesures de sécurité physique conformément à la section 2 de l'annexe 1 portant sur l'exigence E2 de la norme CIP-003-6. (E2)	
E3	**Planification de l'exploitation**	**Moyen**	L'entité responsable a désigné nominativement un *cadre supérieur CIP*, mais a documenté un changement concernant celui-ci dans un délai de plus de 30 jours civils et de moins de 40 jours civils suivant ce changement. (E3)	L'entité responsable a désigné nominativement un *cadre supérieur CIP*, mais a documenté un changement concernant celui-ci dans un délai de plus de 40 jours civils et de moins de 50 jours civils suivant ce changement. (E3).	L'entité responsable a désigné nominativement un *cadre supérieur CIP*, mais a documenté un changement concernant celui-ci dans un délai de plus de 50 jours civils et de moins de 60 jours civils suivant ce changement. (E3).	L'entité responsable n'a pas désigné nominativement un *cadre supérieur CIP*. OU L'entité responsable a désigné nominativement un *cadre supérieur CIP*, mais n'a pas documenté un changement concernant celui-ci dans un délai de 60 jours civils suivant ce changement.

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-003-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E4	**Planification de l'exploitation**	**Faible**	L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais a documenté un changement à la délégation dans un délai de plus de 30 jours civils et de moins de 40 jours civils suivant ce changement. (E4)	L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais a documenté un changement à la délégation dans un délai de plus de 40 jours civils et de moins de 50 jours civils suivant ce changement. (E4)	L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais a documenté un changement à la délégation dans un délai de plus de 50 jours civils et de moins de 60 jours civils suivant ce changement. (E4)	L'entité responsable a délégué des pouvoirs relatifs à des actes autorisés par les normes CIP, mais n'a pas mis en œuvre de processus pour la délégation des actes du *cadre supérieur CIP*. (E4) OU L'entité responsable a désigné un délégataire en indiquant son nom, son titre, la date de la délégation et les actes délégués, mais n'a pas documenté un changement à la délégation dans un délai de 60 jours civils suivant le changement. (E4)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

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 des mesures pour assurer la conformité* ».	
3	16 décembre 2009	Changement du numéro de version de -2 à -3. Dans l'exigence E1.6, suppression de la phrase concernant le retrait du service d'un composant ou d'un système aux fins d'essais, en réponse 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.	Modification en coordination avec les autres normes CIP et révision du format selon le modèle RBS.
5	22 novembre 2013	Ordonnance de la FERC approuvant la norme CIP-003-5.	
6	13 novembre 2014	Adoption par le Conseil d'administration de la NERC.	Mise en œuvre de deux prescriptions de l'ordonnance 791 de la FERC concernant l'obligation de « détecter, évaluer et corriger » ainsi que les réseaux de communication
6	12 février 2015	Adoption par le Conseil d'administration de la NERC.	Remplace la version adoptée par le Conseil le 13 novembre 2014. La version à jour met en œuvre des prescriptions en instance de l'ordonnance 791 relativement aux actifs temporaires et aux *systèmes électroniques BES* à impact faible.
6	21 janvier 2016	Ordonnance de la FERC émise approuvant CIP-003-6. Dossier no. RM15-14-000	

CIP-003-6 – Annexe 1

Exigences des plans de cybersécurité pour les actifs comportant des *systèmes électroniques BES* à impact faible

Les entités responsables doivent intégrer chacune des sections suivantes aux plans de cybersécurité prescrits à l'exigence E2.

Les entités responsables dont les *systèmes électroniques BES* appartiennent à plusieurs catégories d'impact peuvent utiliser les politiques, procédures et processus adoptés pour leurs *systèmes électroniques BES* à impact élevé ou moyen pour leurs plans de cybersécurité visant les systèmes à faible impact. Chaque entité responsable peut élaborer des plans de cybersécurité pour des actifs individuels ou pour des groupes d'actifs.

Section 1. Sensibilisation à la cybersécurité : Chaque entité responsable doit rappeler, au moins une fois tous les 15 mois civils, les pratiques de cybersécurité (lesquelles peuvent comprendre des pratiques de sécurité physiques connexes).

Section 2. Mesures de sécurité physique : Chaque entité responsable doit contrôler l'accès physique, d'après les besoins qu'elle détermine elle-même, 1) à l'actif ou aux emplacements des *systèmes électroniques BES* à impact faible à l'intérieur de l'actif, et 2) aux *points d'accès électronique de système électronique BES à impact faible* (*LEAP*), s'il en existe.

Section 3. Contrôle des accès électroniques : Chaque entité responsable doit :

3.1 pour toute *LERC*, mettre en place un *LEAP* afin de permettre uniquement les accès entrants et sortants bidirectionnels par protocole routable nécessaires ; et

3.2 mettre en place une authentification pour toute *connectivité par lien commuté* qui donne accès à des *systèmes électroniques BES* à impact faible, selon les capacités de l'*actif électronique*.

Section 4. Intervention en cas d'incident de cybersécurité : Chaque entité responsable doit avoir un ou plusieurs plans d'intervention en cas d'incident de cybersécurité, par actif ou par groupe d'actifs, qui doivent comprendre :

4.1 la détection et le classement des *incidents de cybersécurité*, ainsi que les mesures d'intervention ;

4.2 le processus consistant à déterminer si un *incident de cybersécurité* détecté est un *incident de cybersécurité à déclarer*, puis à en aviser l'Electricity Sector Information Sharing and Analysis Center (ES-ISAC), à moins que la loi ne l'interdise ;

4.3 l'établissement des rôles et responsabilités des groupes ou des personnes chargés d'intervenir en cas d'*incident de cybersécurité* ;

4.4 la gestion des *incidents de cybersécurité* ;

4.5 la mise à l'essai des plans d'intervention en cas d'*incident de cybersécurité* au moins une fois tous les 36 mois civils : 1) en répondant à un *incident de cybersécurité à déclarer* réel ; 2) en effectuant un exercice d'entraînement ou sur table de réponse à un *incident de cybersécurité à déclarer* ; ou 3) en effectuant un exercice opérationnel de réponse à un *incident de cybersécurité à déclarer* ; et

4.6 la mise à jour des plans d'intervention en cas d'*incident de cybersécurité*, au besoin, dans les 180 jours civils suivant la mise à l'essai d'un plan d'intervention en cas d'*incident de cybersécurité* ou suivant un *incident de cybersécurité à déclarer* réel.

CIP-003-6 – Annexe 2

Plans de cybersécurité pour les actifs comportant des *systèmes électroniques BES* à impact faible – Exemples de pièces justificatives

Section 1 – Sensibilisation à la cybersécurité – Exemples non limitatifs de pièces justificatives pour la section 1 : documentation attestant que le rappel des pratiques de cybersécurité a été fait au moins une fois tous les 15 mois civils. Les pièces justificatives peuvent porter sur une ou plusieurs des méthodes suivantes :

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

Section 2 – Mesures de sécurité physique – Exemples non limitatifs de pièces justificatives pour la section 2 :

- documentation des mécanismes de contrôle d'accès (carte d'accès, serrures, sécurisation de périmètre, etc.), des mesures de surveillance (systèmes d'alarme, surveillance humaine, etc.) ou d'autres mesures de sécurité physique de nature opérationnelle, administrative ou technique pour le contrôle de l'accès physique :
    a. à l'actif, s'il y a lieu, ou aux emplacements de *système électronique BES* à impact faible à l'intérieur de l'actif ; et
    b. à l'*actif électronique*, le cas échéant, qui comporte un *LEAP*.

Section 3 – Contrôles des accès électroniques – Exemples non limitatifs de pièces justificatives pour la section 3 :

- documentation attestant que des connexions entrantes et sortantes de tout *LEAP* sont limitées à celles que l'entité responsable juge nécessaires (restriction des adresses IP, des ports ou des services, etc.) ; et documentation du mécanisme d'authentification de la *connectivité par lien commuté* (appels sortants limités à un numéro préprogrammé pour la transmission de données, modems à fonction de rappel, modems télécommandés par le centre de contrôle ou la salle de commande, contrôle d'accès dans le *système électronique BES*, etc.).

Section 4 – Intervention en cas d'incident de cybersécurité – Exemples non limitatifs de pièces justificatives pour la section 4 : documents datés (politiques, procédures, processus, etc.) d'un ou de plusieurs plans d'intervention en cas d'*incident de cybersécurité* établis par actif ou par groupe d'actifs, qui comprennent les actions suivantes :

1. détecter les *incidents de cybersécurité*, les classer et y répondre ; déterminer si un *incident de cybersécurité* détecté est un *incident de cybersécurité à déclarer* et aviser l'Electricity Sector Information Sharing and Analysis Center (ES-ISAC) ;

2. établir et documenter les rôles et responsabilités des groupes ou des personnes chargés d'intervenir en cas d'*incident de cybersécurité* (déclenchement, documentation, surveillance, déclaration, etc.) ;
3. gérer les *incidents de cybersécurité* (confinement, élimination, reprise après incident ou résolution de l'incident, etc.) ;
4. mettre à l'essai le ou les plans, avec documents datés attestant qu'un essai a été fait au moins une fois tous les 36 mois civils ; et
5. mettre à jour au besoin les plans d'intervention en cas d'*incident de cybersécurité* dans les 180 jours civils suivant la mise à l'essai ou suivant un *incident de cybersécurité à déclarer* réel.

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) présente 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, les normes CIP sur la cybersécurité de la NERC s'y appliquent. Il est à noter qu'en ce qui concerne les *distributeurs*, la section 4.1 limite l'applicabilité 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 qui, selon la section 4.1, 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* » dans le glossaire de la NERC indique déjà qu'il s'agit d'*éléments* du *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 aide à clarifier quels sont les *installations*, systèmes et équipements visés par les normes.

Exigence E1

Lors de l'élaboration des politiques prescrites à l'exigence E1, le nombre de politiques et leur contenu doivent être guidés par la structure de gestion de l'entité responsable et par son contexte opérationnel. Ces politiques peuvent être intégrées à un programme général de sécurité de l'information pour l'ensemble de l'organisation, ou encore à des programmes particuliers. L'entité responsable a le choix d'élaborer une politique de cybersécurité monolithique qui englobe les thèmes prescrits, 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-003-6.

Si une entité responsable détient des *systèmes électroniques BES* à impact élevé ou moyen, la ou les politiques de cybersécurité doivent couvrir les neuf thèmes prescrits à la partie 1.1 de l'exigence E1 de la norme CIP 003-6. Si une entité responsable a désigné, selon les critères de la norme CIP-002, des actifs comportant des *systèmes électroniques BES* à impact faible, la ou les politiques de cybersécurité doivent couvrir les quatre thèmes prescrits à la partie 1.2 de l'exigence E1.

Les entités responsables qui ont des *systèmes électroniques BES* pour différentes catégories d'impact ne sont pas tenues de créer des politiques de cybersécurité distinctes pour les *systèmes électroniques BES* à impact faible, moyen et élevé. Les entités responsables ont la possibilité d'élaborer des politiques qui s'appliquent à la fois aux trois catégories d'impact.

La mise en œuvre de la politique de cybersécurité n'est pas traitée explicitement dans l'exigence E1 de la norme CIP-003-6, car on considère qu'elle se manifestera dans la bonne mise en œuvre des normes CIP-003 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 de fiabilité de la NERC sur la cybersécurité, mais plutôt à élaborer une politique de cybersécurité globale appropriée à leur organisation. Les éléments d'une politique qui s'étendent au-delà de la portée des normes de fiabilité de la NERC sur la cybersécurité ne seront pas considérés comme donnant lieu à des infractions potentielles ; ils aideront plutôt à témoigner de la culture de conformité au sein de de l'organisation et de sa posture de cybersécurité.

Dans le contexte de la partie 1.1, l'entité responsable devrait tenir compte des points suivants pour chacun des thèmes obligatoires dans sa ou ses politiques de cybersécurité visant ses *systèmes électroniques BES* à impact moyen et élevé :

1.1.1 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

1.1.2 *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 les systèmes 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 contractuels 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

1.1.3 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

1.1.4 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*

1.1.5 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*

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

- Disponibilité des composants de rechange
- Disponibilité des sauvegardes système

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

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

1.1.8 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

1.1.9 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

Les exigences relatives aux dérogations aux politiques de sécurité d'une entité responsable ont été retirées puisqu'il s'agit d'un enjeu de gestion générale qui ne relève pas des exigences de fiabilité. Il s'agit d'une exigence de politique interne et non d'une exigence de fiabilité. Cependant, les entités responsables sont invitées à maintenir cette pratique dans le cadre de leurs politiques de cybersécurité.

Dans le cas présent, et pour toutes les approbations subséquentes exigées par les normes de fiabilité 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

À partir de la liste des actifs comportant des *systèmes électroniques BES* à impact faible établie selon la norme CIP-002, chaque entité responsable doit créer, documenter et mettre en œuvre un ou plusieurs plans de cybersécurité fondés sur des critères objectifs et visant à protéger les *systèmes électroniques BES* à impact faible. Les protections requises par l'exigence E2 sont liées au degré de risque pour le *BES* en cas de mauvaise utilisation ou d'indisponibilité des *systèmes électroniques BES* à impact faible. Le but recherché est que les protections exigées fassent partie d'un programme qui vise les *systèmes électroniques BES* à impact faible de façon collective, au niveau de l'actif ou du site (actifs comportant des *systèmes électroniques BES* à impact faible), et non au niveau des appareils ou des systèmes individuels.

Le plan de cybersécurité doit couvrir quatre grands thèmes, présentés à l'annexe 1 : 1) la sensibilisation à la cybersécurité, 2) les mesures de sécurité physique, 3) le contrôle des accès électroniques pour les *LERC* et la *connectivité par lien commuté*, et 4) l'intervention en cas d'*incident de cybersécurité*.

Exigence E2, annexe 1

Comme il est indiqué, l'annexe 1 présente les sections à inclure dans tout plan de cybersécurité. Il s'agit de donner aux entités qui ont une combinaison de *systèmes électroniques BES* à impact faible, moyen et élevé la possibilité, si elles le souhaitent, d'appliquer à leurs *systèmes électroniques BES* à impact faible (ou à une partie de ceux-ci) les programmes qu'elles ont établis pour les *systèmes électroniques BES* à impact moyen ou élevé, plutôt que de devoir gérer deux programmes différents. Des précisions et éclaircissements pour chacun des quatre thèmes de l'annexe 1 sont présentés ci-après.

Exigence E2, section 1 de l'annexe 1 – Sensibilisation à la cybersécurité

Le programme de sensibilisation à la cybersécurité oblige les entités à rappeler les bonnes pratiques de cybersécurité à leur personnel au moins une fois tous les 15 mois civils. L'entité est libre de choisir les thèmes à couvrir et la manière de communiquer les rappels sur ces thèmes. Quant aux pièces justificatives de conformité, l'entité responsable doit pouvoir présenter le matériel de sensibilisation utilisé, selon la ou les méthodes de communication (affiches, courriels, sujets abordés aux réunions de service, etc.). L'entité responsable n'est pas obligée de tenir des listes de destinataires ni de confirmer la réception par le personnel du matériel de sensibilisation.

Bien que la sensibilisation concerne en particulier la cybersécurité, des thèmes non technologiques ne sont pas à exclure pour autant. Des thèmes appropriés de sécurité physique (sensibilisation au talonnage, protection des cartes d'accès physique, campagnes d'incitation à signaler tout fait suspect, etc.) renforcent aussi la sensibilisation à la cybersécurité. Le but recherché est d'aborder des thèmes pertinents aux différents aspects de la protection des

systèmes électroniques BES.

Exigence E2, section 2 de l'annexe 1 – Mesures de sécurité physique

L'entité responsable doit documenter et mettre en œuvre des mesures de contrôle de l'accès physique 1) aux *systèmes électroniques BES* à impact faible à l'intérieur d'actifs qui comportent de tels systèmes, et 2) aux *LEAP*, s'il en existe. Si le *LEAP* est situé à l'intérieur de l'actif du *BES* et qu'il hérite des mêmes mesures de contrôle d'accès selon la section 2, l'entité responsable peut en tenir compte dans ses politiques ou ses plans de cybersécurité afin d'éviter une documentation redondante des mêmes mesures.

L'entité responsable est libre de choisir les méthodes à utiliser pour atteindre l'objectif de contrôler l'accès physique aux actifs comportant des *systèmes électroniques BES* à impact faible, aux *systèmes électroniques BES* à impact faible eux-mêmes, ou encore aux *LEAP*, s'il en existe. L'entité responsable peut utiliser une ou plusieurs mesures de contrôle d'accès, mesures de surveillance ou autres mesures de sécurité physique de nature opérationnelle, administrative ou technique. Les entités peuvent appliquer des mesures de contrôle d'accès physique à des périmètres étendus (clôtures avec barrières verrouillées, gardiens, politiques d'accès aux sites, etc.) ou encore à des zones plus circonscrites où sont situés les *systèmes électroniques BES* à impact faible, comme les salles de commande ou les centres de contrôle. Il n'est pas exigé d'avoir des programmes d'autorisation des utilisateurs et des listes d'utilisateurs autorisés à un accès physique, bien que ces mesures soient à envisager pour répondre à l'objectif de sécurité.

L'objectif visé est de contrôler l'accès physique d'après les besoins déterminés par l'entité responsable. Les besoins peuvent être documentés au niveau des politiques d'accès au site ou aux systèmes, y compris les *LEAP*. L'exigence n'oblige pas l'entité à spécifier un besoin pour chaque accès ou autorisation d'accès d'un utilisateur.

La surveillance comme mesure de sécurité physique peut servir de complément ou de solution de rechange au contrôle d'accès. Exemples non limitatifs de mesures de surveillance :
1) systèmes d'alarme sensibles au mouvement ou à l'entrée dans la zone contrôlée ou
2) surveillance humaine de la zone contrôlée. La surveillance n'oblige pas nécessairement à tenir des registres, mais pourrait comprendre la détection qu'un accès physique a eu lieu ou été tenté (alarme de porte, surveillance humaine, etc.). Il n'est pas nécessaire d'avoir une surveillance pour chaque *système électronique BES* à impact faible, mais la surveillance doit être au niveau approprié pour atteindre l'objectif de sécurité.

Exigence E2, section 3 de l'annexe 1 – Contrôle des accès électroniques

La section 3 exige la mise en place de protections périmétriques pour les *systèmes électroniques BES* à impact faible lorsque ceux-ci ont une communication bidirectionnelle par protocole routable ou une *connectivité par lien commuté* avec des appareils situés à l'extérieur de l'actif dans lequel se trouvent des *systèmes électroniques BES* à impact faible. Les protections périmétriques contrôlent les communications soit vers un actif comportant des *systèmes électroniques BES* à impact faible, soit vers les *systèmes électroniques BES* à impact faible eux-mêmes, afin de réduire les risques associés à une communication non contrôlée au moyen de protocoles routables ou d'une *connectivité par lien commuté*. 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. L'entité responsable n'est pas obligée d'établir une communication *LERC* ou un *LEAP* en l'absence de communication bidirectionnelle par protocole routable ou de *connectivité par lien commuté* ; dans un tel cas, l'entité peut documenter l'absence d'une telle communication dans son ou ses plans de cybersécurité visant les actifs à impact faible.

Les termes définis *LERC* et *LEAP* sont utilisés pour éviter toute confusion avec des termes semblables associés aux *systèmes électroniques BES à* impact moyen ou élevé (par exemple « *connectivité externe routable* » ou « *point d'accès électronique* »). Afin de mettre les normes à l'abri des changements et des complications technologiques à l'avenir, la définition de *LERC* exclut nommément « les communications point à point entre dispositifs électroniques intelligents qui utilisent des protocoles de communication routables pour assurer des fonctions de commande ou de protection à délai critique entre des actifs de poste de transport comportant des *systèmes électroniques BES* à impact faible », comme la messagerie CEI 61850. Les communications ainsi exclues ne sont pas celles des *centres de contrôle*, mais plutôt celles entre les dispositifs électroniques intelligents eux-mêmes. Une entité responsable qui utilise cette technologie n'est pas tenue de mettre en place un *LEAP*. Cette exception a été ajoutée afin de ne pas compromettre les fonctions à délai critique associées à cette technologie, et de ne pas empêcher le recours futur à de telles fonctions afin d'améliorer la fiabilité au motif qu'elles utiliseraient un protocole routable.

Lorsqu'il s'agit de déterminer si un *système électronique BES* à impact faible comporte une *LERC*, il convient de se référer à la définition de ce terme : « accès interactif direct amorcé par l'utilisateur ou connexion directe entre appareils, vers un ou des *systèmes électroniques BES* à impact faible à partir d'un *actif électronique* situé à l'extérieur de l'actif qui comporte ce ou ces *systèmes électroniques BES* à impact faible, au moyen d'une liaison bidirectionnelle utilisant un protocole routable ». Dans cette définition, les mots « direct » et « directe » servent à indiquer qu'il y a une *LERC* si une personne utilise un autre appareil situé à l'extérieur de l'actif qui comporte le *système électronique BES* à impact faible, et que cette personne peut se connecter (pour ouvrir une session, configurer, lire, interagir, etc.) avec le *système électronique BES* à impact faible au moyen d'une seule session bidirectionnelle avec protocole routable de bout en bout, même s'il y a conversion entre une liaison série et un protocole routable. Une *LERC* existe aussi dans le cas inverse où la personne utilise le *système électronique BES* à impact faible et se connecte à un appareil situé à l'extérieur de l'actif comportant des *systèmes électroniques BES* à impact faible, au moyen d'une seule session bidirectionnelle avec protocole routable de bout en bout. En outre, l'expression « liaison directe entre appareils » indique qu'il y a une *LERC* si l'entité responsable a des appareils qui sont situés à l'extérieur de l'actif comportant le *système électronique BES* à impact faible et qui établissent une communication bidirectionnelle avec protocole routable avec le *système électronique BES* à impact faible, en accès entrant ou sortant.

Lorsqu'elle repère un *LEAP*, l'entité responsable a une certaine latitude quant au choix de l'interface pour l'*actif électronique* qui contrôle la *LERC*. Exemples non limitatifs : l'interface interne (tournée vers les *systèmes électroniques BES* à impact faible) d'un pare-feu externe ou

hôte, l'interface interne d'un routeur muni d'une liste de contrôle d'accès, ou un autre appareil de sécurité. L'entité a aussi une certaine latitude quant à l'emplacement du *LEAP*. Il n'est pas exigé que le *LEAP* soit situé dans l'actif qui comporte les *systèmes électroniques BES* à impact faible. En outre, l'entité n'est pas obligée d'établir un *LEAP* physique unique par actif comportant des *systèmes électroniques BES* à impact faible. L'entité responsable peut avoir un même *actif électronique* regroupant plusieurs *LEAP* qui contrôlent la *LERC* de plusieurs actifs comportant des *systèmes électroniques BES* à impact faible. Cependant, le fait de situer l'actif électronique regroupant plusieurs *LEAP* dans un emplacement externe, avec derrière lui plusieurs actifs comportant des *systèmes électroniques BES* à impact faible, ne doit pas avoir pour effet de rendre possible un accès non contrôlé aux actifs comportant des *systèmes électroniques BES* à impact faible qui partagent l'*actif électronique* regroupant le ou les LEAP.

Dans le modèle de référence 4, la communication passe par un convertisseur IP-série. Il y a effectivement une *LERC* dans ce modèle de référence, car le convertisseur IP-série dans ce cas ne fait rien d'autre que prolonger la communication entre le *système électronique BES* à impact faible et l'*actif électronique* situé à l'extérieur de l'actif comportant le *système électronique BES* à impact faible. Par contre, dans le modèle de référence 6, un *actif électronique* est disposé de manière à réaliser une coupure ou une interruption complète qui ne permet pas aux données de l'utilisateur ou de l'appareil d'aboutir directement au *système électronique BES* à impact faible. L'*actif électronique* dans le modèle de référence 6 empêche l'accès au *système électronique BES* à impact faible à partir de l'*actif électronique* situé à l'extérieur de l'actif comportant le *système électronique BES* à impact faible. En somme, si le convertisseur IP-série déployé ne sert qu'à relayer les données transmises, cette communication de relayage de données est alors une *LERC* et un *LEAP* est requis. Cependant, si le convertisseur IP-série impose une quelconque authentification du flux de données dans l'actif comportant le *système électronique BES* à impact faible avant que la communication puisse aboutir au *système électronique BES* à impact faible, alors ce type de mise en œuvre de convertisseur IP-série n'est pas une *LERC*.

Un *actif électronique* comportant une ou plusieurs interfaces qui remplissent seulement la fonction d'un *LEAP* ne répond pas à la définition de *système de contrôle ou de surveillance des accès électroniques* (*EACMS*) associé aux *systèmes électroniques BES* à impact moyen ou élevé, et est dispensé des exigences applicables à un *EACMS*. Cependant, un *actif électronique* peut avoir certaines interfaces qui jouent le rôle d'un *LEAP* et d'autres interfaces qui jouent le rôle d'un *point d'accès électronique* (*EAP*) pour des *systèmes électroniques BES* à impact moyen ou élevé. Dans ce cas, l'*actif électronique* serait aussi assujetti aux exigences applicables à l'*EACMS* associé aux *systèmes électroniques BES* à impact moyen ou élevé.

Exemples non limitatifs de contrôles d'accès adéquats :

- Toute *LERC* de l'actif franchit un *LEAP* qui applique des autorisations d'accès entrant et sortant explicites, ou une méthode équivalente par laquelle les liaisons entrantes et sortantes sont limitées aux seuls éléments (adresses IP, ports, services, etc.) que l'entité responsable juge nécessaires.
- Comme l'illustre le modèle de référence 1 ci-dessous, le *système électronique BES* à impact faible comporte un pare-feu hôte qui contrôle les accès entrants et sortants.

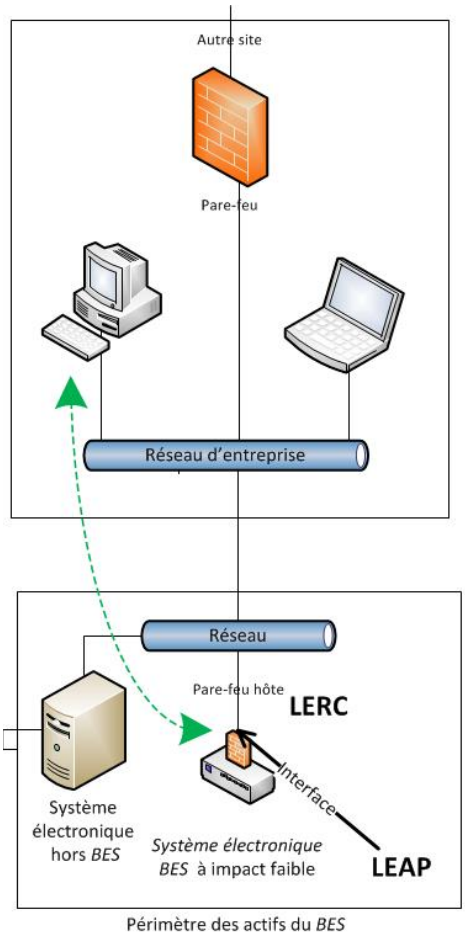
Dans ce modèle, il est également possible que le pare-feu hôte soit situé dans un *actif électronique* hors *BES*. Le but recherché est que le pare-feu hôte contrôle les accès entrants et sortants entre le *système électronique BES* à impact faible et l'actif électronique situé dans le réseau d'entreprise.

- Dans le modèle de référence 5 ci-dessous, un *actif électronique* hors *BES* est interposé entre le *système électronique BES* à impact faible situé dans le réseau du poste électrique et l'*actif électronique* situé dans le réseau d'entreprise. Le but recherché est que l'*actif électronique* hors *BES* assure une « coupure de protocole », de sorte que l'accès au *système électronique BES* à impact faible se fasse seulement à partir de l'*actif électronique* hors *BES* situé à l'intérieur de l'actif comportant le *système électronique BES* à impact faible.
- La *connectivité par lien commuté* avec un *système électronique BES* à impact faible autorise seulement les appels sortants (pas de réponse automatique) vers un numéro préprogrammé pour l'envoi de données. S'il y a *connectivité par lien commuté* entrante, elle est réalisée par un modem à fonction de rappel ou par un modem qui doit être télécommandé par le centre de contrôle ou la salle de commande, qui offre une certaine forme de contrôle d'accès ; sinon, le *système électronique BES* à impact faible doit avoir un contrôle d'accès.

Exemples non limitatifs de situations où les contrôles d'accès seraient insuffisants pour satisfaire à cette exigence :

- Un actif a une *connectivité par lien commuté* et un *système électronique BES* à impact faible est accessible par un modem à réponse automatique qui relie tout appelant à l'*actif électronique*, lequel est muni d'un mot de passe par défaut. Il n'y a pas de véritable contrôle d'accès dans cette situation.
- Un actif comporte une *LERC*, car un *système électronique BES* à l'intérieur de cet actif est équipé d'une carte sans fil reliée à un réseau de télécommunications public, ce qui rend le *système électronique BES* accessible par une adresse IP publique. Essentiellement, les *systèmes électroniques BES* à impact faible ne doivent pas être accessibles à partir d'Internet ou de moteurs de recherche comme Shodan.
- Dans le modèle de référence 5, si l'on utilise seulement des cartes d'interface à double résidence ou multiréseaux sans désactiver le réacheminement IP dans l'*actif électronique* hors *BES* à l'intérieur de la zone DMZ afin d'assurer une coupure entre le *système électronique BES* à impact faible et le réseau d'entreprise, l'exigence de « contrôle » des accès électroniques entrants et sortants ne serait pas respectée en supposant l'absence d'un pare-feu hôte ou d'un autre appareil de sécurité pour cet *actif électronique* hors *BES*.

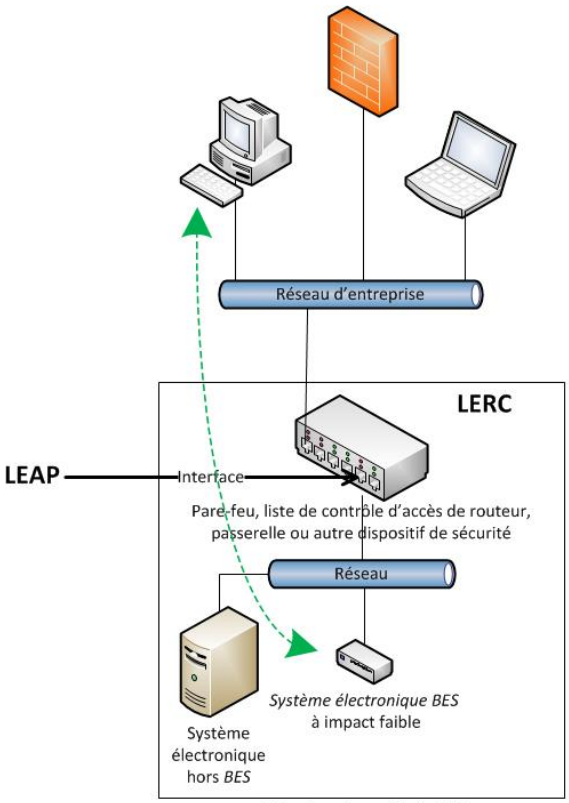
Les schémas ci-après présentent des modèles de référence qui illustrent comment on détermine s'il y a une *LERC* et comment mettre en place un *LEAP*. Ces schémas présentent plusieurs configurations possibles, mais les entités responsables pourront avoir d'autres configurations non illustrées.



Périmètre des actifs du *BES*

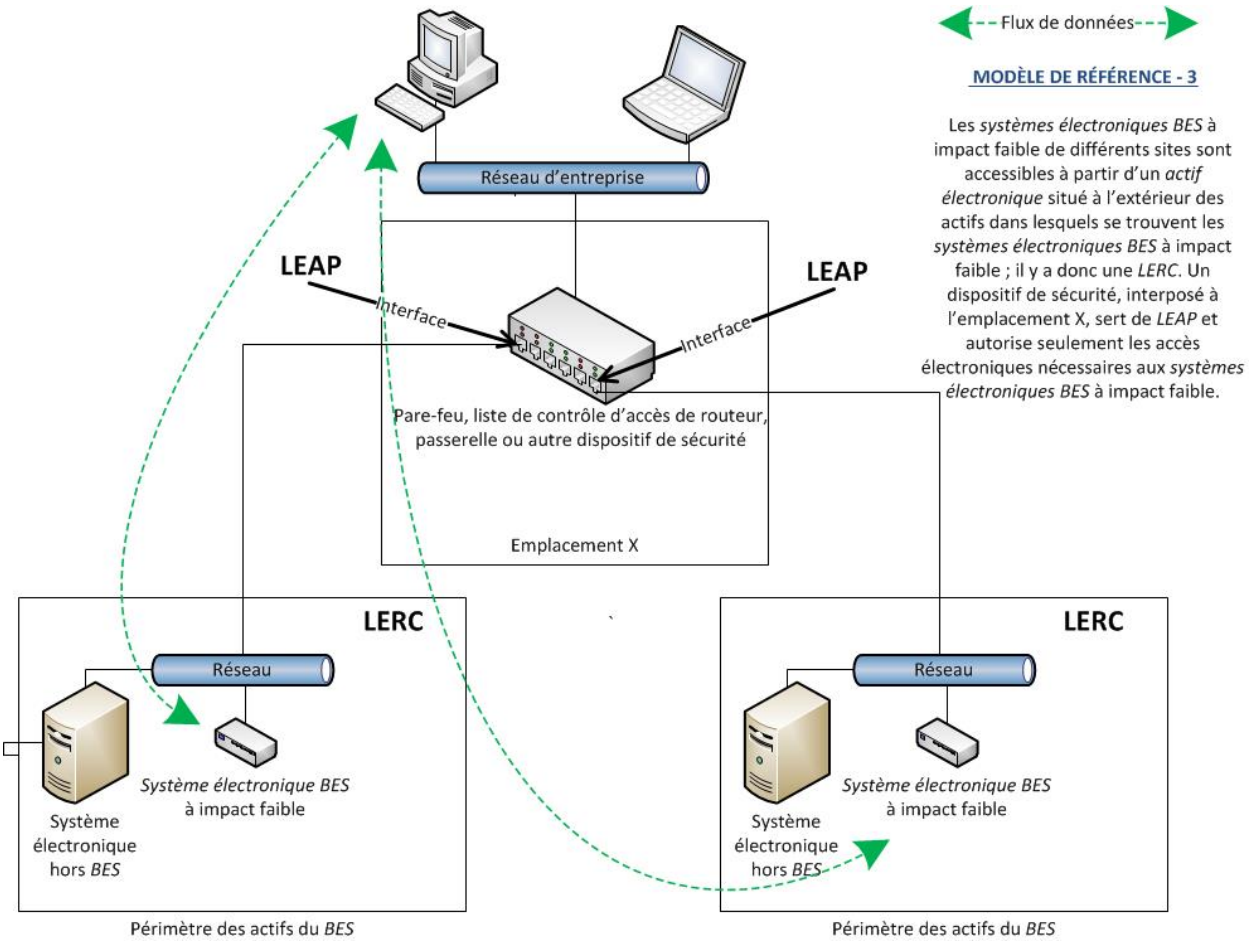
MODÈLE DE RÉFÉRENCE - 1

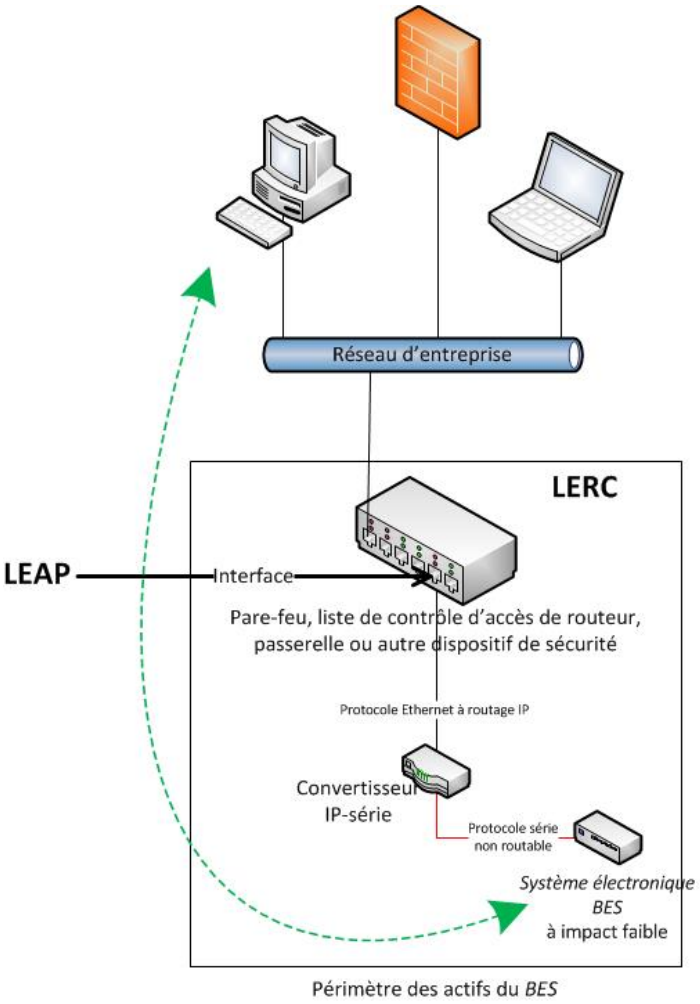
Le *système électronique BES* à impact faible est accessible à partir d'un *actif électronique* situé à l'extérieur de l'actif dans lequel se trouve le *système électronique BES* à impact faible ; il y a donc une LERC. Un pare-feu hôte, configuré à même le *système électronique BES* à impact faible, sert de *LEAP* et autorise seulement les accès électroniques nécessaires au *système électronique BES* à impact faible.



MODÈLE DE RÉFÉRENCE - 2

Le *système électronique BES* à impact faible est accessible à partir d'un *actif électronique* situé à l'extérieur de l'actif dans lequel se trouve le *système électronique BES* à impact faible ; il y a donc une *LERC*. Un dispositif de sécurité, interposé entre le réseau d'entreprise et le *système électronique BES* à impact faible, sert de *LEAP* et autorise seulement les accès électroniques nécessaires au *système électronique BES* à impact faible.

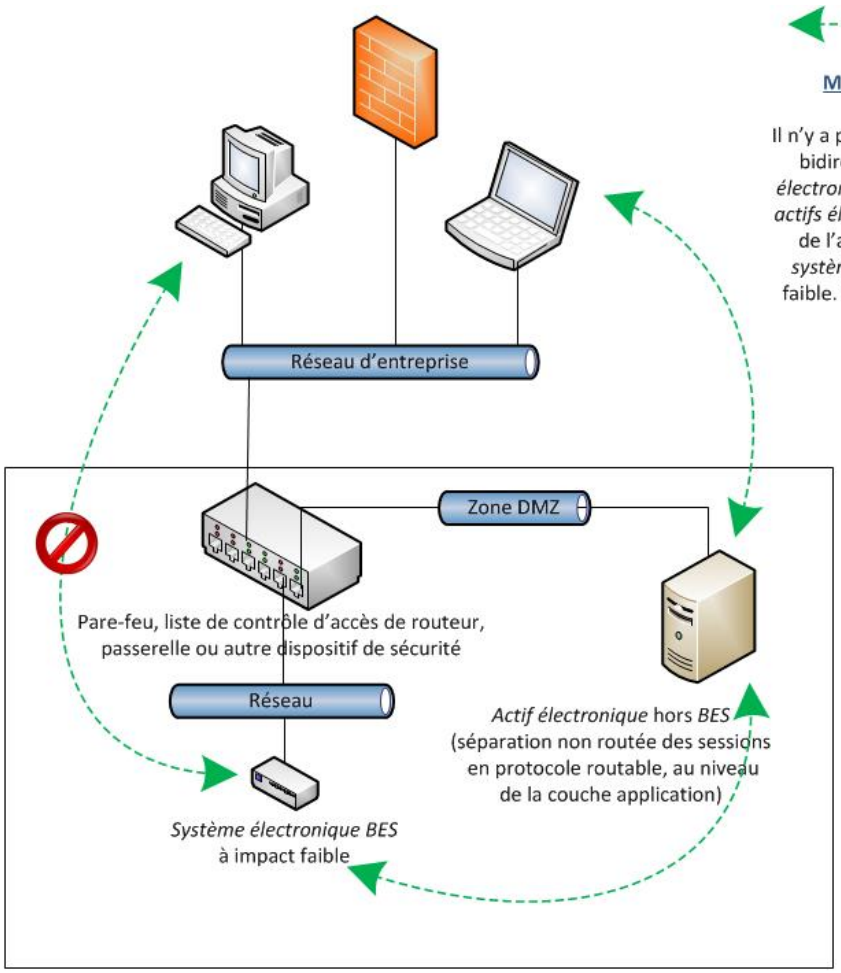

Flux de données
MODÈLE DE RÉFÉRENCE - 3
Les systèmes électroniques BES à impact faible de différents sites sont accessibles à partir d'un actif électronique situé à l'extérieur des actifs dans lesquels se trouvent les systèmes électroniques BES à impact faible ; il y a donc une LERC. Un dispositif de sécurité, interposé à l'emplacement X, sert de LEAP et autorise seulement les accès électroniques nécessaires aux systèmes électroniques BES à impact faible.
Réseau d'entreprise
LEAP
Interface
Interface
LEAP
Pare-feu, liste de contrôle d'accès de routeur, passerelle ou autre dispositif de sécurité
Emplacement X
LERC
Réseau
Système électronique BES à impact faible
Système électronique hors BES
Périmètre des actifs du BES
LERC
Réseau
Système électronique BES à impact faible
Système électronique hors BES
Périmètre des actifs du BES

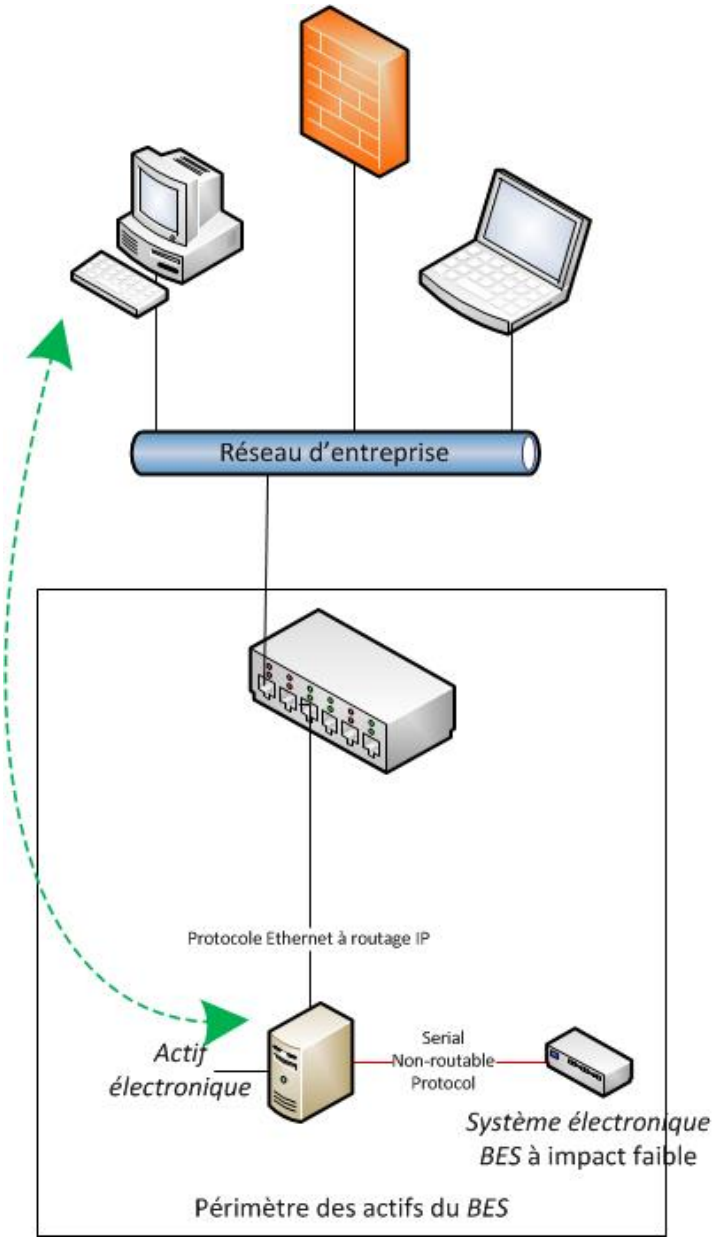


Flux de données

MODÈLE DE RÉFÉRENCE - 4

Le *système électronique BES* à impact faible est accessible à partir d'un *actif électronique* situé à l'extérieur de l'actif dans lequel se trouve le *système électronique BES* à impact faible. Il y a une *LERC*, car le convertisseur IP-série prolonge la communication entre l'*actif électronique* du réseau d'entreprise et le *système électronique BES* à impact faible, lequel est directement adressable de l'extérieur. Un dispositif de sécurité, interposé entre le réseau d'entreprise et le *système électronique BES* à impact faible, autorise seulement les accès électroniques nécessaires au *système électronique BES* à impact faible.

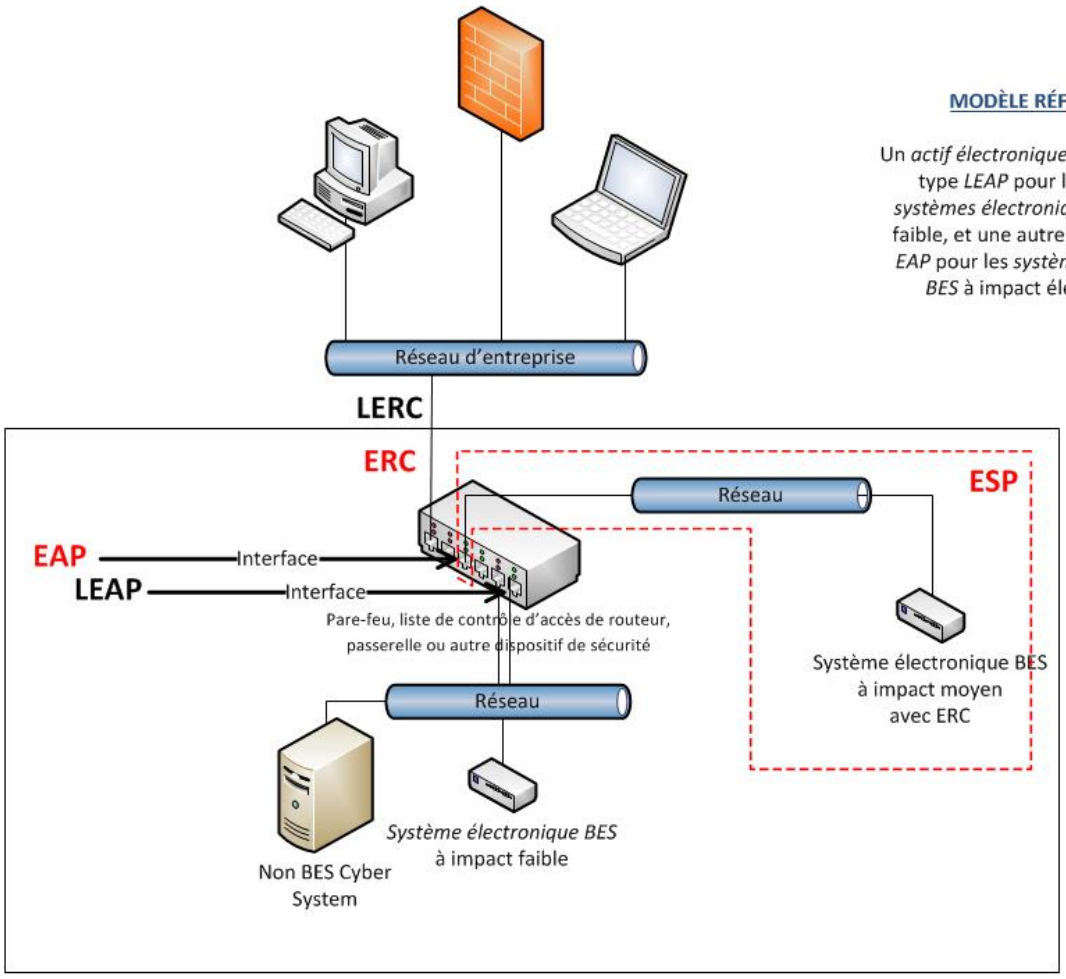

Flux de données
MODÈLE DE RÉFÉRENCE - 5
Il n'y a pas de communication routable bidirectionnelle entre le système électronique BES à impact faible et les actifs électroniques situés à l'extérieur de l'actif dans lequel se trouve le système électronique BES à impact faible. Il n'y a donc pas de LERC dans cet exemple.
Réseau d'entreprise
Zone DMZ
Pare-feu, liste de contrôle d'accès de routeur, passerelle ou autre dispositif de sécurité
Réseau
Actif électronique hors BES (séparation non routée des sessions en protocole routable, au niveau de la couche application)
Système électronique BES à impact faible
Périmètre des actifs du BES



Flux de données

MODÈLE DE RÉFÉRENCE - 6

Dans cet exemple, un *actif électronique* bloque l'accès direct au *système électronique BES* à impact faible. Il y a une coupure au niveau de la couche 7 (couche application), ou encore l'*actif électronique* exige une authentification, puis établit une nouvelle liaison avec le *système électronique BES* à impact faible. Il n'y a donc pas de *LERC* dans cet exemple.



Périmètre des actifs du *BES*

Exigence E2, section 4 de l'annexe 1 – Intervention en cas d'incident de cybersécurité

L'entité doit avoir un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* documentés couvrant chacun des thèmes indiqués à la section 4. Si, dans le cours normal des activités, on observe des opérations suspectes à un actif qui comporte des *systèmes électroniques BES* à impact faible, l'entité mettra en œuvre un plan d'intervention en cas d'*incident de cybersécurité* qui guidera son action et l'amènera à signaler l'incident s'il atteint le niveau d'un *incident de cybersécurité à déclarer*.

Les entités sont libres de segmenter leurs plans d'intervention en cas d'*incident de cybersécurité* exigés à la section 4 de l'annexe 1 par actif ou par groupe d'actifs. Il n'est pas nécessaire que les plans soient établis par site d'actifs ou par *système électronique BES* à impact faible. Les entités peuvent choisir d'adopter un seul plan à l'échelle de l'entreprise pour remplir leurs obligations relativement aux *systèmes électroniques BES* à impact faible.

Les plans doivent être mis à l'essai à intervalles de 36 mois. Il ne s'agit pas d'un exercice par *actif électronique BES* à impact faible ou par type d'*actif électronique BES*, mais plutôt un exercice pour chaque plan d'intervention en cas d'incident créé par l'entité pour satisfaire à cette exigence. Un *incident de cybersécurité à déclarer* réel compte comme essai, au même titre que d'autres essais par simulation. Les exercices dirigés par la NERC, comme la participation à

GridEx, seraient aussi acceptables comme essais pourvu que le plan d'action de l'entité soit exécuté. Cette exigence oblige les entités à tenir à jour leurs plans d'intervention en cas d'*incident de cybersécurité*, et en particulier à les modifier si nécessaire dans les 180 jours suivant un essai ou un incident réel.

Pour les *systèmes électroniques BES* à impact faible, la seule partie de la définition d'*incident de cybersécurité* qui s'appliquerait est la suivante : « acte malveillant ou incident suspect qui perturbe ou avait pour but de perturber le fonctionnement d'un *système électronique BES* ». L'autre partie de cette définition ne doit pas servir à exiger le recours à des *périmètres de sécurité électronique* ou à des *périmètres de sécurité physique* pour les *systèmes électroniques BES* à impact faible.

Exigence E3

L'esprit de l'exigence E3 de la norme CIP-003-6 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 de fiabilité 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 la justification de l'exigence E4 de la norme CIP-003-6, cette exigence vise à démontrer une chaîne d'autorité et d'imputabilité claire en matière de sécurité. L'intention de l'équipe de rédaction (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.

Justification

Pendant l'élaboration de cette norme, des zones de texte ont été incorporées à celle-ci pour exposer la justification de ses diverses parties. Après l'approbation par le Conseil d'administration, le contenu de ces zones de texte a été transféré ci-après.

Justification de l'exigence E1

Une ou plusieurs politiques de sécurité assurent une mise en œuvre efficace des exigences des normes de fiabilité sur la cybersécurité. Ces politiques visent à constituer les bases de la gestion et de la gouvernance pour toutes les exigences applicables aux *systèmes électroniques BES* de l'entité responsable. 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.

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

Justification de l'exigence E2

En réponse à l'ordonnance 791 de la FERC, l'exigence E2 demande aux entités d'élaborer et de mettre en œuvre des plans de cybersécurité afin d'atteindre des objectifs précis en matière de mécanismes de sécurité pour leurs actifs comportant des *systèmes électroniques BES* à impact faible. Les plans de cybersécurité couvrent quatre thèmes : 1) la sensibilisation à la cybersécurité ; 2) les mesures de sécurité physique ; 3) le contrôle des accès électroniques ; et 4) l'intervention en cas d'*incident de cybersécurité*. Ces plans, combinés aux politiques de cybersécurité spécifiées à la partie 1.2 de l'exigence E1, présentent un cadre pour la mise en place de mesures opérationnelles, administratives et techniques visant les *systèmes électroniques BES* à impact faible.

Considérant la diversité des *systèmes électroniques BES* à impact faible dans l'ensemble du *BES*, l'annexe 1 offre aux entités responsables une certaine latitude quant à la manière d'appliquer les mécanismes de sécurité pour atteindre les objectifs de sécurité. En outre, comme beaucoup d'entités responsables ont des *systèmes électroniques BES* pour plusieurs catégories d'impact, rien dans l'exigence ne leur interdit d'utiliser leurs politiques, procédures et processus applicables aux *systèmes électroniques BES* à impact moyen ou élevé pour les mécanismes de sécurité visant les *systèmes électroniques BES* à impact faible, comme l'explique en détail l'annexe 1 relative à l'exigence E2.

Les entités responsables utiliseront leurs actifs comportant des *systèmes électroniques BES* à impact faible (désignés selon les critères de la norme CIP-002) pour déterminer les sites ou emplacements associés à des *systèmes électroniques BES* à impact faible. Cependant, les entités responsables ne sont nullement obligées de tenir des listes de leurs *systèmes électroniques BES* à impact faible et des actifs électroniques connexes, ni de tenir une liste des utilisateurs autorisés.

Justification de l'exigence 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 de la NERC*, de telle sorte que ce terme peut être utilisé dans l'ensemble des normes CIP sans renvoi explicite.

Le paragraphe 296 de l'ordonnance 706 de la FERC 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* « dispose de l'autorité et de la responsabilité pour mener et gérer la mise en œuvre et le respect des exigences de cet ensemble de 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, etc.), la SDT est d'avis que l'exigence que le *cadre supérieur CIP* soit « un dirigeant de la société ou l'équivalent » serait extrêmement difficile à interpréter et à mettre en application de manière homogène.

Justification de l'exigence 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.

Aux paragraphes 379 et 381 de son ordonnance 706, 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 la 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.

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-003-6

3. Objet : Aucune disposition particulière

4. Applicabilité :

4.1. Entités Fonctionnelles

Aucune disposition particulière

4.2. Installations

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

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

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

5. Date d'entrée en vigueur au Québec :

5.1. Adoption de la norme par la Régie de l'énergie : xx mois 20xx

5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 20xx

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

Norme	Révision CIPv6	Date d'entrée en vigueur proposée au Québec		
		Entités visées par la version 1 des normes CIP adoptées par la Régie	Entités ne possédant pas d'installations de production à vocation industrielle et non visées par la version 1 des normes CIP	Entités qui possèdent des installations de production à vocation industrielle
CIP-003-6	Élimination de la formulation « détecter, évaluer et corriger » car elle est vague et sujette à de multiples interprétations	2017-10-01	2018-10-01	2019-04-01
CIP-003-6, E1, l'alinéa 1.1	Politique de cybersécurité documentées pour les *systèmes électroniques BES* à impact « moyen » et « élevé »	2017-10-01	2018-10-01	2019-04-01
CIP-003-6, E1 l'alinéa 1.2	Politique de cybersécurité documentées pour les *systèmes électroniques BES* à impact « faible »	2017-10-01	2019-10-01	2020-04-01
CIP-003-6, E2	Plan de cybersécurité documentées pour les *systèmes électroniques BES* à impact « faible »	2017-10-01	2019-10-01	2020-04-01
CIP-003-6, Annexe 1, Sect.1	Sensibilisation à la cybersécurité pour les *systèmes électroniques BES* à impact « faible »	2017-10-01	2019-10-01	2020-04-01
CIP-003-6, Annexe 1, Sect.2	Contrôle d'accès physique p*our les systèmes électroniques BES* à impact « faible »	2018-09-01	2019-10-01	2020-04-01
CIP-003-6, Annexe 1, Sect.3	Contrôle des accès électroniques *pour les systèmes électroniques BES* à impact « faible »	2018-09-01	2019-10-01	2020-04-01
CIP-003-6, Annexe 1, Sect.4	Réponse aux incidents de cybersécurité pour les *systèmes électroniques BES* à impact « faible »	2017-10-01	2019-10-01	2020-04-01

Les ajouts et modifications proposés au glossaire pour les termes suivants doivent être approuvés et en vigueur en même temps que la norme : [1]

- « *connectivité externe routable à impact faible* »;
- « *point d'accès électronique de système électronique BES à impact faible* »;
- « *actifs électroniques BES* ».

6. Contexte : Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

[1] Cette section sera retirée suivant l'adoption de la norme par la Régie.

Aucune disposition particulière

Annexe 1

Aucune disposition particulière

Annexe 2

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Justification

Aucune disposition particulière

Historique des versions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	xx-mois-xx	Nouvelle annexe.	Nouvelle

A. Introduction

1. Titre : Cybersécurité — Personnel et formation

2. Numéro : CIP-004-6

3. Objet : Réduire au minimum les risques de compromissions susceptibles d'entraîner un fonctionnement incorrect ou une instabilité du *système de production-transport d'électricité* (*BES*) et 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* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale ; et

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

4.1.2.2. Chaque *automatisme de réseau* (SPS) ou *plan de défense* (RAS) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

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

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

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

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

4.1.5. ***Coordonnateur des échanges*** **ou** ***responsable des échanges***

4.1.6. ***Coordonnateur de la fiabilité***

4.1.7. ***Exploitant de réseau de transport***

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

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

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

4.2.1.1. Chaque système de DSF ou de DST qui :

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

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

4.2.1.2. Chaque *automatisme de réseau* ou *plan de défense* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

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

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

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

4.2.3. Exemptions : Sont exemptés de la norme CIP-004-6 :

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 composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme au règlement CFR 10, section 73.54 ;

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

4.2.3.5. les entités responsables qui 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 :

Voir le plan de mise en œuvre de la norme CIP-004-6.

6. Contexte :

La norme CIP-004 fait partie d'une série de normes CIP sur la cybersécurité qui exigent la détermination et la catégorisation initiales des *systèmes électroniques BES*. Ces normes exigent aussi un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.

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

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité doit inclure tout ce qu'elle juge nécessaire dans ses processus documentés, en s'assurant de bien couvrir les exigences pertinentes.

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

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

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

Les mesures auxquelles renvoie l'énoncé initial de l'exigence correspondent simplement aux processus documentés eux-mêmes. La colonne « Mesures » présente des exemples de pièces justificatives attestant la documentation et la mise en œuvre des éléments pertinents dans les processus documentés ; ces exemples sont présentés à titre indicatif, et leur liste ne doit pas être considérée comme exhaustive.

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

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes 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 *BES*. Un examen des tolérances des 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. La SDT (équipe de rédaction) 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 au processus d'identification et de catégorisation de la norme CIP-002-5.1.

- ***Systèmes électroniques BES* à impact moyen –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », processus de désignation et de catégorisation de la norme CIP-002-5.1.

- ***Systèmes électroniques BES* à impact moyen à *connectivité externe routable*** – Désigne uniquement les *systèmes électroniques BES* à impact moyen à *connectivité externe routable*, à l'exclusion des *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'événements 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, couvrent tous les alinéas applicables du tableau E1 (CIP-004-6) – Programme de sensibilisation à la sécurité.
[Facteur de risque de non-conformité : faible] [Horizon : planification de l'exploitation]

M1. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-004-6) – 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-004-6) – Programme de sensibilisation à la sécurité			
Alinéa	**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 pièces justificatives : 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 des preuves de distribution, notamment : • communications ciblées (p. ex., courriels, notes de service, formation en ligne, etc.) ; • communications générales (p. ex., affiches, intranet, brochures, etc.) ; ou • rappels et soutien de la direction (p. ex., présentations, réunions, etc.).

E2. Chaque entité responsable doit mettre en œuvre un ou des programmes de formation sur la cybersécurité axée sur les rôles, les fonctions ou les responsabilités de chacun, qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-004-6) – Programme de formation sur la cybersécurité.
[Facteur de risque de non-conformité : faible] [Horizon : planification de l'exploitation]

M2. Les pièces justificatives doivent comprendre les programmes de formation qui couvrent tous les alinéas applicables du tableau E2 (CIP-004-6) – Programme de formation sur la cybersécurité ; d'autres pièces justificatives doivent attester la mise en œuvre des programmes.

Tableau E2 (CIP-004-6) – Programme de formation sur la cybersécurité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à connectivité externe routable et : 1. les *EACMS* associés ; et 2. les *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	Exemples non limitatifs de pièces justificatives : matériel de formation comme des présentations PowerPoint, des notes à l'intention des formateurs ou des étudiants, ou des documents de cours.

Tableau E2 (CIP-004-6) – Programme de formation sur la cybersécurité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
		associés à l'interconnectabilité et à l'interopérabilité des *systèmes électroniques BES* avec d'autres *actifs électroniques*, y compris des *actifs électroniques transitoires* et des *supports de stockage amovibles*.	
2.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Exiger que soit suivie au complet la formation énoncée à l'alinéa 2.1 avant que soit accordé 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 : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Exiger que la formation énoncée à l'alinéa 2.1 soit suivie au complet au moins une fois tous les 15 mois civils.	Exemple non limitatif de pièces justificatives : registres de formation individuels datés.

E3. Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés d'évaluation des risques liés au personnel en vue de l'octroi ou du maintien des accès électroniques autorisés ou des accès physiques autorisés sans accompagnement à des *systèmes électroniques BES* et qui, collectivement, couvrent tous les parties alinéas applicables du tableau E3 (CIP-004-6) – Programme d'évaluation des risques liés au personnel.
[Facteur de risque de 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, couvrent tous les alinéas applicables du tableau E3 (CIP-004-6) – Programme d'évaluation des risques liés au personnel ; d'autres pièces justificatives doivent attester la mise en œuvre du ou des programmes.

Tableau E3 (CIP-004-6) – Programme d'évaluation des risques liés au personnel			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les PACS associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Processus de confirmation de l'identité.	Exemple non limitatif de pièces justificatives : documents attestant le processus suivi par l'entité responsable pour confirmer l'identité.

Tableau E3 (CIP-004-6) – Programme d'évaluation des risques liés au personnel			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *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 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 pièces justificatives : documents attestant le processus suivi par l'entité responsable pour vérifier les antécédents criminels sur les sept dernières années.

Tableau E3 (CIP-004-6) – Programme d'évaluation des risques liés au personnel			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.3	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *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 pièces justificatives : documents attestant le processus de l'entité responsable pour évaluer les résultats des vérifications des antécédents judiciaires.
3.4	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Critères ou processus pour vérifier que les évaluations des risques liés au personnel dont les contractuels et les fournisseurs de services doivent faire l'objet sont menées conformément aux alinéas 3.1 à 3.3.	Exemples non limitatifs de pièces justificatives : documents attestant les critères ou le processus de l'entité responsable pour vérifier les évaluations des risques liés au personnel pour les contractuels et les fournisseurs de services.
3.5	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *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 alinéas 3.1 à 3.4 au cours des sept dernières années.	Exemples non limitatifs de pièces justificatives : documents attestant 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 un ou plusieurs programmes documentés de gestion des accès qui, collectivement, couvrent tous les alinéas applicables du tableau E4 (CIP-004-6) – Programme de gestion des accès.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation et exploitation le même jour]

M4. Les pièces justificatives doivent comprendre les processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E4 (CIP-004-6) – Programme de gestion des accès ; d'autres pièces justificatives doivent attester la mise en œuvre des mesures du programme de gestion des accès selon la colonne Mesures du tableau.

Tableau E4 (CIP-004-6) – Programme de gestion des accès

Alinéa	Systèmes visés	Exigences	Mesures
4.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Processus d'autorisation selon le besoin déterminé par l'entité responsable, sauf dans des *circonstances CIP exceptionnelles* : 4.1.1. de l'accès électronique ; 4.1.2. de l'accès physique sans accompagnement dans un *périmètre de sécurité physique* ; et 4.1.3. de 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 attestant 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-004-6) – Programme de gestion des accès			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
4.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *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 une comparaison entre la liste automatisée des personnes pour lesquelles on a autorisé l'accès (base de données des activités de fourniture) et la liste automatisée des personnes auxquelles on a fourni un accès (liste des comptes utilisateurs) ; ou • documents datés attestant une comparaison entre la liste des personnes pour lesquelles on a autorisé l'accès (formulaires d'autorisation) et la liste des personnes auxquelles on a fourni un accès (formulaires de fourniture d'accès ou liste des comptes partagés).

Tableau E4 (CIP-004-6) – Programme de gestion des accès			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
4.3	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Dans le cas des accès électroniques, 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 attestant qu'on a vérifié que les droits d'accès du groupe sont autorisés et qu'ils correspondent aux fonctions de toute personne à qui ils sont attribués.

Tableau E4 (CIP-004-6) – Programme de gestion des accès			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
4.4	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	Vérifier, au moins une fois tous les 15 mois civils, que les accès aux emplacements de stockage (physiques ou électroniques) désignés pour l'information de *système électronique BES* sont correctement attribués et qu'ils correspondent 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 attestant qu'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 un ou plusieurs programmes documentés de révocation d'accès qui, collectivement, couvrent tous les alinéas applicables du tableau E5 (CIP-004-6) – Révocation d'accès.
[Facteur de risque de non-conformité : moyen] [Horizon : exploitation le même jour et planification de l'exploitation]

M5. Les pièces justificatives doivent comprendre chacun des programmes documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E5 (CIP-004-6) – Révocation d'accès ; d'autres pièces justificatives doivent attester la mise en œuvre selon la colonne Mesures du tableau.

Tableau E5 (CIP-004-6) – Révocation d'accès			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
5.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PACS* associés.	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 d'accès associé au départ ; et 2. journaux ou autres preuves attestant que la personne ne dispose plus d'un accès.

Tableau E5 (CIP-004-6) – Révocation d'accès			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
5.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *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, déterminée par l'entité responsable, où la personne n'a plus besoin de ces accès.	Exemples non limitatifs de pièces justificatives : 1. formulaire d'activité ou d'approbation daté attestant l'examen des accès logique et physique ; et 2. journaux ou autres preuves attestant que la personne ne dispose plus des accès que l'entité responsable détermine comme n'étant plus nécessaires.
5.3	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *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 au plus tard du jour civil suivant le départ.

Tableau E5 (CIP-004-6) – Révocation d'accès			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
5.4	*Systèmes électroniques BES* à impact élevé et : • les *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 un logiciel d'application 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 : • les *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, déterminée par l'entité responsable, où la personne n'a plus besoin de cet accès. Si l'entité responsable détermine et documente qu'un délai plus long est nécessaire 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 changé dans les 30 jours civils suivant le départ ; • formulaire d'activité ou d'approbation attestant que le mot de passe a été changé 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 changé dans les 10 jours civils suivant la fin de ces circonstances.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Selon la définition des règles de procédure de la NERC, le terme « responsable des mesures pour assurer la conformités » (CEA) désigne la NERC ou l'entité régionale dans leurs rôles respectifs de surveillance de la conformité aux normes de fiabilité de la NERC.

1.2. Conservation des pièces justificatives

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

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

- Chaque entité 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 de conformité

Déclarations de non-conformité

Plaintes

1.4. Autres informations sur la conformité

Aucune

2. Tableau des éléments de conformité

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			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 moins de 10 jours civils après le début d'un trimestre civil 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 civil subséquent. (1.1)	L'entité responsable n'a pas rappelé les pratiques de cybersécurité au cours d'un trimestre civil, mais l'a fait au cours du trimestre civil suivant, plus de 30 jours après le début de ce trimestre. (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 pendant au moins deux trimestres civils consécutifs. (1.1)
E2	**Planification de l'exploitation**	**Faible**	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais en omettant un des thèmes de formation des alinéas 2.1.1 à 2.1.9 de	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais en omettant deux des thèmes de formation des alinéas 2.1.1 à 2.1.9 de	L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais en omettant trois des thèmes de formation des alinéas 2.1.1 à 2.1.9 de	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

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			l'exigence. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former une personne (sauf en cas de *circonstances CIP exceptionnelles*) avant de lui accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former une personne ayant un accès électronique autorisé ou un accès physique	l'exigence. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former deux personnes (sauf en cas de *circonstances CIP exceptionnelles*) avant de leur accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former deux personnes ayant un accès électronique autorisé ou un accès physique	l'exigence. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former trois personnes (sauf en cas de *circonstances CIP exceptionnelles*) avant de leur accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former trois personnes ayant un accès électronique autorisé ou un accès physique	chacun. (E2) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais en omettant quatre ou plus des thèmes de formation des alinéas 2.1.1 à 2.1.9 de l'exigence. (2.1) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former quatre personnes ou plus (sauf en cas de *circonstances CIP exceptionnelles*) avant de leur accorder un accès électronique autorisé ou un accès physique autorisé sans

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			autorisé sans accompagnement dans les 15 mois civils suivant la fin de la dernière formation qu'elle a suivie. (2.3)	autorisé sans accompagnement dans les 15 mois civils suivant la fin de la dernière formation qu'elle a suivie. (2.3)	autorisé sans accompagnement dans les 15 mois civils suivant la fin de la dernière formation qu'elle a suivie. (2.3)	accompagnement. (2.2) OU L'entité responsable a mis en œuvre un programme de formation sur la cybersécurité, mais a omis de former quatre personnes ou plus ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans les 15 mois civils suivant la date de fin de la dernière formation qu'elle a suivie. (2.3)
E3	**Planification de l'exploitation**	**Moyen**	L'entité responsable a un programme d'évaluation des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services), mais a omis d'effectuer la	L'entité responsable a un programme d'évaluation des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services), mais a omis d'effectuer la	L'entité responsable a un programme d'évaluation des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services), mais a omis d'effectuer la	L'entité responsable n'a pas inclus tous les éléments des alinéas 3.1 à 3.4 dans les programmes documentés d'évaluation des risques liés au personnel (PRA) pour les personnes, y

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			PRA comme condition pour accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement à une personne. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de service) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis de confirmer l'identité d'une personne. (3.1 et 3.4) OU	PRA comme condition pour accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement à deux personnes. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis de confirmer l'identité de deux personnes. (3.1 et 3.4) OU	PRA comme condition pour accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement à trois personnes. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis de confirmer l'identité de trois personnes. (3.1 et 3.4) OU	compris les contractuels et les fournisseurs de services, en vue de l'obtention et du maintien 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 (y compris les contractuels et les fournisseurs de services), mais a omis d'effectuer la PRA comme condition pour accorder un accès électronique autorisé ou un accès physique autorisé sans accompagnement à quatre personnes ou

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis les vérifications exigées en 3.2.1 et 3.2.2 pour une personne. (3.2 et 3.4) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services)	L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis les vérifications exigées en 3.2.1 et 3.2.2 pour deux personnes. (3.2 et 3.4) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services)	L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis les vérifications exigées en 3.2.1 et 3.2.2 pour trois personnes. (3.2 et 3.4) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services)	plus. (E3) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis de confirmer l'identité de quatre personnes ou plus. (3.1 et 3.4) OU L'entité responsable a un processus de vérification des antécédents judiciaires sur les sept années précédentes pour

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis d'évaluer la vérification des antécédents judiciaires pour l'autorisation d'accès d'une personne. (3.3 et 3.4) OU L'entité responsable a omis l'évaluation des risques liés au personnel (PRA) pour une personne ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans un délai de 7 années civiles suivant la réalisation de la PRA	ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis d'évaluer la vérification des antécédents judiciaires pour l'autorisation d'accès de deux personnes. (3.3 et 3.4) OU L'entité responsable a omis l'évaluation des risques liés au personnel (PRA) pour deux personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans un délai de 7 années civiles suivant la réalisation de la PRA	ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis d'évaluer la vérification des antécédents judiciaires pour l'autorisation d'accès de trois personnes. (3.3 et 3.4) OU L'entité responsable a omis l'évaluation des risques liés au personnel (PRA) pour trois personnes ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans un délai de 7 années civiles suivant la réalisation de la PRA	les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a omis les vérifications exigées en 3.2.1 et 3.2.2 pour quatre personnes ou plus. (3.2 et 3.4) OU L'entité responsable a effectué des évaluations des risques liés au personnel (PRA) pour les personnes (y compris les contractuels et les fournisseurs de services) ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement, mais a

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			précédente. (3.5)	précédente. (3.5)	précédente. (3.5)	omis d'évaluer la vérification des antécédents judiciaires pour l'autorisation d'accès de quatre personnes ou plus. (3.3 et 3.4) OU L'entité responsable a omis l'évaluation des risques liés au personnel (PRA) pour quatre personnes ou plus ayant un accès électronique autorisé ou un accès physique autorisé sans accompagnement dans un délai de 7 années civiles suivant la réalisation de la PRA précédente. (3.5)
E4	**Planification de l'exploitation**	**Moyen**	L'entité responsable n'a pas vérifié que les personnes ayant un accès	L'entité responsable n'a pas vérifié que les personnes ayant un accès	L'entité responsable n'a pas vérifié que les personnes ayant un accès	L'entité responsable n'a pas mis en œuvre un programme documenté

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
	et exploitation du jour même		électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des registres d'accès autorisé pendant un trimestre civil, mais l'a fait moins de 10 jours civils après le début d'un trimestre civil subséquent. (4.2) OU L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente 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,	électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des registres d'accès autorisé pendant un trimestre civil, mais l'a fait entre 10 et 20 jours civils après le début d'un trimestre civil subséquent. (4.2) OU L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente 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,	électronique ou un accès physique sans accompagnement en vigueur sont consignées dans des registres d'accès autorisé pendant un trimestre civil, mais l'a fait entre 20 et 30 jours civils après le début d'un trimestre civil subséquent. (4.2) OU L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente 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, ,	pour la gestion des accès. (E4) OU L'entité responsable a mis en œuvre un ou plusieurs programmes documentés pour la gestion des accès comprenant un processus pour autoriser l'accès électronique, l'accès physique sans accompagnement ou l'accès aux emplacements de stockage désignés pour l'information de *système électronique BES*. (4.1) OU L'entité responsable n'a pas vérifié que les personnes ayant un accès électronique ou un accès physique sans

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			mais a constaté que, pour 5 % ou moins de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires. (4.3) OU L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les accès aux emplacements de stockage désignés pour l'information de *système électronique BES* sont corrects et nécessaires, mais a constaté que pour 5 % ou moins de ses emplacements de stockage de l'information de *système électronique BES*, les droits d'accès étaient incorrects ou non	mais a constaté que pour plus de 5 % mais au plus 10 % de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires. (4.3) OU L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les accès aux emplacements de stockage désignés pour l'information de *système électronique BES* sont corrects et nécessaires, mais a constaté que pour plus de 5 % mais au plus 10 % de ses emplacements de stockage de l'information de *système électronique*	mais a constaté que pour plus de 10 % mais au plus 15 % de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non nécessaires. (4.3) OU L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les accès aux emplacements de stockage désignés pour l'information de *système électronique BES* sont corrects et nécessaires, mais a constaté que pour plus de 10 % mais au plus 15 % de ses emplacements de stockage de l'information de *système électronique*	accompagnement en vigueur sont consignées dans des registres d'accès autorisé pendant deux trimestres civils consécutifs ou plus. (4.2) OU L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente 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, , mais a constaté que pour plus de 15 % de ses *systèmes électroniques BES*, les droits d'accès étaient incorrects ou non

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			nécessaires. (4.4)	*BES*, les droits d'accès étaient incorrects ou non nécessaires. (4.4)	*BES*, les droits d'accès étaient incorrects ou non nécessaires. (4.4)	nécessaires. (4.3) OU L'entité responsable a mis en œuvre des processus pour vérifier dans les 15 mois civils suivant la vérification précédente que les accès aux emplacements de stockage désignés pour l'information de *système électronique BES* sont corrects et nécessaires, mais a constaté que pour plus de 15 % de ses emplacements de stockage de l'information de *système électronique BES*, les droits d'accès étaient incorrects ou non nécessaires. (4.4)
E5	**Exploitation du jour même et**	**Moyen**	L'entité responsable a mis en œuvre un ou plusieurs processus pour	L'entité responsable a mis en œuvre un ou plusieurs processus pour	L'entité responsable a mis en œuvre un ou plusieurs processus pour	L'entité responsable n'a mis en œuvre aucun programme documenté

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
	planification de l'exploitation		révoquer l'accès des personnes aux emplacements de stockage désignés pour l'information de *système électronique BES*, mais dans le cas d'une personne, la révocation n'a pas été faite avant la fin du jour civil suivant la date et l'heure de prise d'effet du départ. (5.3) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès des personnes à leurs comptes utilisateurs lors de leur départ, mais la révocation n'a pas été faite dans les 30 jours civils suivant la date du départ pour une	retirer la capacité d'accès physique sans accompagnement et d'*accès distant interactif* lors d'un départ ou pour mener à bien ce retrait dans les 24 heures suivant le départ, mais a omis de déclencher ce retrait pour une personne. (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 des 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 individuels	retirer la capacité d'accès physique sans accompagnement et d'*accès distant interactif* lors d'un départ ou pour mener à bien ce retrait dans les 24 heures suivant le départ, mais a omis de déclencher ce retrait pour deux personnes. (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 des 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 individuels	de révocation d'accès pour les accès électroniques, les accès physiques sans accompagnement ou pour les emplacements de stockage des 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 mener à bien ce retrait dans les 24 heures suivant le départ, mais a omis de déclencher ce retrait pour trois personnes ou plus. (5.1)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			personne ou plus. (5.4) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour changer les mots de passe des comptes partagés connus des utilisateurs lors de leur départ, de leur réaffectation ou de leur mutation, mais ce changement n'a pas été fait dans les 30 jours civils suivant la date du départ, de la réaffectation ou de la mutation pour une personne ou plus. (5.5) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer et	et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée. (5.2) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès des personnes aux emplacements de stockage désignés pour l'information de *système électronique BES*, mais dans le cas de deux personnes, la révocation n'a pas été faite avant la fin du jour civil suivant la date et l'heure de prise d'effet du départ. (5.3)	et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée. (5.2) OU L'entité responsable a mis en œuvre un ou plusieurs processus pour révoquer l'accès des personnes aux emplacements de stockage désignés pour l'information de *système électronique BES*, mais dans le cas de trois personnes ou plus, la révocation n'a pas été faite avant la fin du jour civil suivant la date et l'heure de prise d'effet du départ. (5.3)	OU L'entité responsable a mis en œuvre un ou plusieurs processus pour déterminer qu'une personne n'a plus besoin de conserver des 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 individuels et les accès physiques autorisés sans accompagnement avant la fin du jour civil suivant la date prédéterminée. (5.2)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-004-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			documenter les circonstances opérationnelles atténuantes suivant un départ, une réaffectation ou une mutation, mais n'a pas changé un ou plusieurs mots de passe de comptes partagés connus d'un utilisateur dans les 10 jours civils suivant la fin de circonstances opérationnelles atténuantes. (5.5)			

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

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. Dans l'exigence E1.6, suppression de la phrase concernant le retrait du service d'un composant ou d'un système aux fins d'essais, en réponse 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.	Modification en coordination avec les autres normes CIP et révision du format selon le modèle RBS.
5	22 novembre 2013	Ordonnance de la FERC approuvant la norme CIP-004-5.	
5.1	30 septembre 2013	Modification de deux VSL à l'exigence E4.	Errata
6	13 novembre 2014	Adoption par le Conseil d'administration de la NERC.	Mise en œuvre de deux prescriptions de l'ordonnance 791 de la FERC concernant l'obligation de « détecter, évaluer et corriger » ainsi que les réseaux de communication.
6	12 février 2015	Adoption par le conseil d'administration de la NERC.	Remplace la version adoptée par le conseil d'administration le 13 novembre 2014. La version à jour met en œuvre des prescriptions en instance de l'ordonnance 791 relativement aux actifs temporaires et aux *systèmes électroniques BES* à impact faible.
6	21 janvier 2016	Ordonnance de la FERC émise approuvant CIP-003-6. Dossier no. RM15-14-000	

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) présente 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, les normes CIP sur la cybersécurité de la NERC s'y appliquent. Il est à noter qu'en ce qui concerne les *distributeurs*, la section 4.1 limite l'applicabilité 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 qui, selon la section 4.1, est visée par les exigences de la norme. Comme il est indiqué à la section d'exemption 4.2.3.5, la présente norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou moyen selon la catégorisation de la norme CIP-002-5.1. 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* » dans le glossaire de la NERC indique déjà qu'il s'agit d'*éléments* du *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 aide à clarifier quels sont les *installations*, systèmes et équipements visés par les normes.

Exigence E1

Le programme de sensibilisation à la sécurité se veut un programme d'information, et non de formation. 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'a pas à fournir des documents qui attestent que chaque personne a reçu ou compris l'information, mais elle doit conserver en tout temps le matériel utilisé pour le programme : affiches, notes de service, présentations, etc.

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

- communications ciblées (courriels, notes de service, formation en ligne, etc.) ;
- communications générales (affiches, intranet, brochures, etc.) ;
- rappels et soutien de la direction (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* ; elle doit comporter 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 comprendre plusieurs modules et modes de prestation, mais un seul

programme de formation pour toutes les personnes à former est aussi acceptable. L'entité responsable peut, à sa guise, axer la formation sur les fonctions, les rôles ou les responsabilités.

Le paragraphe 434 de l'ordonnance 706 de la FERC intègre à la formation un nouvel élément qui concerne les équipements et les logiciels de réseau ainsi que d'autres éléments d'interconnectabilité électronique nécessaires à l'exploitation et au contrôle des *systèmes électroniques BES*. La formation doit également porter sur les risques associés au branchement et à l'utilisation d'*actifs électroniques transitoires* et de *supports de stockage amovibles* dans des *systèmes électroniques BES* ou à l'intérieur d'un *périmètre de sécurité électronique*. Comme l'indique le paragraphe 135 de l'ordonnance 791 de la FERC, des *actifs électroniques transitoires* et des *supports de stockage amovibles* ont été la cause de cas concrets de contamination de systèmes de commande industrielle de production d'électricité par des maliciels ; la formation à leur utilisation est donc essentielle pour la protection des *systèmes électroniques BES*. Il ne s'agit pas de donner une formation technique aux personnes responsables des équipements et des logiciels de réseau, mais plutôt d'informer les utilisateurs de systèmes sur les 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*, ainsi que les contractuels et les fournisseurs de services, suivent une formation sur la cybersécurité avant d'obtenir 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*, ainsi que les contractuels et les fournisseurs de services, avant que soit accordé cet accès, exception faite des circonstances exceptionnelles qui ont une incidence sur la fiabilité du *BES* ou la capacité d'intervention d'urgence, qui sont précisées au programme et approuvées par le cadre supérieur désigné ou son délégataire. Le contrôle de l'identité doit être réalisé en respectant les lois fédérales, d'État, provinciales et locales ainsi que 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'État, 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 être faite. Il peut s'agir, par exemple, de personnes de moins de 25 ans dont les antécédents à titre de jeune

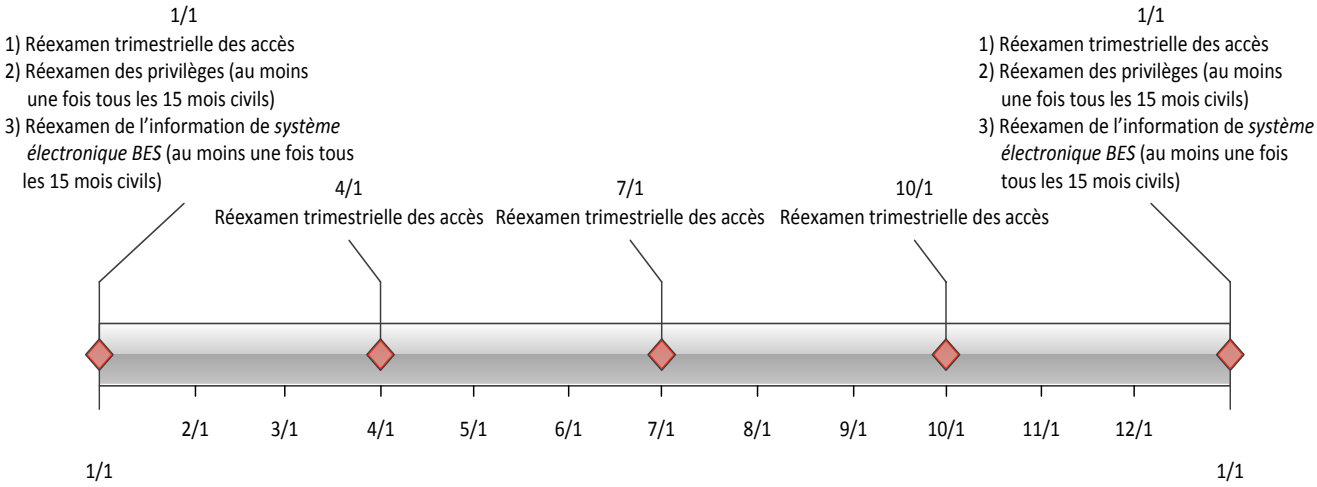
contrevenant sont protégés en vertu de la loi, de personnes qui ont résidé à des endroits où il est impossible d'obtenir des vérifications d'antécédents judiciaires ou de personnes dont l'emploi est régi par une convention collective qui l'interdit. Dans de tels cas, l'entité responsable doit tenir compte 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 années 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 opérationnels 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 réexamens trimestriels ainsi que des réexamens au moins une fois tous les 15 mois civils. Les réexamens 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.

Le réexamen 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 ce réexamen en mettant en place un accès basé sur les rôles. Cette méthode consiste à définir les rôles au sein du système (répartiteur, technicien, récepteur de rapports, administrateur, etc.), puis à grouper les droits d'accès selon ces différents rôles, et enfin 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 réexamen des droits d'accès des comptes individuels. Un calendrier type de tous les réexamens énoncés à l'exigence E4 est illustré ci-dessous.



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

Si les résultats des réexamens de comptes trimestriels ou des réexamens 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, la 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 du départ d'un employé (cessation d'emploi) prévoit des procédures démontrant que la révocation de l'accès se produit en même temps que le départ. On y admet que le moment du départ peut varier selon les circonstances. Quelques scénarios courants et processus possibles selon le moment du départ 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.

Scénario	Processus possible
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, si le dernier jour de travail est plusieurs semaines avant la date du départ	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 » d'une personne un processus dont le résultat final est l'impossibilité pour elle d'obtenir un accès électronique aux *systèmes électroniques BES* en utilisant les identifiants de connexion qui lui ont été attribués ou qu'elle connaît. 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 prescrite 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 locaux pour l'accès à des *actifs électroniques BES* (c.-à-d. des comptes spécifiques à ces *actifs électroniques*), 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 consister à dresser une simple liste de toutes les autorisations associées à la personne et à travailler en collaboration avec les gestionnaires respectifs pour déterminer de quels accès la personne aura encore 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 de réexamen de ces droits d'accès ou les inclure dans le réexamen trimestriel des comptes ou le réexamen 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 changeraient constamment en raison du roulement du personnel.

L'exigence 5.5 précise que les mots de passe de comptes partagés doivent être changés dans les 30 jours civils suivant le départ 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 celles-ci. Les documents consignant ces activités doivent être conservés afin de démontrer que l'entité responsable a suivi le plan qu'elle a établi.

Justification

Pendant l'élaboration de cette norme, des zones de texte ont été incorporées à celle-ci pour exposer la justification de ses diverses parties. Après l'approbation par le Conseil d'administration, le contenu de ces zones de texte a été transféré ci-après.

Justification de l'exigence E1 :

Faire en sorte qu'une entité responsable dont des employés ont un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *actifs électroniques BES* prenne des mesures pour que les employés ayant de tels accès soient toujours au fait de ses pratiques de sécurité.

Justification de l'exigence 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 appropriée avant de se voir accorder des accès.

Justification de l'exigence 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.

Justification de l'exigence 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 » désigne l'octroi d'une permission par une ou des personnes habilitées par l'entité responsable à autoriser cet octroi ; ce pouvoir fait partie des délégations indiquées à la norme CIP-003-6. La « fourniture » désigne les mesures prises pour fournir un accès à une personne.

L'accès est constitué des accès physique, logique et distant à des *actifs électroniques* qui font partie du *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 (système de contrôle des accès physiques, système d'accès distant, services d'annuaire, etc.).

Les *circonstances CIP exceptionnelles* doivent être définies dans une politique de l'entité responsable conformément à la norme CIP-003-6 ; elles constituent une exception à l'exigence d'autorisation d'accès aux *systèmes électroniques BES* et à l'information de *système électronique BES*.

Les réexamens trimestriels prescrits à l'alinéa 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, cette liste 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 réexamens 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, la 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.

Justification de l'exigence 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. Cela est particulièrement important dans les situations où des personnes sont licenciées ou réaffectées contre leur gré, 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, la SDT a choisi de ne pas préciser de délais en heures dans l'exigence (p. ex. « révoquer l'accès dans l'heure suivant le départ »). Le moment du départ d'une personne 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 est plus expéditive si elle survient en même temps que les premières étapes de ce processus.

L'accès est constitué des accès physique, logique et distant à des *actifs électroniques* qui font partie du *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 (système de contrôle des accès physiques, système d'accès distant, services d'annuaire, etc.).

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-004-6

3. Objet : Aucune disposition particulière

4. Applicabilité :

4.1. Entités fonctionnelles

Aucune disposition particulière

4.2. Installations

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

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

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

5. Date d'entrée en vigueur au Québec :

5.1. Adoption de la norme par la Régie de l'énergie : xx mois 20xx

5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 20xx

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

Norme	Révision CIPv6	Date d'entrée en vigueur proposée au Québec		
		Entités visées par la version 1 des normes CIP adoptées par la Régie	Entités ne possédant pas d'installations de production à vocation industrielle et non visées par la version 1 des normes CIP	Entités qui possèdent des installations de production à vocation industrielle
CIP-004-6	Ajout des *actifs électronique transitoires* (TCA) et les *supports d'information de stockage* (RM) à la formation	**2017-10-01**	**2018-10-01**	**2019-04-01**

Les ajouts et modifications proposés au glossaire pour les termes suivants doivent être approuvés et en vigueur en même temps que la norme : [1]

- « *actif électronique transitoire* »
- « *support d'information de stockage* »
- « *actifs électroniques BES* »

6. Contexte : Aucune disposition particulière

[1] Cette section sera retirée suivant l'adoption de la norme par la Régie.

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Justification

Aucune disposition particulière

Historique des versions

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

A. Introduction

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

2. Numéro : CIP-006-6

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 *système de production-transport d'électricité* (*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* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale ; et

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

4.1.2.2 Chaque *automatisme de réseau (SPS)* ou *plan de défense (RAS)* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

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

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

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

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

4.1.5 ***Coordonnateur des échanges*** **ou** ***responsable des échanges***

4.1.6 ***Coordonnateur de la fiabilité***

4.1.7 ***Exploitant de réseau de transport***

4.1.8 ***Propriétaire d'installation de transport***

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

4.2.1 ***Distributeur*** **:** Un ou plusieurs des *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* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale ; et

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

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les *distributeurs* :

Toutes les *installations* du *BES*.

4.2.3 Exemptions : Sont exemptés de la norme CIP-006-6 :

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 composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme au règlement CFR 10, section 73.54 ;

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

4.2.3.5 les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* classés dans les catégories « impact élevé » ou « impact moyen » selon le processus de désignation et de catégorisation de la norme CIP-002-5.1.

5. Dates d'entrée en vigueur

Voir le plan de mise en œuvre de la norme CIP-006-6

6. Contexte

La norme CIP-006 fait partie d'une série de normes CIP sur la cybersécurité qui exigent la détermination et la catégorisation initiales des *systèmes électroniques BES*. Ces normes exigent aussi un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.

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

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité doit inclure tout ce qu'elle juge nécessaire dans ses processus documentés, en s'assurant de bien couvrir les exigences pertinentes.

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

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont des exemples qui figurent dans les normes. La mise en œuvre

complète des normes de fiabilité CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

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

Les mesures auxquelles renvoie l'énoncé initial de l'exigence correspondent simplement aux processus documentés eux-mêmes. La colonne « Mesures » présente des exemples de pièces justificatives attestant la documentation et la mise en œuvre des éléments pertinents dans les processus documentés ; ces exemples sont présentés à titre indicatif, et leur liste ne doit pas être considérée comme exhaustive.

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

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes 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 *BES*. Un examen des tolérances des 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. La SDT (équipe de rédaction) CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- ***Systèmes électroniques BES* à impact élevé –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.
- ***Systèmes électroniques BES* à impact moyen –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.

- ***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*, à l'exclusion des *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'événements 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 un ou plusieurs plans de sécurité physique documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-006-6) – Plan de sécurité physique. *[Facteur de risque de non-conformité : moyen] [Horizon : planification à long terme et exploitation le même jour]*

M1. Les pièces justificatives doivent comprendre chacun des plans de sécurité physique documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-006-6) – Plan de sécurité physique ; d'autres pièces justificatives doivent attester la mise en œuvre selon la colonne Mesures du tableau.

Tableau E1 (CIP-006-6) – Plan de sécurité physique			
Alinéa	**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 pièces justificatives : documentation attestant que des mesures opérationnelles ou administratives sont en place.

Tableau E1 (CIP-006-6) – Plan de sécurité physique			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.2	*Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *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 pièces justificatives : 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, comme des listes de personnes autorisées et les registres d'accès correspondants.
1.3	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PCA* associés.	Si c'est 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 pièces justificatives : 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, comme des listes de personnes autorisées et les registres d'accès correspondants.

Tableau E1 (CIP-006-6) – Plan de sécurité physique			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.4	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PCA* associés.	Surveiller les accès non autorisés à un point d'accès physique d'un *périmètre de sécurité physique*.	Exemple non limitatif de pièces justificatives : documentation des mécanismes de surveillance des accès non autorisés à un point d'accès physique d'un *périmètre de sécurité physique*.

Tableau E1 (CIP-006-6) – Plan de sécurité physique			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.5	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; et 2. les *PCA* associés.	Déclencher une alarme ou une alerte en réponse à la détection d'un accès non autorisé à un point d'accès physique d'un *périmètre de sécurité physique*, à l'intention du 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 pièces justificatives : des énoncés dans le plan de sécurité physique décrivant le processus de déclenchement d'une alarme ou d'une alerte en réponse à un accès non autorisé à un 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 déclenchée et communiquée conformément au plan d'intervention en cas d'*incident de cybersécurité* lié au *BES*, comme 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 déclenchée 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* afin de détecter les accès physiques non autorisés à un *système de contrôle des accès physiques*.	Exemple non limitatif de pièces justificatives : documentation des mécanismes de détection des accès physiques non autorisés à un PACS.

Tableau E1 (CIP-006-6) – Plan de sécurité physique			
Alinéa	**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*.	Déclencher une alarme ou une alerte en réponse à la détection d'un accès physique non autorisé à un *système de contrôle des accès physiques,* à l'intention du 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 pièces justificatives : des énoncés dans le plan de sécurité physique précisant qu'une alarme ou une alerte est déclenchée 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 déclenchée et communiquée conformément au plan d'intervention en cas d'*incident de cybersécurité* lié au *BES*, comme 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 déclenchée et communiquée.

Tableau E1 (CIP-006-6) – Plan de sécurité physique			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.8	*Systèmes électroniques BES* à impact élevé et : 1. les EACMS associés ; et 2. les PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les EACMS associés ; et 2. les 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 et de connaître la date et l'heure de l'accès.	Exemple non limitatif de pièces justificatives : 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 attestant que cette consignation a été mise en œuvre, comme des registres d'accès physique aux *périmètres de sécurité physique* indiquant 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 : 1. les EACMS associés ; et 2. les PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les EACMS associés ; et 2. les 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 pièces justificatives : documents datés, comme des registres des accès physiques aux *périmètres de sécurité physique* indiquant la date et l'heure de l'accès au *périmètre de sécurité physique*.
1.10	Systèmes électroniques BES à impact élevé et : • les PCA associés. *Systèmes électroniques BES* à impact moyen aux *centres de*	Restreindre l'accès physique aux câbles et autres composants de communication non programmables qui servent à interrelier des *actifs électroniques* visés situés dans un	Exemples non limitatifs de pièces justificatives : documents attestant la mise en œuvre par l'entité responsable des restrictions d'accès physique (câblage et composants sous

Tableau E1 (CIP-006-6) – Plan de sécurité physique			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
	contrôle et : • les PCA associés.	même *périmètre de sécurité électronique*, si ces câbles et composants se trouvent à l'extérieur d'un *périmètre de sécurité physique*. En l'absence de restriction d'accès physique à de tels câblages et composants, l'entité responsable doit documenter et mettre en œuvre une ou plusieurs des mesures suivantes : • cryptage des données qui transitent par ces câbles et composants ; ou • surveillance de l'état de la liaison de communication constituée par ces câbles et composants, avec déclenchement d'une alarme ou d'une alerte sur détection d'une défaillance de communication à l'intention du personnel désigné dans le plan d'intervention en cas d'*incident de cybersécurité* lié au *BES*, dans les 15 minutes suivant la détection ; ou • protection logique d'une efficacité équivalente.	conduit ou enfermés dans des chemins de câbles, etc.), du cryptage des données, de la surveillance ou d'une protection logique d'une efficacité équivalente.

E2. Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes de contrôle des visiteurs documentés qui, collectivement, couvrent tous les alinéas du tableau E2 (CIP-006-6) – Programme de contrôle des visiteurs. *[Facteur de risque de non-conformité : moyen] [Horizon : exploitation le même jour]*

M2. Les pièces justificatives doivent comprendre un ou plusieurs programmes de contrôle des visiteurs documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-006-6) – Programme de contrôle des visiteurs ; d'autres pièces justificatives doivent attester la mise en œuvre selon la colonne Mesures du tableau.

Tableau E2 (CIP-006-6) – Programme de contrôle des visiteurs			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et : 1. les EACMS associés ; et 2. les PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les EACMS associés ; et 2. les 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 pièces justificatives : 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 œuvre, comme des registres de visiteurs.
2.2	*Systèmes électroniques BES* à impact élevé et : 1. les EACMS associés ; et 2. les PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les EACMS associés ; et 2. les PCA associés.	Exiger la consignation manuelle ou automatique de l'entrée de tout visiteur dans un *périmètre de sécurité physique* ainsi que de sa sortie, notamment la date et l'heure de la première entrée et de la dernière sortie, le nom du visiteur et le nom de son répondant, sauf dans des *circonstances CIP exceptionnelles*.	Exemple non limitatif de pièces justificatives : 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 attestant que cette mesure a été mise en œuvre, comme des registres de visiteurs datés renfermant les données pertinentes.

Tableau E2 (CIP-006-6) – Programme de contrôle des visiteurs			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.3	*Systèmes électroniques BES* à impact élevé et : 1. les EACMS associés ; et 2. les PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les EACMS associés ; et 2. les PCA associés.	Conserver les registres des visiteurs durant au moins 90 jours civils.	Exemple non limitatif de pièces justificatives : 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, couvrent tous les alinéas applicables du tableau E3 (CIP-006-6) – Programme de maintenance et d'essais.
[Facteur de risque de 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, couvrent tous les alinéas applicables du tableau E3 (CIP-006-6) – Programme de maintenance et d'essais ; d'autres pièces justificatives doivent attester la mise en œuvre selon la colonne Mesures du tableau.

Tableau E3 (CIP-006-6) – 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*. Équipements 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*.	Les opérations de maintenance et d'essai de chaque *système de contrôle des accès physiques* et de chaque équipement ou dispositif installé localement au *périmètre de sécurité physique* doivent être effectuées au moins une fois tous les 24 mois civils afin d'assurer leur bon fonctionnement.	Exemple non limitatif de pièces justificatives : 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 des équipements ou dispositifs installés localement à un *périmètre de sécurité physique* visé, et des pièces justificatives additionnelles attestant que les essais ont été effectués, comme des registres de maintenance datés, ou tout autre document attestant que la maintenance et les essais ont été effectués pour chaque système et dispositif visé au moins une fois tous les 24 mois civils.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Selon la définition des règles de procédure de la NERC, le terme « *responsable des mesures* » (CEA) désigne la NERC ou l'entité régionale dans leurs rôles respectifs de surveillance de la conformité aux normes de fiabilité de la NERC.

1.2. Conservation des pièces justificatives

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

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

- Chaque entité 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 de conformité

Déclarations de non-conformité

Plaintes

1.4. Autres informations sur la conformité

Aucune.

2. Tableau des éléments de conformité

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1	**Planification à long terme** **Exploitation le même jour**	**Moyen**				L'entité responsable n'a documenté ou mis en œuvre aucun plan de sécurité physique. (E1) OU 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 mécanismes de contrôle des accès physiques, mais il n'y a pas au moins un mécanisme de contrôle pour restreindre l'accès aux systèmes

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						applicables. (1.2) OU L'entité responsable a documenté et mis en œuvre des mécanismes de contrôle des accès physiques, mais il n'y a pas au moins deux mécanismes de contrôle différents pour restreindre l'accès aux systèmes applicables. (1.3) OU L'entité responsable n'a pas de processus pour surveiller les accès non autorisés à un point d'accès physique d'un *périmètre de sécurité physique*. (1.4) OU L'entité responsable n'a pas de processus pour déclencher une

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						alerte en cas de détection d'un accès non autorisé à un point d'accès physique d'un *périmètre de sécurité physique* ou pour communiquer cette alerte au personnel désigné dans un délai de 15 minutes. (1.5) OU L'entité responsable n'a pas de processus pour surveiller chaque *système de contrôle des accès physiques* à la recherche d'accès physiques non autorisés à un *système de contrôle des accès physiques*. (1.6) OU L'entité responsable n'a pas de processus pour déclencher une alerte en cas d'accès physique non autorisé

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						aux *systèmes de contrôle des accès physiques* ou pour communiquer cette alerte au personnel désigné dans un délai de 15 minutes. (1.7) OU L'entité responsable n'a pas de processus pour consigner les accès physiques autorisés à chaque *périmètre de sécurité physique*, avec l'information 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

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						90 jours civils. (1.9) OU L'*entité responsable* n'a pas documenté ni mis en œuvre des restrictions d'accès physique, du cryptage, de la surveillance ou d'autres protections logiques d'une efficacité équivalente pour des câbles et autres composants de communication non programmables qui servent à interrelier des *actifs électroniques* visés situés dans un même *périmètre de sécurité électronique*, si ces câbles et composants se trouvent à l'extérieur d'un *périmètre de*

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						sécurité physique. (1.10)
E2	**Exploitation le même jour**	**Moyen**	Sans objet	Sans objet	Sans objet	L'entité responsable n'a pas adopté 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 adopté ou mis en 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

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						son répondant. (2.2) OU L'entité responsable n'a pas adopté ou mis en œuvre un programme de contrôle des visiteurs pour conserver les registres des visiteurs durant au moins 90 jours. (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 équipements ou dispositifs installés localement au *périmètre de sécurité physique,* mais a terminé l'essai exigé dans un délai de plus de 24 mois civils et d'au plus 25 mois civils.	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 équipements ou dispositifs installés localement au *périmètre de sécurité physique,* mais a terminé l'essai exigé dans un délai de plus de 25 mois civils et d'au plus 26 mois civils.	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 équipements ou dispositifs installés localement au *périmètre de sécurité physique,* mais a terminé l'essai exigé dans un délai de plus de 26 mois civils et d'au plus 27 mois civils.	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 équipements ou dispositifs installés localement au *périmètre de sécurité physique.* (3.1) OU L'entité responsable a

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-006-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			(3.1)	(3.1)	(3.1)	documenté et mis en œuvre un programme de maintenance et d'essai des *systèmes de contrôle des accès physiques* et des équipements ou dispositifs installés localement au *périmètre de sécurité physique,* mais n'a pas terminé l'essai exigé dans un délai de 27 mois civils. (3.1)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

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.	

Version	Date	Intervention	Suivi des modifications
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.	Modification en coordination avec les autres normes CIP et révision du format selon le modèle RBS.
5	22 novembre 2013	Ordonnance de la FERC approuvant CIP-006-5.	
5	9 juillet 2014	Lettre d'ordonnance de la FERC approuvant les révisions des VRF et des VSL de certaines normes CIP.	L'exigence E3 de la norme CIP-006-5 passe de faible à moyen.
6	13 novembre 2014	Adoption par le Conseil d'administration de la NERC.	
6	21 janvier 2016	Ordonnance de la FERC émise approuvant CIP-003-6. Dossier no. RM15-14-000	

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) présente 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, les normes CIP sur la cybersécurité de la NERC s'y appliquent. Il est à noter qu'en ce qui concerne les *distributeurs*, la section 4.1 limite l'applicabilité 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 qui, selon la section 4.1, est visée par les exigences de la norme. Comme il est indiqué à la section d'exemption 4.2.3.5, la présente norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou moyen selon la catégorisation de la norme CIP-002-5.1. 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* » dans le glossaire de la NERC indique déjà qu'il s'agit d'*éléments* du *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 aide à clarifier quels sont les *installations*, systèmes et équipements visés par les normes.

Généralités

Même si l'accent de cette norme de fiabilité 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 un périmètre à six parois demeurera le mécanisme principal pour le contrôle et la journalisation des accès aux *systèmes électroniques BES* et le déclenchement des alertes afférentes. Ensemble, les mécanismes décrits ci-après 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 produit 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 *périmètre de sécurité physique* pour contrôler les accès aux *systèmes électroniques BES* visés. Ces *PACS* n'ont pas à respecter les alinéas 1.1, 1.6 et 1.7 de l'exigence E1 en plus de ce qui s'applique déjà au *périmètre de sécurité physique*.

Le nouvel alinéa 1.10 de l'exigence E1 de la norme CIP-006-6 met en œuvre la prescription du paragraphe 150 de l'ordonnance 791 de la FERC. Cette exigence vise la protection du câblage et des composants de communication non programmables situés à l'intérieur d'un *périmètre de sécurité électronique* (*ESP*), mais qui se prolonge à l'extérieur d'un *périmètre de sécurité physique* (*PSP*). Cette protection, qui rejoint la description faite dans la demande de validation de l'interprétation fournie à PacifiCorp sur la norme CIP-006-2, présentée par la NERC et acceptée par la FERC, doit être réalisée soit par la protection physique des câbles et composants qui sortent d'un *PSP* (par exemple au moyen de conduits ou de chemins de câbles sécurisés), soit par le cryptage des données, par la surveillance des circuits ou par une protection logique d'une efficacité équivalente. Il s'agit de faire en sorte que les protections physiques réduisent la possibilité de sabotage ou d'accès direct aux dispositifs non programmables. Les conduits, les chemins de câbles sécurisés et les armoires de communication sécurisées sont des exemples de ces types de protection. Ces mesures de sécurité physique doivent être mises en œuvre façon à permettre de détecter ou de constater après coup le sabotage possible du câblage et des composants non programmables. Il pourrait s'agir d'un simple cadenas sur une armoire de communication si l'entité est en mesure de constater que le cadenas a été coupé. Un autre moyen pourrait être un câblage armé ou encore le tube en acier inoxydable ou en aluminium qui protège la fibre à l'intérieur d'un câble de garde à fibre optique (CGFO). Lorsqu'on utilise l'une de ces diverses méthodes, il faut prendre soin de protéger toute la longueur du câblage, y compris les points de raccordement qui peuvent se trouver à l'extérieur d'un *PSP*.

Cette partie de l'exigence vise uniquement les portions du câblage et des composants de communication non programmables qui se trouvent à l'extérieur du *PSP*, mais à l'intérieur de l'*ESP*. Dès que ce câblage et ces composants de communication non programmables sont situés à l'intérieur du *PSP*, cette partie de l'exigence ne s'applique plus.

L'exigence porte spécifiquement sur la protection physique du câblage et des composants de communication, puisqu'elle fait partie d'une norme sur la sécurité physique et que la lacune de protection indiquée dans l'ordonnance 791 de la FERC concerne la protection physique. Cependant, cette partie de l'exigence reconnaît qu'il existe plusieurs manières d'assurer la protection du câblage et des composants de communication non programmables. En particulier, l'exigence permet à l'entité d'opter pour une solution autre qu'une protection physique dans une situation où l'entité ne peut pas mettre en œuvre une protection physique, ou si elle choisit simplement de ne pas mettre en œuvre une telle protection. L'entité n'est nullement tenue de justifier ou d'expliquer pourquoi elle a opté pour des protections logiques plutôt que pour les mesures physiques indiquées dans l'exigence.

Les mesures de protection non physique indiquées à l'alinéa 1.10 de l'exigence E1 de la norme CIP-006-6 (cryptage et surveillance des circuits) ont été jugées acceptables dans la demande de validation de l'interprétation fournie à PacifiCorp sur la norme CIP-006-2, présentée par la NERC et acceptée par la FERC (RD10-13-000). Si une entité choisit de mettre en œuvre « une protection logique d'une efficacité équivalente » au lieu des mécanismes de protection indiqués dans la norme, l'entité devrait normalement documenter pourquoi elle considère cette protection comme étant d'une efficacité équivalente. La NERC explique dans sa requête sur l'interprétation fournie à PacifiCorp sur la norme CIP-006-2 que les mesures concernent

l'accès ainsi que le sabotage physique. Par conséquent, l'entité peut choisir d'indiquer comment sa protection peut assurer la détection du sabotage. L'entité peut aussi choisir d'expliquer comment sa protection est équivalente aux autres options logiques présentées dans la norme relativement à la triade « confidentialité, intégrité et disponibilité ». L'entité peut trouver utile de soumettre ses plans à l'entité régionale avant la mise en œuvre, mais elle n'est pas tenue de le faire.

Cette exigence ne spécifie pas de protection physique pour des équipements de tiers, comme l'indique l'ordonnance 791-A de la FERC. L'exigence accorde à l'entité la latitude voulue pour concevoir son *ESP* et aussi pour le prolonger à l'extérieur de son *PSP* au moyen des mécanismes logiques spécifiés à la partie 1.10 de l'exigence E1 de la norme CIP-006-6, notamment le cryptage (option indiquée nommément dans l'ordonnance 791-A de la FERC). Ces mécanismes devraient offrir aux *systèmes électroniques BES* de l'entité une protection suffisante pour qu'il ne soit pas nécessaire d'appliquer des mesures à des équipements de tiers lorsque l'entité utilise des liaisons de communication louées.

En plus du câblage, les composants visés par cette partie de l'exigence sont les composants situés à l'extérieur d'un *PSP* et qui pourraient presque être considérés comme des *actifs électroniques BES* ou des *actifs électroniques protégés*, sauf qu'ils ne répondent pas à la définition d'*actif électronique* puisqu'ils ne sont pas programmables. Exemples non limitatifs de tels composants non programmables : commutateurs, concentrateurs, panneaux de répartition, convertisseurs de support, adaptateurs de port et raccords non gérés.

Exigence E2

Les données d'accès des visiteurs doivent être consignées une seule fois par visite et non chaque fois que le visiteur 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.

La 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 à effectuer sur l'équipement et les dispositifs installés localement pour assurer le contrôle des accès aux *périmètres de sécurité physique*, ainsi que le déclenchement 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*.

Justification :

Pendant l'élaboration de cette norme, des zones de texte ont été incorporées à celle-ci pour exposer la justification de ses diverses parties. Après l'approbation par le Conseil d'administration, le contenu de ces zones de texte a été transféré ci-après.

Justification de l'exigence 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 *périmètre de sécurité physique* pour contrôler les accès aux *systèmes électroniques BES* visés. Ces *PACS* n'ont pas à respecter les alinéas 1.1, 1.6 et 1.7 de l'exigence E1 en plus de ce qui s'applique déjà au *périmètre de sécurité physique*.

Quant à l'alinéa 1.10 de l'exigence E1, lorsque des câbles ou autres composants non programmables du réseau de communication d'un *centre de contrôle* ne peuvent pas être sécurisés dans un *périmètre de sécurité physique* (*PSP*), il faut prendre des mesures pour assurer l'intégrité des *systèmes électroniques BES*. Si des trajets de communication sont exposés à l'extérieur d'un *PSP*, il faut mettre en place des protections physiques ou logiques afin de réduire la probabilité que des attaques par interposition puissent compromettre l'intégrité des *actifs électroniques BES* raccordés ou des *PCA* qui doivent résider dans des *PSP*. Bien qu'il convienne d'envisager d'abord une protection physique du câblage et des composants de communication non programmables, la SDT comprend que certaines configurations se prêtent mal à des restrictions d'accès physique et que les entités responsables sont en mesure de défendre raisonnablement leurs composants de communication exposés physiquement au moyen de protections logiques supplémentaires.

Justification de l'exigence E2 :

Il s'agit de 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.

Justification de l'exigence E3 :

Il s'agit de faire en sorte que tous les dispositifs et *systèmes de contrôle des accès physiques* continuent de fonctionner correctement.

Annexe QC-CIP-006-6
Dispositions particulières de la norme CIP-006-6 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-006-6

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

4.1. Entités Fonctionnelles

Aucune disposition particulière

4.2. Installations

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

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

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

5. **Date d'entrée en vigueur 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 :

Norme	Révision CIPv6	Date d'entrée en vigueur proposée au Québec		
		Entités visées par la version 1 des normes CIP adoptées par la Régie	Entités ne possédant pas d'installations de production à vocation industrielle et non visées par la version 1 des normes CIP	Entités qui possèdent des installations de production à vocation industrielle
CIP-006-6	Élimination de la formulation « détecter, évaluer et corriger » car elle est vague et sujette à de multiples interprétations	2017-10-01	2018-10-01	2019-04-01
CIP-006-6, E1, l'alinéa 1.10	Pour les systèmes électroniques BES existants des centres de contrôles	2017-10-01	2018-10-01	2019-04-01

Les ajouts et modifications proposés au glossaire pour les termes suivants doivent être approuvés et en vigueur en même temps que la norme : [1]

- « *actifs électroniques BES* »;
- « *actifs électroniques protégés* ».

6. Contexte :

Aucune disposition particulière

[1] Cette section sera retirée suivant l'adoption de la norme par la Régie.

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Justification

Aucune disposition particulière

Historique des versions

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-007-6

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 *système de production-transport d'électricité* (*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* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale ; et

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

4.1.2.2 Chaque *automatisme de réseau (SPS)* ou *plan de défense (RAS)* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

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

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

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

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

4.1.5 ***Coordonnateur des échanges* ou *responsable des échanges***

4.1.6 ***Coordonnateur de la fiabilité***

4.1.7 ***Exploitant de réseau de transport***

4.1.8 ***Propriétaire d'installation de transport***

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

4.2.1 Distributeur : Un ou plusieurs des *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* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale ; et

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

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du *BES*.

4.2.3 Exemptions : Sont exemptés de la norme CIP-007-6 :

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 composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme au règlement CFR 10, section 73.54 ;

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

4.2.3.5 les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* classés dans les catégories « impact élevé » ou « impact moyen » selon le processus de désignation et de catégorisation de la norme CIP-002-5.1.

5. Dates d'entrée en vigueur :

Voir le plan de mise en œuvre de la norme CIP-007-6.

6. Contexte :

La norme CIP-007 fait partie d'une série de normes CIP sur la cybersécurité qui exigent la détermination et la catégorisation initiales des *systèmes électroniques BES*. Ces normes exigent aussi un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.

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

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité doit inclure tout ce qu'elle juge nécessaire dans ses processus documentés, en s'assurant de bien couvrir les exigences pertinentes.

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

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation

du personnel sont des exemples qui figurent dans les normes. La mise en œuvre complète des normes de fiabilité CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

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

Les mesures auxquelles renvoie l'énoncé initial de l'exigence correspondent simplement aux processus documentés eux-mêmes. La colonne « Mesures » présente des exemples de pièces justificatives attestant la documentation et la mise en œuvre des éléments pertinents dans les processus documentés ; ces exemples sont présentés à titre indicatif, et leur liste ne doit pas être considérée comme exhaustive.

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

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes 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 *BES*. Un examen des tolérances des 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. La SDT (équipe de rédaction) CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- ***Systèmes électroniques BES* à impact élevé –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.

- ***Systèmes électroniques BES* à impact moyen –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.
- ***Systèmes électroniques BES* à impact moyen de *centres de contrôle* –** Désigne uniquement les *systèmes électroniques BES* à impact moyen situés dans des *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*, à l'exclusion des *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'événements et d'alerte.
- ***Systèmes de contrôle des accès physiques* (*PACS*)** – Désigne tout *système de contrôle des accès physique*s associés 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 un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-007-6) – Ports et services.
[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation le même jour]

M1. Les pièces justificatives doivent comprendre chacun des processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-007-6) – Ports et services ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-007-6) – Ports et services			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.1	*Systèmes électroniques BES* à impact élevé et : 1. les EACMS associés ; 2. les PACS associés ; et 3. les PCA associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les EACMS associés ; 2. les PACS associés ; et 3. les PCA associés.	Si cela est 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 d'écoute des *actifs électroniques*, pris individuellement ou collectivement, provenant des fichiers de configuration des dispositifs, du résultat de commandes comme 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-007-6) – Ports et services			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.2	*Systèmes électroniques BES* à impact élevé et : 1. les *PCA* associés ; et 2. les composants de communication non programmables associés situés à la fois dans un *périmètre de sécurité physique* et dans un *périmètre de sécurité électronique*. *Systèmes électroniques BES* à impact moyen de *centres de contrôle* et : 1. les *PCA* associés ; et 2. les composants de communication non programmables associés situés à la fois dans un *périmètre de sécurité physique* et dans un *périmètre de sécurité électronique*.	Empêcher l'utilisation de ports d'entrée-sortie physiques non nécessaires utilisés pour la connectivité de réseau, les commandes pupitre ou les *supports de stockage amovibles*.	Exemple non limitatif de pièces justificatives : 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 un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-007-6) – Gestion des correctifs 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 qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés; et 3. les *PCA* associés.	Un processus de gestion des correctifs portant sur le suivi, l'évaluation et l'installation des correctifs 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 correctifs de cybersécurité destinés aux *actifs électroniques* visés qui sont actualisables et pour lesquels il existe une source de correctifs.	Exemples non limitatifs de pièces justificatives : documentation d'un processus de gestion des correctifs 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-007-6) – Gestion des correctifs de sécurité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Au moins une fois tous les 35 jours civils, évaluer l'applicabilité des correctifs de sécurité publiés par la ou les sources indiquées à l'alinéa 2.1 depuis l'évaluation précédente.	Exemple non limitatif de pièces justificatives : une évaluation effectuée ou citée par une entité responsable ou réalisée en son nom et portant sur les correctifs de sécurité publiés par les sources documentées, et ce, au moins tous les 35 jours civils.

Tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.3	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Pour les correctifs jugés applicables selon l'alinéa 2.2, prendre une des mesures suivantes dans les 35 jours civils suivant la fin de l'évaluation : • appliquer les correctifs applicables ; • créer un plan d'atténuation daté ; ou • réviser un plan d'atténuation existant. Les plans d'atténuation doivent comprendre les mesures que l'entité responsable compte prendre pour atténuer les vulnérabilités visées par chaque correctif de sécurité, ainsi qu'un délai de mise en œuvre de ces mesures.	Exemples non limitatifs de pièces justificatives : • enregistrements d'installation des correctifs (p. ex. rapport exporté d'un outil automatisé de gestion des correctifs indiquant 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 atténuer les vulnérabilités visées par le correctif de sécurité et qui précise un délai d'exécution des mesures d'atténuation.

Tableau E2 (CIP-007-6) – Gestion des correctifs de sécurité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.4	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Pour chaque plan d'atténuation créé ou mis à jour selon l'alinéa 2.3, mettre le plan en œuvre dans le délai qui y est précisé, à moins qu'une révision du plan ou un prolongement du délai indiqué à l'alinéa 2.3 soit approuvé par le *cadre supérieur CIP* ou son délégataire.	Exemple non limitatif de pièces justificatives : registres de mise en œuvre des plans d'atténuation.

E3. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E3 (CIP-007-6) – Protection contre les programmes malveillants.
[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation le même jour]

M3. Les pièces justificatives doivent comprendre chacun des processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E3(CIP-007-6) – Protection contre les programmes malveillants ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E3 (CIP-007-6) – Protection contre les programmes malveillants			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Utiliser une ou des méthodes pour bloquer, détecter ou prévenir les programmes malveillants.	Exemple non limitatif de pièces justificatives : suivis de la mise en œuvre de ces méthodes par l'entité responsable (au moyen de logiciels antivirus habituels, du renforcement des systèmes, de politiques, etc.).

Tableau E3 (CIP-007-6) – Protection contre les programmes malveillants			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Atténuer 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 performance de ces processus lorsque des programmes malveillants sont détectés.
3.3	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Pour les méthodes indiquées à l'alinéa 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 pièces justificatives : documentation décrivant le processus de mise à jour des signatures et des séquences de code.

E4. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E4 (CIP-007-6) – Surveillance des événements de sécurité.
[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation le même jour et évaluation des activités d'exploitation]

M4. Les pièces justificatives doivent comprendre chacun des processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E4 (CIP-007-6) – Surveillance des événements de sécurité ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E4 (CIP-007-6) – Surveillance des événements de sécurité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
4.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *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 ; et 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 automatiquement, et, le cas échéant, qu'il est configuré pour journaliser. Cette liste doit comprendre les types d'événements obligatoires.

Tableau E4 (CIP-007-6) – Surveillance des événements de sécurité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
4.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *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 l'alinéa 4.1 ; et 4.2.2. échec détecté de la journalisation des événements définis à l'alinéa 4.1.	Exemples non limitatifs de pièces justificatives : liste, générée manuellement ou automatiquement, des événements de sécurité qui, selon l'entité responsable, nécessitent des alertes, y compris une liste, générée manuellement ou automatiquement, indiquant la configuration des alertes.

Tableau E4 (CIP-007-6) – Surveillance des événements de sécurité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
4.3	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen de *centres de contrôle* et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Si cela est techniquement faisable, conserver les journaux des événements exigés à l'alinéa 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 automatiquement 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 : 1. les *EACMS* associés ; et 2. les *PCA* associés.	Examiner un résumé ou un échantillon des événements journalisés, tels que définis par l'entité responsable, à intervalles d'au plus 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 un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E5 (CIP-007-6) – 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 qui, collectivement, couvrent tous les alinéas applicables du tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
5.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen de *centres de contrôle* et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Avoir une ou plusieurs méthodes pour imposer l'authentification de tout accès utilisateur interactif, si cela est techniquement faisable.	Exemple non limitatif de pièces justificatives : documentation décrivant le mode d'authentification des accès.

Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
5.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	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 pièces justificatives : 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 : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Recenser toutes les personnes ayant un accès autorisé à des comptes partagés.	Exemple non limitatif de pièces justificatives : liste des comptes partagés et des personnes qui y ont un accès autorisé.

Tableau E5 (CIP-007-6) – Contrôle des accès aux systèmes			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
5.4	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *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-007-6) – Contrôle des accès aux systèmes			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
5.5	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	En ce qui concerne l'authentification uniquement par mot de passe 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 ; et 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, etc.) ou du maximum permis par l'*actif électronique*, selon la moindre des deux.	Exemples non limitatifs de pièces justificatives : • rapports générés automatiquement 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-007-6) – Contrôle des accès aux systèmes			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
5.6	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Si cela est techniquement faisable, pour toute authentification uniquement par mot de passe 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 automatiquement ou captures d'écran montrant la fréquence de changement de 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 : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen de *centres de contrôle* et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Si cela est techniquement faisable : • limiter le nombre de tentatives d'authentification infructueuses ; ou • générer des alertes après un certain nombre de tentatives d'authentification infructueuses.	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'authentification infructueuses.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Selon la définition des règles de procédure de la NERC, le terme « *responsable des mesures pour assurer la conformité* » (*CEA*) désigne la NERC ou l'entité régionale dans leurs rôles respectifs de surveillance de la conformité aux normes de fiabilité de la NERC.

1.2. Conservation des pièces justificatives

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

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

- Chaque entité 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 approuvé 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 de mise en application des normes

Audits de conformité

Déclarations sur la conformité

Contrôles ponctuels

Enquêtes de conformité

Déclarations de non-conformité

Plaintes

1.4. Autres informations sur la conformité

Aucune.

2. Tableau des éléments de conformité

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1	**Exploitation le même jour**	**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 de stockage amovibles*. (1.2)	L'entité responsable a mis en œuvre et documenté des processus pour déterminer les ports et services nécessaires, mais un ou plusieurs ports logiques accessibles par le réseau et jugés non nécessaires étaient activés même s'il était techniquement faisable de les désactiver. (1.1)	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus parmi les éléments applicables du tableau E1 (CIP-007-6). (E1)
E2	**Planification de l'exploitation**	**Moyen**	L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour évaluer l'applicabilité des correctifs de sécurité publiés et non installés, mais a évalué l'applicabilité des correctifs de sécurité dans un délai de plus de 35 jours civils et d'au plus 50 jours civils après l'évaluation précédente pour la ou les sources indiquées. (2.2) OU L'entité responsable a un ou plusieurs processus documentés pour l'évaluation des correctifs	L'entité responsable a documenté ou mis en œuvre un ou plusieurs processus pour la gestion des correctifs, mais n'a inclus aucun processus comprenant la désignation de la ou des sources pour le suivi ou l'évaluation des correctifs de cybersécurité destinés aux *actifs électroniques* visés. (2.1) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour évaluer l'applicabilité des correctifs de sécurité publiés et non	L'entité responsable a documenté ou mis en œuvre un ou plusieurs processus pour la gestion des correctifs, mais n'a inclus aucun processus pour l'installation des correctifs de cybersécurité destinés aux *actifs électroniques* visés. (2.1) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour évaluer l'applicabilité des correctifs de sécurité publiés et non installés, mais n'a pas évalué l'applicabilité des	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus parmi les éléments applicables du tableau E2 (CIP-007-6). (E2) OU L'entité responsable a documenté ou mis en œuvre un ou plusieurs processus pour la gestion des correctifs, mais n'a inclus aucun processus pour le suivi, l'évaluation ou l'installation des correctifs de cybersécurité destinés aux *actifs électroniques* visés. (2.1)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			de cybersécurité, mais, afin d'atténuer les vulnérabilités exposées par les correctifs de sécurité applicables, a appliqué les correctifs applicables, créé un plan d'atténuation daté, ou révisé un plan d'atténuation existant dans un délai de plus de 35 jours civils et d'au plus 50 jours civils après la fin de l'évaluation. (2.3)	installés, mais a évalué l'applicabilité des correctifs de sécurité dans un délai de plus de 50 jours civils et d'au plus 65 jours civils après l'évaluation précédente pour la ou les sources indiquées. (2.2) OU L'entité responsable a un ou plusieurs processus documentés pour l'évaluation des correctifs de cybersécurité, mais, afin d'atténuer les vulnérabilités exposées par les correctifs de sécurité applicables, a appliqué les correctifs applicables, créé un plan d'atténuation daté ou révisé un plan d'atténuation existant dans un délai de plus de 50 jours civils et d'au plus 65 jours civils après la fin de l'évaluation. (2.3)	correctifs de sécurité dans les 65 jours civils après l'évaluation précédente pour la ou les sources indiquées. (2.2) OU L'entité responsable a un ou plusieurs processus documentés pour l'évaluation des correctifs de cybersécurité, mais, afin d'atténuer les vulnérabilités exposées par les correctifs de sécurité applicables, n'a pas appliqué les correctifs applicables, créé un plan d'atténuation daté ou révisé un plan d'atténuation existant dans les 65 jours civils après la fin de l'évaluation. (2.3)	OU L'entité responsable a documenté un plan d'atténuation pour un correctif 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 délégataire. (2.4) OU L'entité responsable a documenté un plan d'atténuation pour un correctif de cybersécurité applicable, mais n'a pas mis en œuvre le plan tel que créé ou révisé dans le délai spécifié dans le plan. (2.4)
E3	**Exploitation le même jour**	**Moyen**	Sans objet	L'entité responsable a mis en œuvre un ou plusieurs processus documentés, mais, dans les cas où des signatures ou des séquences de code sont utilisées, l'entité	L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour la protection contre les programmes malveillants, mais n'a pas atténué la menace des programmes	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus parmi les éléments applicables du tableau E3 (CIP-007-6). (E3)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				responsable n'a pas traité de l'essai des signatures et des séquences de code. (3.3)	malveillants détectés. (3.2) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour la protection contre les programmes malveillants, 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 programmes malveillants. (3.3)	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 malveillants. (3.1)
E4	**Exploitation le même jour et évaluation des activités d'exploitation**	**Moyen**	L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour repérer les *incidents de cybersécurité* non détectés en examinant, au moins tous les 15 jours civils, un résumé ou un échantillon des événements journalisés défini par l'entité, mais a raté un intervalle et terminé l'examen dans les 22 jours civils après l'examen précédent. (4.4)	L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour repérer les *incidents de cybersécurité* non détectés en examinant, au moins tous les 15 jours civils, un résumé ou un échantillon des événements journalisés défini par l'entité, mais a raté un intervalle et terminé l'examen dans les 30 jours civils après l'examen précédent. (4.4)	L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour générer des alertes pour les événements de sécurité nécessaires (selon le jugement de l'entité responsable) pour les systèmes applicables (selon les capacités du dispositif ou du système), mais n'a pas généré d'alertes pour tous les types d'événements indiqués en 4.2.1 à 4.2.2. (4.2) OU	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs processus parmi les éléments applicables du tableau E4 (CIP-007-6). (E4) OU L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour journaliser les événements pour les systèmes applicables (selon les capacités du dispositif ou du système), mais n'a pas journalisé tous les types d'événements requis

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
					L'entité responsable a documenté et mis en œuvre un ou plusieurs processus pour journaliser les événements applicables indiqués en 4.1 (si cela est 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. (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 examinant, au moins tous les 15 jours civils, un résumé ou un échantillon des événements journalisés défini par l'entité, mais a raté deux intervalles ou plus. (4.4)	indiqués en 4.1.1 à 4.1.3. (4.1)
E5	**Planification de l'exploitation**	**Moyen**	L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification uniquement par mot de passe de l'accès utilisateur	L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification uniquement par mot de passe de l'accès utilisateur	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'inventaire de tous	L'entité responsable n'a pas mis en œuvre ou documenté un ou plusieurs des processus qui couvrent les alinéas applicables du

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			interactif, mais a imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe dans un délai de plus de 15 mois civils et d'au plus 16 mois civils après le dernier changement de mot de passe. (5.6)	interactif, mais a imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe dans un délai de plus de 16 mois civils et d'au plus 17 mois civils après le dernier changement de mot de passe. (5.6)	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. (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 le recensement des personnes ayant un accès autorisé à des comptes partagés. (5.3) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification uniquement par mot de passe de l'accès utilisateur interactif qui n'imposent pas, par des moyens techniques ou procéduraux, un des deux paramètres de mot de passe indiqués en 5.5.1 et 5.5.2. (5.5) OU	tableau E5 (CIP-007-6). (E5) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais n'a pas de méthodes pour imposer l'authentification de l'accès utilisateur interactif même si c'est techniquement faisable. (5.1) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais n'a pas, selon les capacités du dispositif, changé les mots de passe par défaut connus. (5.4) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification uniquement par mot de passe de l'accès utilisateur interactif qui n'imposent, par des moyens techniques

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
					L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification uniquement par mot de passe de l'accès utilisateur interactif, mais a imposé par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe dans un délai de plus de 17 mois civils et d'au plus 18 mois civils après le dernier changement de mot de passe. (5.6)	ou procéduraux, aucun des paramètres de mot de passe indiqués en 5.5.1 et 5.5.2. (5.5) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour l'authentification uniquement par mot de passe 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 un délai de 18 mois civils après le dernier changement de mot de passe. (5.6) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés pour le contrôle des accès aux systèmes, mais n'a pas soit limité le nombre de tentatives d'authentification infructueuses, soit généré des alertes après un certain

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-007-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						nombre de tentatives d'authentification infructueuses, même si c'est techniquement faisable. (5.7)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	16 janvier 2006	E3.2 — Remplacement de « Control Center » par « control center ».	24 mars 2006
2	30 septembre 2009	Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes. Suppression de la mention sur la prise en compte des considérations d'affaires. Remplacement de l'organisation régionale de fiabilité par l'entité régionale comme entité responsable. Reformulation de la date d'entrée en vigueur. Remplacement de « Responsabilité de la surveillance de la conformité » par « Responsable des mesures pour assurer la conformité ».	
3	16 décembre 2009	Changement du numéro de version de -2 à -3. Approbation par le Conseil d'administration de la NERC. Dans l'exigence 1.6, suppression de la phrase concernant le retrait du service d'un composant ou d'un	

		système aux fins d'essais, en réponse 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.	Remaniement en coordination avec les autres normes CIP et révision du format selon le modèle RBS.
5	22 novembre 2013	Ordonnance de la FERC approuvant la norme CIP-007-5.	
6	13 novembre 2014	Adoption par le Conseil d'administration de la NERC.	Mise en œuvre de deux prescriptions de l'ordonnance 791 de la FERC concernant l'obligation de « détecter, évaluer et corriger » ainsi que les réseaux de communication.
6	12 février 2015	Adoption par le conseil d'administration de la NERC	Remplace la version adoptée par le conseil d'administration le 13 novembre 2014. La version à jour met en œuvre des prescriptions en instance de l'ordonnance 791 relativement aux actifs temporaires et aux *systèmes électroniques BES* à impact faible.
6	21 janvier 2016	Ordonnance de la FERC émise approuvant CIP-003-6. Dossier no. RM15-14-000	

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) présente 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, les normes CIP sur la cybersécurité de la NERC s'y appliquent. Il est à noter qu'en ce qui concerne les *distributeurs*, la section 4.1 limite l'applicabilité 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 qui, selon la section 4.1, est visée par les exigences de la norme. Comme il est indiqué à la section d'exemption 4.2.3.5, la présente norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou moyen selon la catégorisation de la norme CIP-002-5.1. 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* » dans le glossaire de la NERC indique déjà qu'il s'agit d'*éléments* du *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 aide à clarifier 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 de la SDT est de faire en sorte que l'entité sache quels ports et services connexes sont accessibles (« ports d'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, la 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 du *périmètre de sécurité électronique* 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.

Les ports réseau visés par cet alinéa de l'exigence ne se limitent pas à ceux du *système électronique BES* lui-même. Les ports réseau physiques comprennent ceux qui peuvent exister dans des dispositifs non programmables comme des commutateurs, des concentrateurs ou des panneaux de répartition non gérés.

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 *périmètre de sécurité physique*, qui empêche 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 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 possiblement infecté sur le port USB du pupitre d'un répartiteur afin d'en recharger la pile.

La colonne Systèmes visés de l'alinéa 1.2 de l'exigence E1 a été modifiée dans la version CIP-007-6, de manière à s'appliquer aux « composants de communication non programmables associés situés à la fois dans un *périmètre de sécurité physique* et dans un *périmètre de sécurité*

électronique ». Sont ainsi visés uniquement les composants de communication non programmables qui sont situés dans un *périmètre de sécurité physique* et aussi dans un *périmètre de sécurité électronique*, et non les composants situés dans un seul périmètre, comme l'illustre le schéma suivant :

Location of nonprogrammable communication components	Emplacement des composants de communication non programmables
PSP	Périmètre de sécurité physique
ESP	Périmètre de sécurité électronique
Applicability of CIP-007-6 R1, Part 1.2 for nonprogrammable communication components	Applicabilité de l'alinéa 1.2 de l'exigence E1 de la norme CIP-007-6 aux composants de communication non programmables

Exigence E2

L'intention de la 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 atténuer les effets. Il ne s'agit pas de leur imposer l'installation de chaque correctif 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 correctifs 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 correctifs 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 correctifs qui aborde le suivi, l'évaluation et l'installation des correctifs de cybersécurité. Cette exigence s'applique uniquement aux correctifs 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 correctifs permettant de corriger des problèmes de cybersécurité et exclut les correctifs 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 nouveaux correctifs de cybersécurité pertinentes pour les *actifs électroniques*. La documentation de la source de correctifs est exigée à l'étape de suivi pour déterminer à quel moment commence la période d'évaluation. Cette exigence tient compte des situations où un correctifs de sécurité peut

provenir d'une première source (comme un fournisseur de systèmes d'exploitation), mais qu'elle doit être approuvée ou certifiée par une autre source (comme 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 correctifs de sécurité, de correctifs et de mises à jour. Une source de correctifs 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 correctifs, 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 correctifs de sécurité dans les 35 jours civils suivant leur publication par la source suivie. L'évaluation doit consister à déterminer l'applicabilité de chaque à l'environnement et aux systèmes propres à l'entité. Cela consiste principalement à vérifier si le correctif s'applique à un composant logiciel ou matériel particulier que l'entité a installé dans un *actif électronique* visé. Un correctif conçu 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 le correctif est non pertinent, il lui suffit de le documenter et de le justifier pour être conforme. Si le correctif est pertinent, 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 correctifs de sécurité, des correctifs ou des mises à jour ou des mesures de neutralisation. Il est en effet possible que des correctifs, 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'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 correctif 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 le correctif, soit de documenter, au moyen d'un nouveau plan d'atténuation ou de la mise à jour d'un plan existant, ce qu'elle entend faire pour atténuer la vulnérabilité et à quel moment elle compte le faire. Il est parfois plus judicieux, pour protéger la fiabilité, de ne pas installer un correctif, auquel cas l'entité peut consigner les mesures qu'elle a prises pour atténuer la vulnérabilité. Lorsque des correctifs de sécurité sont jugés pertinents, l'entité responsable doit, dans les 35 jours civils, les installer, créer un plan d'atténuation daté qui décrit les mesures à prendre ou celles qu'elle a déjà prises pour atténuer les vulnérabilités visées par les correctifs de sécurité, ou réviser un plan d'atténuation 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 d'atténuation dont il est question dans la présente norme désignent des documents internes et ne doivent pas être confondus avec les plans d'atténuation 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 contrôle créés pour y faire face, il n'est pas pratique de prescrire dans la norme la façon de protéger chaque *actif électronique* contre les maliciels. 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, 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 atténuée. 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 atténuer 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 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 d'atténuer la menace posée par le programme malveillant qui a été identifié.

Les entités doivent aussi être au courant des exigences de protection contre les maliciels applicables aux *actifs électroniques temporaires* et aux *supports de stockage amovibles* (« dispositifs temporaires ») énoncées dans la norme CIP-010-2. Les protections prescrites dans l'exigence E3 de la norme CIP-007-6 complètent ces obligations supplémentaires visant les dispositifs temporaires, mais ne suffisent pas pour s'y conformer.

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 maliciel 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 son *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 répertoriés 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'événement 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 de la SDT n'est pas qu'une exception liée à la faisabilité technique (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 dans 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 pour certains comptes en dehors des heures ouvrables ;
- changements de configuration non autorisés ;
- insertion d'un support de stockage amovible en infraction à une politique.

4.3 Les journaux créés conformément à l'alinéa 4.1 doivent être conservés dans 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 compte dont il est question dans cette exigence comprennent les suivants :

- Compte utilisateur partagé : compte employé par plusieurs utilisateurs – employés ou contractuels – dans le cours normal des activités. Il se trouve habituellement dans un dispositif qui ne prend pas en charge les comptes d'utilisateur individuel.
- 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 partagé.

- 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 contractuels 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 partagé 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 partagés 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 cet alinéa de l'exigence. Les entités peuvent aussi choisir de tenir une liste distincte pour les comptes partagés. Les deux formes de preuves sont conformes au résultat visé, soit conserver le contrôle des comptes partagés.

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.

Des 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 Des 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 nombre d'échecs doit être assez élevé pour éviter les faux positifs imputables à des utilisateurs autorisés qui ne réussissent pas à s'authentifier, mais assez bas pour contrer les attaques étalées 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.

Justification

Pendant l'élaboration de cette norme, des zones de texte ont été incorporées à celle-ci pour exposer la justification de ses diverses parties. Après l'approbation par le Conseil d'administration, le contenu de ces zones de texte a été transféré ci-après.

Justification de l'exigence E1

Cette exigence vise à réduire au minimum 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.

En réponse au renvoi par la FERC (paragraphe 149 de son ordonnance 791) à la mesure de sécurité PE-4 de la norme NIST 800-53, révision 3, l'alinéa 1.2 a été modifié pour englober les *PCA* et les composants de communication non programmables. Cette extension de l'applicabilité étend la portée des dispositifs qui bénéficient de la « défense en profondeur » invoquée par l'alinéa 1.2 de l'exigence E1.

L'applicabilité est limitée aux composants de communication non programmables situés à la fois dans un *périmètre de sécurité physique* et dans un *périmètre de sécurité électronique* afin de permettre à l'entité responsable d'établir un *périmètre de sécurité électronique* étendu (avec des protections logiques correspondantes indiquées à l'alinéa 1.10 de l'exigence E1 et la norme CIP-006). Dans un tel scénario, les composants non programmables du réseau de communication peuvent se trouver hors du contrôle de l'entité responsable (s'ils font, par exemple, partie intégrante du réseau de télécommunication commercial).

Justification de l'exigence E2

La gestion des correctifs 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.

Justification de l'exigence 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*.

Justification de l'exigence 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.

Justification de l'exigence E5

Il s'agit de 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'alinéa 5.1 de l'exigence 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'alinéa 5.2 de l'exigence porte sur les comptes par défaut et autres comptes génériques. Le fait que l'entité consigne quelle 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*. Cet alinéa de l'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'alinéa 5.3 de l'exigence porte sur les personnes ayant accès aux comptes partagés. L'objectif est de neutraliser le risque d'accès non autorisé par l'intermédiaire de comptes partagés. 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 partagés 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'alinéa 5.4 de l'exigence 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 automatiquement 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 afin de 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 dévoiler un mot de passe crypté, ainsi que de remplacer tout mot de passe qui aurait été divulgué 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'utilisateur individuel. Toutefois, dans le cas des comptes partagés 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'alinéa 5.7 de l'exigence aide à prévenir les attaques perpétrées en ligne visant les mots de passe en limitant le nombre de tentatives possibles. 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*.

Annexe QC-CIP-007-6
Dispositions particulières de la norme CIP-007-6 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-007-6

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

4.1. Entités fonctionnelles

Aucune disposition particulière

4.2. Installations

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

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

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

5. **Date d'entrée en vigueur 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 :

Norme	Révision CIPv6	Date d'entrée en vigueur proposée au Québec		
		Entités visées par la version 1 des normes CIP adoptées par la Régie	Entités ne possédant pas d'installations de production à vocation industrielle et non visées par la version 1 des normes CIP	Entités qui possèdent des installations de production à vocation industrielle
CIP-007-6	Élimination de la formulation « détecter, évaluer et corriger » car elle est vague et sujette à de multiples interprétations	2017-10-01	2018-10-01	2019-04-01
CIP-007-6, E1, l'alinéa 1.2	Pour les PCA et les composantes de communication non programmables situés à la fois dans un périmètre de sécurité physique et dans un périmètre de sécurité électronique pour les systèmes électronique BES à impact moyen ou élevé)	2017-10-01	2018-10-01	2019-04-01

Les ajouts et modifications proposés au glossaire pour les termes suivants doivent être approuvés et en vigueur en même temps que la norme : [1]

- « *actif électronique transitoire* » ;
- « *support d'information de stockage* » ;
- « *actifs électroniques BES* » ;
- « *actifs électroniques protégés* ».

6. Contexte :

Aucune disposition particulière

[1] Cette section sera retirée suivant l'adoption de la norme par la Régie.

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

Aucune disposition particulière

1.2. Processus de surveillance et de mise en application des normes

Aucune disposition particulière

1.3. 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

Justification

Aucune disposition particulière

Historique des versions

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-009-6

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 *système de production-transport d'électricité* (*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* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale ; et

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

4.1.2.2 Chaque *automatisme de réseau* ou *plan de défense* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

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

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

4.1.3 Exploitant d'installation de production

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

4.1.5 ***Coordonnateur des échanges ou responsable des échanges***

4.1.6 ***Coordonnateur de la fiabilité***

4.1.7 ***Exploitant de réseau de transport***

4.1.8 ***Propriétaire d'installation de transport***

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

4.2.1 **Distributeur :** Un ou plusieurs des *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* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale ; et

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

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

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

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

4.2.2 **Entités responsables indiquées en 4.1, sauf les distributeurs :**

Toutes les *installations* du BES.

4.2.3 **Exemptions :** Sont exemptés de la norme CIP-009-6 :

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 composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme au règlement CFR 10, section 73.54 ;

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

4.2.3.5 les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* classés dans les catégories « impact élevé » ou « impact moyen » selon le processus de désignation et de catégorisation de la norme CIP-002-5.1.

5. Dates d'entrée en vigueur

Voir le plan de mise en œuvre de la norme CIP-009-6.

6. Contexte :

La norme CIP-009 fait partie d'une série de normes CIP sur la cybersécurité qui exigent la détermination et la catégorisation initiales des *systèmes électroniques BES*. Ces normes exigent aussi un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.

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

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité doit inclure tout ce qu'elle juge nécessaire dans ses processus documentés, en s'assurant de bien couvrir les exigences pertinentes.

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

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

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

Les mesures auxquelles renvoie l'énoncé initial de l'exigence correspondent simplement aux processus documentés eux-mêmes. La colonne « Mesures » présente des exemples de pièces justificatives attestant la documentation et la mise en œuvre des éléments pertinents dans les processus documentés ; ces exemples sont présentés à titre indicatif, et leur liste ne doit pas être considérée comme exhaustive.

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

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et le 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 BES. Un examen des tolérances des 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. La SDT (équipe de rédaction) CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- ***Systèmes électroniques BES* à impact élevé –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.
- ***Systèmes électroniques BES* à impact moyen –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.
- ***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 catégorie « impact moyen », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.

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

B. Exigences et mesures

E1. Chaque entité responsable doit avoir un ou plusieurs plans de rétablissement documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-009-6) – 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, couvrent tous les alinéas applicables du tableau E1 (CIP-009-6) – Caractéristiques d'un plan de rétablissement.

Tableau E1 (CIP-009-6) – Caractéristiques d'un plan de rétablissement			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.1	*Systèmes électroniques BES* à impact élevé et : 1. les EACMS associés ; et 2. les PACS associés. *Systèmes électroniques BES* à impact moyen et : 1. les EACMS associés ; et 2. les 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 : 1. les EACMS associés ; et 2. les PACS associés. *Systèmes électroniques BES* à impact moyen et : 1. les EACMS associés ; et 2. les 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-009-6) – Caractéristiques d'un plan de rétablissement			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.3	*Systèmes électroniques BES* à impact élevé et : 1. les EACMS associés ; et 2. les PACS associés. *Systèmes électroniques BES* à impact moyen et : 1. les EACMS associés ; et 2. les 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 : 1. les EACMS associés ; et 2. les PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et : 1. les EACMS associés ; et 2. les PACS associés.	Un ou plusieurs processus de vérification du bon déroulement des processus de sauvegarde énoncés à l'alinéa 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 : 1. les EACMS associés ; et 2. les PACS associés. *Systèmes électroniques BES* à impact moyen et : 1. les EACMS associés ; et 2. les 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 son ou ses plans de rétablissement documentés, qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-009-6) – 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 notamment des documents qui, collectivement, attestent la mise en œuvre de tous les alinéas applicables du tableau E2 (CIP-009-6) – Mise en œuvre et essais du plan de rétablissement.

Tableau E2 (CIP-009-6) – Mise en œuvre et essais du plan de rétablissement			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et : 1. les EACMS associés ; et 2. les PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et : 1. les EACMS associés ; et 2. les PACS associés.	Tester chacun des plans de rétablissement visés par l'exigence E1 au moins une fois tous les 15 mois civils : • par un rétablissement 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 d'un essai du plan de rétablissement (rétablissement 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 d'un exercice sur papier ou d'un exercice opérationnel complet : avis de réunion, procès-verbaux ou autres documents consignant les résultats des exercices peuvent constituer des pièces justificatives.

Tableau E2 (CIP-009-6) – Mise en œuvre et essais du plan de rétablissement			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.2	*Systèmes électroniques BES* à impact élevé et : 1. les EACMS associés ; et 2. les PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et : 1. les EACMS associés ; et 2. les 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 du test ainsi que les critères de vérification que l'information est utilisable (charger une bande de données, parcourir le contenu de la bande, etc.) et de sa compatibilité avec les configurations courantes des systèmes (points de comparaison manuels ou automatisés entre le contenu des supports de sauvegarde et la configuration courante, etc.).
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 chacun des alinéas applicables du tableau E3 (CIP-009-6) – Examen, mise à jour et communication d'un plan de rétablissement. *[Facteur de risque de la non-conformité : faible] [Horizon : évaluation des activités d'exploitation]*

M3. Les pièces justificatives acceptables doivent notamment attester la conformité à chacun des alinéas applicables du tableau E3 (CIP-009-6) – Examen, mise à jour et communication d'un plan de rétablissement.

Tableau E3 (CIP-009-6) – Examen, mise à jour et communication d'un plan de rétablissement			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes électroniques BES* à impact élevé et : 1. les EACMS associés ; et 2. les PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et : 1. les EACMS associés ; et 2. les 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 de 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 de plan révisé, par exemple : • courriels ; • US Postal Service ou autre service postal ; • système de distribution électronique ; ou

Tableau E3 (CIP-009-6) – Examen, mise à jour et communication d'un plan de rétablissement			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
			• feuilles de présence aux formations.
3.2	*Systèmes électroniques BES* à impact élevé et : 1. les EACMS associés ; et 2. les PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et : 1. les EACMS associés ; et 2. les 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 des mesures pour assurer la conformité

Selon la définition des règles de procédure de la NERC, le terme « *responsable de la surveillance de l'application des normes* » (CEA) désigne la NERC ou l'entité régionale dans leurs rôles respectifs de surveillance de la conformité aux normes de fiabilité de la NERC.

1.2. Conservation des pièces justificatives

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

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

- Chaque entité 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 de mise en application des normes

Audits de conformité

Déclarations sur la conformité

Contrôles ponctuels

Enquêtes de conformité

Déclarations de non-conformité

Plaintes

1.4. Autres informations sur la conformité

Aucune.

2. Tableau des éléments de conformité

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1	**Planification à long terme**	**Moyen**	Sans objet	L'entité responsable a créé un ou des plans de rétablissement, mais en omettant une des exigences des alinéas 1.2 à 1.5.	L'entité responsable a créé un ou des plans de rétablissement, mais en omettant deux des exigences des alinéas 1.2 à 1.5.	L'entité responsable n'a pas créé de 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 en omettant les conditions de déclenchement de l'alinéa 1.1. OU L'entité responsable a créé un ou des plans de rétablissement pour les *systèmes électroniques BES*, mais en omettant au moins trois des exigences des alinéas 1.2 à 1.5.
E2	**Planification de l'exploitation** **Exploitation en temps réel**	**Faible**	L'entité responsable a testé le ou les plans de rétablissement conformément à l'alinéa 2.1 (E2) dans un intervalle de plus de 15 mois civils et d'au plus 16 mois civils	L'entité responsable a testé le ou les plans de rétablissement conformément à l'alinéa 2.1 (E2) dans un intervalle de plus de 16 mois civils et d'au plus 17 mois civils	L'entité responsable a testé le ou les plans de rétablissement conformément à l'alinéa 2.1 (E2) dans un intervalle de plus de 17 mois civils et d'au plus 18 mois civils	L'entité responsable n'a pas testé le ou les plans de rétablissement conformément à l'alinéa 2.1 (E2) dans un intervalle de 18 mois civils entre les tests. (2.1)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			entre les tests. (2.1) 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 l'alinée 2.2 (E2) dans un intervalle de plus de 15 mois civils et d'au plus 16 mois civils entre les tests. (2.2) OU L'entité responsable a testé le plan de rétablissement conformément à l'alinéa 2.3 (E2) dans un intervalle de plus de 36 mois civils et d'au plus 37 mois civils entre les tests. (2.3)	entre les tests. (2.1) 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 l'alinéa 2.2 (E2) dans un intervalle de plus de 16 mois civils et d'au plus 17 mois civils entre les tests. (2.2) OU L'entité responsable a testé le plan de rétablissement conformément à l'alinéa 2.3 (E2) dans un intervalle de plus de 37 mois civils et d'au plus 38 mois civils entre les tests. (2.3)	entre les tests. (2.1) 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 l'alinéa 2.2 (E2) dans un intervalle de plus de 17 mois civils et d'au plus 18 mois civils entre les tests. (2.2) OU L'entité responsable a testé le plan de rétablissement conformément à l'alinéa 2.3 (E2) dans un intervalle de plus de 38 mois civils et d'au plus 39 mois civils entre les tests. (2.3)	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 l'alinéa 2.2 (E2) dans un intervalle de 18 mois civils entre les tests. (2.2) OU L'entité responsable n'a pas testé le ou les plans de rétablissement conformément à l'alinéa 2.3 (E2) dans un intervalle de 39 mois civils entre les tests. (2.3)
E3	**Évaluation des activités d'exploitation**	**Faible**	L'entité responsable a avisé chaque personne ou groupe jouant un rôle défini dans le ou les plans de rétablissement des mises à jour dans un délai de plus de 90 jours civils et de moins de 120 jours civils suivants la réalisation	L'entité responsable a mis à jour le ou les plans de rétablissement en tenant compte de toutes les leçons apprises documentées dans un délai de plus de 90 jours civils et de moins de 120 jours civils suivants chaque test de plan de	L'entité responsable a documenté les leçons apprises ou leur absence dans un délai de plus de 90 jours civils et de moins de 120 jours civils suivant chaque test de plan de rétablissement ou rétablissement réel. (3.1.1)	L'entité responsable n'a documenté ni les leçons apprises ni leur absence dans un délai de 120 jours civils suivant chaque test de plan de rétablissement ou rétablissement réel. (3.1.1)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			complète de la mise à jour. (3.1.3)	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 dans un délai de 120 jours civils suivant la réalisation complète de la mise à jour. (3.1.3) OU L'entité responsable a mis à jour le ou les plans de rétablissement et avisé chaque personne ou groupe jouant un rôle défini dans un délai de plus de 60 jours civils et de moins de 90 jours civils suivants un des changements ci-après que l'entité responsable juge susceptible d'avoir un impact sur la capacité d'exécuter le plan : (3.2) • rôles et responsabilités • intervenants, ou • changements	OU L'entité responsable n'a pas mis à jour le ou les plans de rétablissement en tenant compte de toutes les leçons apprises documentées dans un délai de 120 jours civils suivant chaque test de plan de rétablissement ou rétablissement réel. (3.1.2) 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 dans un délai de 90 jours civils suivants un des changements ci-après que l'entité responsable juge susceptible d'avoir un impact sur la capacité d'exécuter le plan : (3.2) • rôles et responsabilités • intervenants, ou • changements technologiques.	

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-6)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				technologiques.		

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

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.	
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.	Modification en coordination avec les autres normes CIP et révision du format selon le modèle RBS.
5	22 novembre 2013	Ordonnance de la FERC approuvant la norme CIP-009-5.	
6	13 novembre 2014	Adoption par le Conseil d'administration de la NERC.	Mise en œuvre de prescriptions de l'ordonnance 791.
6	21 janvier 2016	Ordonnance de la FERC émise approuvant CIP-003-6. Dossier no. RM15-14-000	

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) présente 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, les normes CIP sur la cybersécurité de la NERC s'y appliquent. Il est à noter qu'en ce qui concerne les *distributeurs*, la section 4.1 limite l'applicabilité 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 qui, selon la section 4.1, est visée par les exigences de la norme. Comme il est indiqué à la section d'exemption 4.2.3.5, la présente norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou moyen selon la catégorisation de la norme CIP-002-5.1. 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* » dans le glossaire de la NERC indique déjà qu'il s'agit d'*éléments* du *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 aide à clarifier 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*. Septembre 2011. En ligne à l'adresse suivante : 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. Mai 2010. En ligne à l'adresse suivante : 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 de fiabilité 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 (estimation d'état, contingences et : http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_RBR_ROP_10152015_RR15-4.pdf

mesures correctives, gestion prévisionnelle des retraits, etc.). Un seul plan de rétablissement de *systèmes électroniques BES* devrait être suffisant pour plusieurs installations similaires, comme celles qu'on trouve dans les postes électriques ou les centrales.

Selon l'alinéa 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.

Selon l'alinéa 1.2, les entités doivent désigner les personnes chargées des mesures de rétablissement du *système électronique BES* visé.

Selon l'alinéa 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.

Selon l'alinéa 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. Cet alinéa de l'exigence n'impose pas l'exécution 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.

Selon l'alinéa 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* constitue la cause du 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 individuellement. Les *systèmes électroniques BES* qui sont répartis et en grand nombre, comme ceux qu'on trouve 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 faire en sorte que le plan soit 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 (bureaux locaux conjoints, centres des opérations d'urgence, etc.) et sur le terrain (pompiers décontaminant des mannequins, etc.). »

Selon l'alinéa 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 l'alinéa 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 l'alinéa 1.3. Cet essai doit comprendre les étapes nécessaires pour s'assurer que l'information est à la fois utilisable et à jour. 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 alinéas de cette 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.

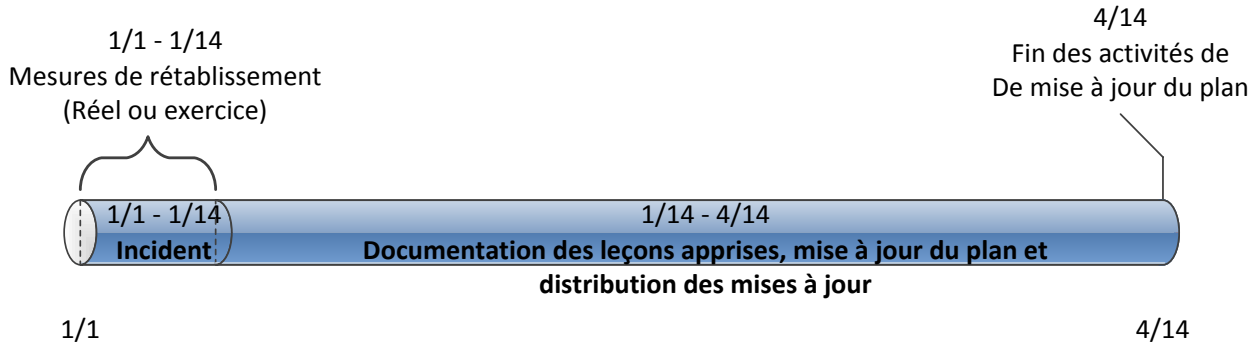


Figure 1 : Calendrier pour l'exigence E3 de la norme CIP-009-6

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.

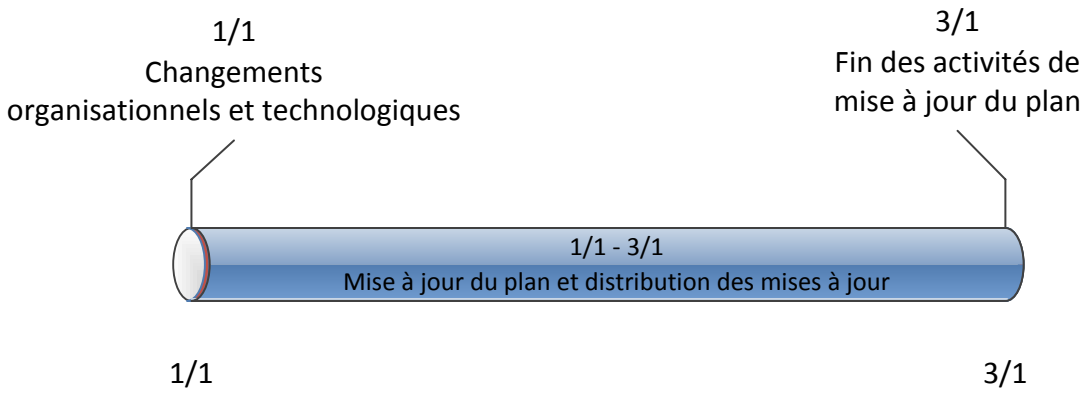


Figure 2 : Calendrier pour les changements au plan de l'alinéa 3.2.

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 cryptées.

Justification

Pendant l'élaboration de cette norme, des zones de texte ont été incorporées à celle-ci pour exposer la justification de ses diverses parties. Après l'approbation par le Conseil d'administration, le contenu de ces zones de texte a été transféré ci-après.

Justification de l'exigence 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.

Justification de l'exigence E2

La mise en œuvre d'un plan de rétablissement efficace réduit les risques posés au 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.

L'alinéa 2.2 de cette exigence offre une assurance supplémentaire quant à l'information (bandes de sauvegarde, centres miroirs, 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 échantillon qui offre l'assurance que l'information est utilisable.

Justification de l'exigence 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, selon l'alinéa 3.1, et ii) réviser le plan, selon l'alinéa 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 celui-ci nécessite des modifications.

Annexe QC-CIP-009-6
Dispositions particulières de la norme CIP-009-6 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-009-6

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

   4.1. Entités fonctionnelles

   4.2. Installations

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

   Exemptions additionnelles

   Sont exemptés de l'application de la présente norme :

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

5. **Date d'entrée en vigueur 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 :

Annexe QC-CIP-009-6
Dispositions particulières de la norme CIP-009-6 applicables au Québec

Norme	Révision CIPv6	Date d'entrée en vigueur proposée au Québec		
		Entités visées par la version 1 des normes CIP adoptées par la Régie	Entités ne possédant pas d'installations de production à vocation industrielle et non visées par la version 1 des normes CIP	Entités qui possèdent des installations de production à vocation industrielle
CIP-009-6	Élimination de la formulation « détecter, évaluer et corriger » car elle est vague et sujette à de multiples interprétations	2017-10-01	2018-10-01	2019-04-01

6. Contexte :

Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et de mise en application des normes

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

Justification

Aucune disposition particulière

Historique des versions

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-010-2

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 *système de production-transport d'électricité* (*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* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale ; et

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

4.1.2.2 Chaque *automatisme de réseau (SPS)* ou *plan de défense (RAS)* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

4.1.2.3 Chaque *système de protection* applicable au *transport* (à l'exclusion des systèmes DSF et DST) 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 prochains groupes de production à démarrer.

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

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

4.1.5 ***Coordonnateur des échanges*** **ou** ***responsable des échanges***

4.1.6 ***Coordonnateur de la fiabilité***

4.1.7 ***Exploitant de réseau de transport***

4.1.8 ***Propriétaire d'installation de transport***

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

4.2.1 **Distributeur** : Un ou plusieurs des *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* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale ; et

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

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

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

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

4.2.2 **Entités responsables indiquées en 4.1, sauf les *distributeurs*** :

Toutes les *installations* du *BES*.

4.2.3 **Exemptions :** Sont exemptés de la norme CIP-010-2 :

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 composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme au règlement CFR 10, section 73.54 ;

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

4.2.3.5 les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* classés dans les catégories « impact élevé » ou « impact moyen » selon le processus de désignation et de catégorisation de la norme CIP-002-5.1.

5. Dates de mise en vigueur

Voir le plan de mise en œuvre de la norme CIP-010-2.

6. Contexte :

La norme CIP-010 fait partie d'une série de normes CIP sur la cybersécurité qui exigent la détermination et la catégorisation initiales des *systèmes électroniques BES*. Ces normes exigent aussi un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.

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

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité doit inclure tout ce qu'elle juge nécessaire dans ses processus documentés, en s'assurant de bien couvrir les exigences pertinentes.

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

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

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

Les mesures auxquelles renvoie l'énoncé initial de l'exigence correspondent simplement aux processus documentés eux-mêmes. La colonne « Mesures » présente des exemples de pièces justificatives attestant la documentation et la mise en œuvre des éléments pertinents dans les processus documentés ; ces exemples sont présentés à titre indicatif, et leur liste ne doit pas être considérée comme exhaustive.

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

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes 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 *BES*. Un examen des tolérances des 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. La SDT (équipe de rédaction) CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- ***Systèmes électroniques BES* à impact élevé –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.
- ***Systèmes électroniques BES* à impact moyen –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.
- ***Systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*) –** Désigne tout *système de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d'authentification et systèmes de surveillance de registre d'événements et d'alerte.
- ***Systèmes de contrôle des accès physiques* (*PACS*) –** Désigne tout *système de contrôle des accès physique*s associés 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 un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-010-2) – 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, couvrent tous les alinéas applicables du tableau E1 (CIP-010-2) – Gestion des changements de configuration ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-010-2) – Gestion des changements de configuration

Alinéa	Systèmes visés	Exigences	Mesures
1.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Établir une configuration de référence, individuellement ou par groupe, qui doit comprendre les points suivants : 1.1.1. système ou systèmes 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. tout correctif 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.
1.2	*Systèmes électroniques BES* à impact	Autoriser et documenter tout	Exemples non limitatifs de pièces

Tableau E1 (CIP-010-2) – Gestion des changements de configuration			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
	élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	changement par rapport à la configuration de référence existante.	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 : 1. les *EACMS* associés ; 2. les *PACS* associés ; et les *PCA* associés.*Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *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.
1.4	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Pour tout changement par rapport à la configuration de référence existante : 1.4.1. avant le changement, déterminer les mécanismes de cybersécurité des normes CIP-005 et CIP-007	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-010-2) – Gestion des changements de configuration			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
	Systèmes électroniques BES à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	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.	
1.5	*Systèmes électroniques BES* à impact élevé.	Si cela est 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 des normes CIP-005 et CIP-007 ne sont pas dégradés ; et 1.5.2. documenter les résultats des	Exemples non limitatifs de pièces justificatives : 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.

Tableau E1 (CIP-010-2) – Gestion des changements de configuration			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
		essais et, si un environnement d'essai a été 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.	

E2. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-010-2) – Surveillance de la 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, couvrent tous les alinéas applicables du tableau E2 (CIP-010-2) – Surveillance de la configuration ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-010-2) – Surveillance de la configuration			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PCA* associés.	Au moins une fois tous les 35 jours civils, vérifier s'il y a eu des changements dans la configuration de référence (décrite à l'alinéa 1.1 de l'exigence E1). 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, couvrent tous les alinéas applicables du tableau E3 (CIP-010-2) – 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, couvrent tous les alinéas applicables du tableau E3 (CIP-010-2) – Analyses de vulnérabilité ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E3 (CIP-010-2) – Analyses de vulnérabilité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *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-010-2) – Analyses de vulnérabilité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*Systèmes électroniques BES* à impact élevé.	Si cela est 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 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.	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-010-2) – Analyses de vulnérabilité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.3	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *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 : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Documenter les résultats des analyses effectuées conformément aux alinéas 3.1, 3.2 et 3.3 ainsi que le plan d'action visant à corriger ou à atténuer les vulnérabilités constatées 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 d'ordres de travail, suivi des mesures au moyen d'une feuille de calcul, etc.).

E4. Chaque entité responsable, pour ses *systèmes électroniques BES* à impact moyen et élevé ainsi que les *actifs électroniques* protégés connexes, doit mettre en œuvre (sauf dans des *circonstances CIP exceptionnelles*) un ou plusieurs plans documentés concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles* ; ces plans doivent être conformes aux sections de l'annexe 1.
[Facteur de risque de la non-conformité : moyen] [Horizon : planification à long terme et planification de l'exploitation]

M4. Les pièces justificatives doivent comprendre chacun des plans documentés qui concernent les *actifs électroniques temporaires* et les *supports de stockage amovibles* et qui, collectivement, couvrent toutes les sections applicables de l'annexe 1 ; d'autres pièces justificatives doivent attester la mise en œuvre de ces plans. D'autres exemples de pièces justificatives pour les différentes sections sont présentés à l'annexe 2. Si une entité responsable n'utilise pas d'*actifs électroniques temporaires* ni de *supports de stockage amovibles*, les pièces justificatives appropriées peuvent comprendre, sans limitation, une déclaration, une politique ou tout autre document affirmant que l'entité responsable n'utilise pas d'*actifs électroniques temporaires* ou de *supports de stockage amovibles.*

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Selon la définition des règles de procédure de la NERC, le terme « responsable des mesures pour assurer la conformité » (CEA) désigne la NERC ou l'entité régionale dans leurs rôles respectifs de surveillance de la conformité aux normes de fiabilité de la NERC.

1.2. Conservation des pièces justificatives

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

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

- Chaque entité 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 de mise en application des normes

Audits de conformité

Déclarations sur la conformité

Contrôles ponctuels

Enquêtes de conformité

Déclarations de non-conformité

Plaintes

1.4. Autres informations sur la conformité

Aucune.

2. Tableau des éléments de conformité

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-2)			
			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 comprennent seulement quatre des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1)	L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprennent seulement trois des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1)	L'entité responsable a documenté et mis en œuvre un ou des processus de gestion des changements de configuration qui comprennent seulement deux des éléments de référence exigés en 1.1.1 à 1.1.5. (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 comprennent seulement un des éléments de référence exigés en 1.1.1 à 1.1.5. (1.1) OU L'entité responsable n'a pas de processus qui exige l'autorisation et la documentation des changements par

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-2)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						rapport à la configuration de référence existante. (1.2) OU L'entité responsable n'a pas de 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 n'a pas de processus pour déterminer les mécanismes de sécurité requis dans les normes CIP-005 et CIP-007 qui pourraient être touchés par des

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-2)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						changements par rapport à la configuration de référence existante. (1.4.1) OU L'entité responsable a un ou des processus pour déterminer les mécanismes de sécurité requis dans les normes CIP-005 et CIP-007 qui pourraient être touchés par 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 dégradés par suite du changement. (1.4.2 et 1.4.3) OU

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-2)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						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 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 a été utilisé, pour documenter les différences entre les environnements d'essai et de production. (1.5.2)
E2	**Planification de**	**Moyen**	Sans objet	Sans objet	Sans objet	L'entité responsable n'a pas documenté ou

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-2)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
	l'exploitation					mis en œuvre de processus pour vérifier, au moins une fois tous les 35 jours civils, s'il y a eu des changements non autorisés dans la configuration de référence, pour documenter ceux-ci et pour faire enquête. (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 dans un délai de plus de 15 mois et de moins de 18 mois suivant la dernière analyse de l'un de ses *systèmes électroniques BES* visés.	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 dans un délai de plus de 18 mois et de moins de 21 mois suivant la dernière analyse de l'un de ses *systèmes électroniques BES* visés.	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 dans un délai de plus de 21 mois et de moins de 24 mois suivant la dernière analyse de l'un de ses *systèmes électroniques BES* visés.	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*

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-2)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			(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 dans un délai de plus de 36 mois et de moins de 39 mois suivants la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2)	(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 dans un délai de plus de 39 mois et de moins de 42 mois suivants la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2)	(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 dans un délai de plus de 42 mois et de moins de 45 mois suivants la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2)	*électroniques BES* visés, mais elle a effectué une analyse de vulnérabilité plus 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 documentés d'analyse de vulnérabilité active pour les systèmes visés, mais elle a effectué une analyse de vulnérabilité active dans un délai de plus de 45 mois suivants la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2) OU

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-2)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						L'entité responsable a mis en œuvre et documenté un ou plusieurs processus d'analyse de vulnérabilité pour 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

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-2)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
						documenté les résultats des analyses de vulnérabilité, les plans d'action pour corriger ou atténuer les vulnérabilités constatées dans les analyses, la date planifiée d'achèvement du plan d'action et l'état d'exécution des plans d'atténuation. (3.4)
E4	**Planification à long terme et planification de l'exploitation**	**Moyen**	L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas géré ses *actifs électroniques temporaires* conformément à la section 1.1 de l'annexe 1 complémentaire à	L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en œuvre les mesures applicables aux *supports de stockage amovibles* conformément à la section 3 de l'annexe 1 complémentaire à	L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas établi les autorisations relatives aux *actifs électroniques temporaires* conformément à la section 1.2 de l'annexe 1	L'entité responsable n'a pas documenté ou mis en œuvre un ou plusieurs plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles* conformément à l'exigence E4 de la norme CIP-010-2. (E4)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-2)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			l'exigence E4 de la norme CIP-010-2. (E4) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas documenté les mesures applicables aux *supports de stockage amovibles* conformément à la section 3 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-2. (E4) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage*	l'exigence E4 de la norme CIP-010-2. (E4) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas documenté les mesures d'atténuation du risque lié aux vulnérabilités logicielles, à l'introduction de programmes malveillants ou aux utilisations non autorisées pour des *actifs électroniques temporaires* gérés par l'entité responsable conformément aux sections 1.3, 1.4 et 1.5 de l'annexe 1	complémentaire à l'exigence E4 de la norme CIP-010-2. (E4) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en œuvre les mesures d'atténuation du risque lié aux vulnérabilités logicielles, à l'introduction de programmes malveillants ou aux utilisations non autorisées pour des *actifs électroniques temporaires* gérés par l'entité responsable conformément aux sections 1.3, 1.4 et 1.5	

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-2)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
			amovibles, mais n'a pas documenté les autorisations relatives aux *actifs électroniques temporaires* qu'elle gère elle-même conformément à la section 1.2 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-2. (E4)	complémentaire à l'exigence E4 de la norme CIP-010-2. (E4) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas documenté les mesures d'atténuation du risque lié aux vulnérabilités logicielles ou à l'introduction de programmes malveillants pour des *actifs électroniques temporaires* gérés par une tierce partie conformément aux sections 2.1, 2.2 et 2.3 de l'annexe 1 complémentaire à l'exigence E4 de la	de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-2. (E4) OU L'entité responsable a documenté son ou ses plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*, mais n'a pas mis en œuvre les mesures d'atténuation du risque lié aux vulnérabilités logicielles ou à l'introduction de programmes malveillants pour des *actifs électroniques temporaires* gérés par une tierce partie conformément aux sections 2.1, 2.2 et 2.3 de l'annexe 1 complémentaire à	

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-010-2)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				norme CIP-010-2. (E4)	l'exigence E4 de la norme CIP-010-2. (E4)	

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Principes directeurs et fondements techniques (ci-après).

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	Ordonnance de la FERC approuvant la norme CIP-010-1. (L'ordonnance entre en vigueur le 3 février 2014.)	
2	13 novembre 2014	Adoption par le Conseil d'administration de la NERC.	Mise en œuvre de deux prescriptions de l'ordonnance 791 de la FERC concernant l'obligation de « détecter, évaluer et corriger » ainsi que les réseaux de communication.
2	12 février 2015	Adoption par le Conseil d'administration de la NERC.	Remplace la version adoptée par le Conseil le 13 novembre 2014. La version à jour met en œuvre des prescriptions en instance de l'ordonnance 791 relativement aux actifs temporaires et aux systèmes électroniques BES à impact faible.
6	21 janvier 2016	Ordonnance de la FERC émise approuvant CIP-003-6. Dossier no. RM15-14-000	

CIP-010-2 – Annexe 1

Exigences détaillées des plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*

Les entités responsables doivent intégrer chacune des sections suivantes à leurs plans, prescrits à l'exigence E4, concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*.

Section 1. *Actifs électroniques temporaires* gérés par l'entité responsable.

1.1. Gestion des *actifs électroniques temporaires* : Les entités responsables doivent gérer leurs *actifs électroniques temporaires*, individuellement ou par groupe : 1) en permanence, afin d'assurer la conformité aux exigences pertinentes en tout temps ; 2) à la demande, en appliquant les exigences pertinentes avant d'établir la connexion à un système électronique BES ; ou 3) selon une combinaison des moyens 1) et 2) ci-dessus.

1.2. Autorisations relatives aux *actifs électroniques temporaires* : Pour chaque *actif électronique temporaire* ou groupe d'*actifs électroniques temporaires*, chaque entité responsable doit autoriser :

1.2.1. les utilisateurs (individuellement, par groupe ou par rôle) ;

1.2.2. les emplacements (individuellement ou par groupe) ; et

1.2.3. les utilisations, qui doivent être limitées aux actions nécessaires pour assurer les fonctions opérationnelles.

1.3. Atténuation du risque lié aux vulnérabilités logicielles : Utiliser un ou plusieurs des moyens suivants pour réaliser l'objectif d'atténuer le risque lié aux vulnérabilités présentées par des logiciels sans correctifs dans l'*actif électronique temporaire* (selon les capacités de ce dernier) :

- application de correctifs, manuellement ou par mises à jour systématiques ;
- systèmes d'exploitation et logiciels exécutables uniquement à partir de supports non inscriptibles ;
- renforcement du système d'exploitation ; ou
- autres moyens d'atténuer le risque lié aux vulnérabilités logicielles.

1.4. Atténuation du risque lié à l'introduction de programmes malveillants : Utiliser un ou plusieurs des moyens suivants pour réaliser l'objectif d'atténuer le risque lié à l'introduction de programmes malveillants (selon les capacités de l'*actif électronique temporaire*) :

- logiciel antivirus, avec mises à jour manuelles ou systématiques des signatures ou des séquences de code ;
- liste blanche d'applications ; ou

- autres moyens d'atténuer le risque lié à l'introduction de programmes malveillants.

1.5. Atténuation du risque lié aux utilisations non autorisées : Utiliser un ou plusieurs des moyens suivants pour réaliser l'objectif d'atténuer le risque lié aux utilisations non autorisées d'*actifs électroniques temporaires* :

- restriction de l'accès physique ;
- cryptage de disque intégral avec authentification ;
- authentification multifactorielle ; ou
- autres moyens d'atténuer le risque lié aux utilisations non autorisées.

Section 2. *Actifs électroniques temporaires* gérés par une tierce partie autre que l'entité responsable.

2.1 Atténuation du risque lié aux vulnérabilités logicielles : Utiliser un ou plusieurs des moyens suivants pour réaliser l'objectif d'atténuer le risque lié aux vulnérabilités présentées par les logiciels sans correctifs dans l'*actif électronique temporaire* (selon les capacités de ce dernier) :

- examen des correctifs de sécurité installés ;
- examen de la procédure d'application des correctifs par la tierce partie ;
- examen d'autres mesures d'atténuation du risque lié aux vulnérabilités logicielles adoptées par la tierce partie ; ou
- autres moyens d'atténuer le risque lié aux vulnérabilités logicielles.

2.2 Atténuation du risque lié à l'introduction de programmes malveillants : Utiliser un ou plusieurs des moyens suivants pour réaliser l'objectif d'atténuer le risque lié à l'introduction programmes malveillants (selon les capacités de l'actif électronique temporaire) :

- examen du degré de maintien à jour de l'antivirus ;
- examen de la procédure de mise à jour de l'antivirus adoptée par la tierce partie ;
- examen de l'utilisation par la tierce partie de listes blanches d'applications ;
- examen de l'utilisation de systèmes d'exploitation et de logiciels exécutables uniquement à partir de supports non inscriptibles ;
- examen des mesures de renforcement du système d'exploitation adoptées par la tierce partie ; ou
- autres moyens d'atténuation du risque lié aux programmes malveillants.

2.3 Pour tout moyen d'atténuation du risque lié aux vulnérabilités logicielles ou à l'introduction de programmes malveillants mis en œuvre conformément aux

alinéas 2.1 et 2.2, l'entité responsable doit déterminer si d'autres mesures d'atténuation sont nécessaires et appliquer ces mesures avant de connecter l'*actif électronique temporaire*.

Section 3. *Supports de stockage amovibles*

3.1. Autorisations relatives aux *supports de stockage amovibles* : Pour chaque *support d'information amovible* ou groupe de *supports de stockage amovibles*, chaque entité responsable doit autoriser :

3.1.1. les utilisateurs (individuellement, par groupe ou par rôle) ; et

3.1.2. les emplacements (individuellement ou par groupe).

3.2. Atténuation du risque lié aux programmes malveillants : Afin de réaliser l'objectif d'atténuer le risque lié à l'introduction de programmes malveillants dans des *systèmes électroniques BES* à impact élevé ou moyen et dans les *actifs électroniques protégés* connexes, chaque entité responsable doit :

3.2.1. prendre des mesures pour détecter les programmes malveillants sur les *supports de stockage amovibles* au moyen d'un *actif électronique* autre qu'un *système électronique BES* ou que des *actifs électroniques protégés* ; et

3.2.2. neutraliser la menace de programmes malveillants détectés sur des *supports de stockage amovibles* avant de connecter ces supports à un *système électronique BES* à impact moyen ou élevé ou à des *actifs électroniques protégés* connexes.

CIP-010-2 – Annexe 2

Exemples de pièces justificatives pour les plans concernant les *actifs électroniques temporaires* et les *supports de stockage amovibles*

Section 1.1 : Exemples non limitatifs de pièces justificatives pour la section 1.1 : méthodes de gestion des *actifs électroniques temporaires*. Cette information peut faire partie des plans concernant les *actifs électroniques temporaires*, de la documentation concernant les autorisations relatives aux *actifs électroniques temporaires* gérés par l'entité responsable, ou encore d'une politique de sécurité.

Section 1.2 : Exemples non limitatifs de pièces justificatives pour la section 1.2 : documentation de systèmes de gestion des actifs ou de gestion des ressources humaines, ou formulaires ou feuilles de chiffrier indiquant les autorisations relatives aux *actifs électroniques temporaires* gérés par l'entité responsable. Cette information peut aussi être documentée dans le document principal du plan.

Section 1.3 : Exemples non limitatifs de pièces justificatives pour la section 1.3 : documentation des moyens utilisés pour atténuer le risque lié aux vulnérabilités présentées par les logiciels sans correctifs, comme la gestion des correctifs de sécurité, l'utilisation de systèmes d'exploitation sur support non inscriptible, le renforcement du système d'exploitation ou d'autres moyens d'atténuation appropriés. Les pièces justificatives peuvent provenir de systèmes de gestion des changements, de solutions de gestion systématique des correctifs, de procédures ou processus concernant l'utilisation de systèmes d'exploitation sur support amovible, ou de procédures ou processus associés aux pratiques de renforcement du système d'exploitation. Si un *actif électronique temporaire* n'a pas la capacité de mettre en œuvre certains moyens d'atténuation du risque lié aux vulnérabilités présentées par les logiciels sans correctifs, les pièces justificatives peuvent comprendre une documentation du fournisseur ou de l'entité responsable indiquant que l'*actif électronique temporaire* n'a pas cette capacité.

Section 1.4 : Exemples non limitatifs de pièces justificatives pour la section 1.4 : documentation des moyens utilisés pour atténuer le risque lié à l'introduction de programmes malveillants, comme des logiciels antivirus et des processus de gestion des mises à jour des signatures ou des séquences de code, des pratiques de liste blanche d'applications, des processus de restriction des communications ou d'autres moyens d'atténuation appropriés. Si un *actif électronique temporaire* n'a pas la capacité de mettre en œuvre certains moyens d'atténuation du risque lié à l'introduction de programmes malveillants, les pièces justificatives peuvent comprendre une documentation du fournisseur ou de l'entité responsable indiquant que l'*actif électronique temporaire* n'a pas cette capacité.

Section 1.5 : Exemples non limitatifs de pièces justificatives pour la section 1.5 : documentation (politiques ou procédures) des moyens de restriction des accès physiques ; description de la solution de cryptage de disque intégral et du protocole d'authentification ; description de la solution d'authentification multifactorielle ; ou documentation d'autres moyens d'atténuer le risque lié aux utilisations non autorisées.

Section 2.1 : Exemples non limitatifs de pièces justificatives pour la section 2.1 : documentation de systèmes de gestion des changements, courriels ou procédures qui documentent un examen des correctifs de sécurité installées ; notes de service, courriels, politiques ou contrats d'une tierce partie autre que l'entité responsable qui décrivent le processus d'application de correctifs ou d'atténuation du risque lié aux vulnérabilités exécuté par la tierce partie ; pièces justificatives de systèmes de gestion des changements, courriels, documentation de système ou contrats indiquant que l'entité responsable juge acceptables les pratiques de la tierce partie ; ou documentation d'autres moyens d'atténuation du risque lié aux vulnérabilités logicielles d'*actifs électroniques temporaires* gérés par la tierce partie. Si un *actif électronique temporaire* n'a pas la capacité de mettre en œuvre certains moyens d'atténuation du risque lié aux vulnérabilités présentées par les logiciels sans correctifs, les pièces justificatives peuvent comprendre une documentation de l'entité responsable ou de la tierce partie indiquant que l'actif électronique temporaire n'a pas cette capacité.

Section 2.2 : Exemples non limitatifs de pièces justificatives pour la section 2.2 : documentation de systèmes de gestion des changements, courriels ou procédures qui documentent un examen du degré de maintien à jour des antivirus installés ; notes de service, courriels, documentation de système, politiques ou contrats d'une tierce partie autre que l'entité responsable qui décrivent le processus de mise à jour des antivirus, l'utilisation d'une liste blanche d'applications, l'utilisation de systèmes d'exploitation sur support externe ou le renforcement du système d'exploitation par la tierce partie ; pièces justificatives de systèmes de gestion des changements, courriels ou contrats indiquant que l'entité responsable juge acceptables les pratiques de la tierce partie ; ou documentation d'autres moyens d'atténuation du risque lié à l'introduction de programmes malveillants pour les *actifs électroniques temporaires* gérés par la tierce partie. Si un *actif électronique temporaire* n'a pas la capacité de mettre en œuvre certains moyens d'atténuation du risque lié à l'introduction de programmes malveillants, les pièces justificatives peuvent comprendre une documentation de l'entité responsable ou de la tierce partie indiquant que l'*actif électronique temporaire* n'a pas cette capacité.

Section 2.3 : Exemples non limitatifs de pièces justificatives pour la section 2.3 : documentation de systèmes de gestion des changements, courriels ou contrats attestant qu'un examen a été effectué pour déterminer le besoin de

mesures d'atténuation supplémentaires, et que ces mesures ont été mises en œuvre avant la connexion de l'*actif électronique temporaire* géré par une tierce partie autre que l'entité responsable.

Section 3.1 : Exemples non limitatifs de pièces justificatives pour la section 3.1 : documentation de systèmes de gestion des actifs ou de gestion des ressources humaines, formulaires ou feuilles de chiffrier indiquant les autorisations relatives aux *supports de stockage amovibles*. La documentation doit désigner les *supports de stockage amovibles* (individuellement ou par groupe), les utilisateurs autorisés (individuellement, par groupe ou par rôle) et les emplacements autorisés (individuellement ou par groupe).

Section 3.2 : Exemples non limitatifs de pièces justificatives pour la section 3.2 : processus documentés des moyens d'atténuation du risque lié aux programmes malveillants, comme les résultats de balayage paramétré pour les *supports de stockage amovibles* ou la mise en œuvre du balayage à la demande ; processus documentés des moyens d'atténuation du risque lié aux programmes malveillants détectés sur les *supports de stockage amovibles*, comme les journaux créés par les mécanismes de détection qui montrent les résultats du balayage et indiquent la neutralisation des programmes malveillants détectés sur les *supports de stockage amovibles*, ou une confirmation documentée par l'entité que les *supports de stockage amovibles* sont considérés comme exempts de tout programme malveillant.

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) présente 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, les normes CIP sur la cybersécurité de la NERC s'y appliquent. Il est à noter qu'en ce qui concerne les *distributeurs*, la section 4.1 limite l'applicabilité 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 qui, selon la section 4.1, est visée par les exigences de la norme. Comme il est indiqué à la section d'exemption 4.2.3.5, la présente norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou moyen selon la catégorisation de la norme CIP-002-5.1. 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* » dans le glossaire de la NERC indique déjà qu'il s'agit d'*éléments* du *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 aide à clarifier 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 correctifs 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 précisée. 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. La 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 commercial ou distribués à titre de logiciel

libre. 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 commercial 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-007-6. Les ports accessibles doivent être indiqués dans la configuration de référence. Les correctifs de sécurité appliqués doivent comprendre tous les correctifs antérieurs et courants appliqués sur l'actif électronique. Alors que l'alinéa 2.1 de l'exigence E2 de la norme CIP-007-6 stipule que les entités doivent se tenir informées des correctifs de sécurité, les évaluer et les appliquer, l'alinéa 1.1.5 de l'exigence E1 de la norme CIP-010 stipule que les entités doivent consigner tous les correctifs appliqués, antérieurs et courants.

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 – Correctif 12345, Correctif 67890, Correctif 34567 et Correctif 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 alinéas pertinents 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. La 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 correctifs de sécurité concernent seulement l'exigence E2 de la norme CIP-007 (gestion des correctifs de sécurité). La 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. La SDT 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 correctifs 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, la 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 ses 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.

Exigence E4

Comme la plupart des *actifs électroniques BES* et des *systèmes électroniques BES* sont isolés des réseaux externes publics ou non fiables, les *actifs électroniques temporaires* et les *supports de stockage amovibles* se présentent assurément comme un vecteur de cyberattaques. Ceux-ci constituent souvent le seul moyen d'entrée et de sortie des fichiers pour des zones sécurisées dans le cadre d'opérations de maintenance, de surveillance ou de dépannage de systèmes névralgiques. Afin de protéger les *actifs électroniques BES* et les *systèmes électroniques BES*, les entités sont tenues de documenter et de mettre en œuvre un plan de gestion de l'utilisation des *actifs électroniques temporaires* et des *supports de stockage amovibles*. L'élaboration de ce plan amène l'entité responsable à documenter des

processus que son organisation est capable de mettre en œuvre et qui cadrent avec ses processus de gestion des changements.

Les *actifs électroniques temporaires* et les *supports de stockage amovibles* sont des dispositifs connectés temporairement : 1) à un *actif électronique BES*, 2) à un réseau à l'intérieur d'un périmètre de sécurité électronique (ESP) ou 3) à un *actif électronique protégé*. Les *actifs électroniques temporaires* et les *supports de stockage amovibles* n'assurent pas de services liés à la fiabilité du *BES* et ne font pas partie de l'*actif électronique BES* auquel ils sont connectés. Exemples non limitatifs de ces dispositifs connectés temporairement :

- équipements de diagnostic ;
- renifleurs de paquets ;
- équipements de maintenance de *systèmes électroniques BES* ;
- équipements de configuration de *systèmes électroniques BES*; ou
- équipements d'analyse de vulnérabilité.

Les *actifs électroniques temporaires* sont très variés ; ils vont des dispositifs conçus spécialement pour la maintenance d'équipements liés au *BES* à des appareils courants (ordinateurs portatifs ou de bureau, tablettes, etc.) qui peuvent simplement se connecter à des *systèmes électroniques BES* ou exécuter des applications afférentes à ceux-ci et qui sont capables de transmettre du code exécutable. Les *supports de stockage amovibles* visés par cette exigence peuvent être des disquettes, des cédéroms, des clés USB, des disques durs externes et des cartes ou lecteurs à mémoire flash (non volatile).

Bien que les définitions d'*actif électronique temporaire* et de *support d'information amovible* comprennent une condition qui limite à 30 jours leur durée de connexion, la section 1.1 de l'annexe 1 permet à l'entité responsable d'incorporer à son plan des traitements appliqués en permanence ou à la demande ainsi que des mesures indépendantes de l'état de connexion ou de déconnexion. Il est à noter qu'un traitement à la demande n'est à appliquer que lorsqu'on s'apprête à connecter l'*actif électronique temporaire* ou le *support d'information amovible* à un *système électronique BES* ou à un *actif électronique protégé* ; une fois l'*actif électronique temporaire* ou le *support d'information amovible* déconnecté, les exigences présentées ici cessent de s'appliquer tant qu'on ne s'apprête pas de nouveau à le connecter à l'*actif électronique BES* ou à l'*actif électronique protégé*.

L'annexe vise à spécifier les ressources et les moyens de sécurité auxquels peuvent avoir recours les entités responsables d'après le type d'un actif, son propriétaire et l'entité ou la partie qui le gère.

À partir de la liste d'options présentée à l'annexe 1 pour chacun des thèmes de cybersécurité, l'entité responsable est libre de choisir le ou les moyens qui lui conviennent le mieux. L'entité responsable est invitée à documenter comment et quand elle entend gérer les *actifs électroniques temporaires* sous son contrôle ou examiner ceux placés sous le contrôle d'autres entités. L'entité responsable doit éviter de mettre en place des fonctions de sécurité susceptibles d'affaiblir la fiabilité du réseau en agissant d'une manière qui nuirait au

fonctionnement ou au soutien d'*actifs électroniques temporaires*, d'*actifs électroniques BES* ou d'*actifs électroniques protégés*.

Atténuation du risque lié aux vulnérabilités

Des expressions comme « atténuer le risque » ou « atténuation du risque » sont utilisées dans les sections de l'annexe 1 à l'endroit des risques présentés par les programmes malveillants, les vulnérabilités logicielles et les utilisations non autorisées lorsqu'il s'agit de connecter des *actifs électroniques temporaires* et des *supports de stockage amovibles*. Le choix du mot « atténuer » ou « atténuation » laisse entendre qu'il n'est pas exigé de parer à chacune des vulnérabilités possibles, car beaucoup d'entre elles peuvent être inconnues ou ne pas avoir d'effet sur le système auquel l'*actif électronique temporaire* ou *le support d'information amovible* est connecté. L'exigence d'atténuation consiste à réduire les risques pour la sécurité associés à la connexion de l'*actif électronique temporaire*.

Prise en compte des capacités de l'*actif électronique temporaire*

Comme dans d'autres normes CIP, les moyens à utiliser par l'entité se limitent à ceux que le système est capable de mettre en œuvre. L'expression « selon les capacités de l'*actif électronique temporaire* » sert à éviter le recours à une exception pour raison technique (TFE) lorsqu'il est évident que certains moyens ne sont pas utilisables avec tel ou tel dispositif. Par exemple, dans le cas des programmes malveillants, bien des types de dispositifs n'ont pas la capacité de faire fonctionner un logiciel antivirus ; par conséquent, la mise en œuvre d'un logiciel antivirus ne serait pas exigée pour ces dispositifs.

Exigence E4, section 1 de l'annexe 1 – *Actifs électroniques temporaires* gérés par l'entité responsable

Section 1.1 – Les entités exercent un degré de contrôle élevé sur les actifs qu'elles gèrent elles-mêmes. Les exigences présentées ici donnent aux entités la souplesse de préautoriser un ensemble de dispositifs, d'autoriser les dispositifs au moment de leur connexion, ou encore de combiner ces deux méthodes. Les dispositifs peuvent être gérés individuellement ou par groupe.

Section 1.2 – Les entités doivent documenter et mettre en œuvre leurs processus d'autorisation pour l'utilisation des *actifs électroniques temporaires* qu'ils gèrent directement. Les *actifs électroniques temporaires* peuvent être désignés individuellement ou par type d'actifs. Afin de respecter cet élément de l'exigence, l'entité doit documenter les éléments suivants :

1.2.1 Les utilisateurs (individuellement, par groupe ou par rôle) autorisés à utiliser les *actifs électroniques temporaires*. On peut inscrire à cette fin le nom de la personne, le nom d'un service ou le titre d'un poste. Attention : il faut déterminer si ces utilisateurs doivent aussi avoir un accès électronique autorisé au système pertinent conformément à la norme CIP-004.

1.2.2 Les emplacements où les *actifs électroniques temporaires* sont autorisés. On peut inscrire à cette fin un emplacement particulier ou un groupe d'emplacements.

1.2.3 L'utilisation prévue ou approuvée des *actifs électroniques temporaires* (individuellement, par groupe ou par rôle). Il faut aussi indiquer les logiciels ou progiciels qui sont autorisés pour des fonctions ou des tâches opérationnelles bien définies (transfert de données, analyse de vulnérabilité, maintenance, dépannage, etc.) ainsi que les interfaces réseau approuvées (par exemple les liaisons sans fil, y compris la communication en champ proche ou par Bluetooth, et les liaisons filaires). Les utilisations et les logiciels ou progiciels non spécifiquement inscrits comme acceptables doivent être considérés comme interdits. Les programmes de sensibilisation à la sécurité et de formation en cybersécurité de la norme CIP-004 peuvent servir à informer le personnel quant aux activités ou aux utilisations autorisées ou interdites (par exemple l'utilisation d'un dispositif pour naviguer sur Internet ou lire des courriels, ou encore pour accéder à des réseaux sans fil dans des hôtels ou d'autres commerces).

Les entités doivent se montrer prudentes dans l'utilisation d'*actifs électroniques temporaires* et s'assurer que ceux-ci n'ont pas de fonctions activées (par exemple la connectivité sans fil ou Bluetooth) qui permettraient au dispositif de servir de relais entre un réseau extérieur et un système visé. Dans un tel cas, l'*actif électronique temporaire* deviendrait un *point d'accès électronique* non autorisé, en contravention avec l'exigence E1 de la norme CIP-005.

Il faut prêter attention aux *actifs électroniques temporaires* qui peuvent être utilisés avec des actifs situés dans des zones ayant des degrés d'impact différents (impacts élevé, moyen et faible). Ces zones d'impact ont différents niveaux de protection en vertu des normes CIP, et il faut prendre des mesures pour atténuer le risque lié à l'introduction de programmes malveillants à partir d'une zone d'impact moindre. Une entité pourrait juger préférable d'avoir des *actifs électroniques temporaires* distincts pour chaque degré d'impact.

Section 1.3 – Les entités doivent documenter et mettre en œuvre leurs processus visant à atténuer le risque lié aux vulnérabilités présentées par les logiciels sans correctifs, en adoptant une ou plusieurs des mesures de protection indiquées. Ces mesures doivent tenir compte des capacités de chaque dispositif. Étant donné la très grande diversité des types de dispositifs qui peuvent servir d'*actifs électroniques temporaires* ainsi que les progrès dans les solutions de gestion des vulnérabilités logicielles, les options présentées laissent la porte ouverte à des solutions de rechange (technologies ou processus) qui atténueraient adéquatement le risque lié à ces vulnérabilités.

- L'application de correctifs, avec mises à jour manuelles ou systématiques, offre à l'entité responsable une certaine latitude quant à l'utilisation de ses *actifs électroniques temporaires*. L'entité peut décider de mettre en place pour ses *actifs électroniques temporaires* un processus normalisé d'application de correctifs de sécurité selon un calendrier régulier, ou plutôt d'appliquer les correctifs de sécurité nécessaires à un *actif électronique temporaire* avant de le connecter à un *actif électronique* visé. Contrairement à l'exigence E2 de la norme CIP-007, l'entité n'a pas à élaborer de plans d'atténuation datés ou d'autres documents au-delà de ce qui est nécessaire pour déterminer que l'*actif électronique temporaire* reçoit les

correctifs de sécurité appropriées.

- L'utilisation de systèmes d'exploitation et de logiciels exécutables uniquement à partir de supports non inscriptibles permet d'avoir un système d'exploitation protégé qui ne peut être modifié de manière à transmettre des programmes malveillants. Lorsqu'une entité crée un système d'exploitation personnalisé sur support externe, elle doit vérifier l'image pendant sa création afin de s'assurer que l'image ne contient aucun programme malveillant.
- Le renforcement du système d'exploitation consiste à éliminer tous les logiciels et utilitaires non essentiels et à n'installer que le minimum indispensable au fonctionnement de l'ordinateur, ce qui aide à réduire les vulnérabilités. Les programmes supplémentaires peuvent offrir des fonctionnalités utiles, mais ils peuvent aussi receler des « portes dérobées » d'accès au système ; leur élimination a pour effet de renforcer le système.
- Si elle opte pour des moyens autres que ceux qui sont suggérés pour atténuer le risque lié aux vulnérabilités logicielles, l'entité doit établir une documentation qui indique comment ces moyens réalisent l'objectif d'atténuer le risque en question.

Section 1.4 – Les entités doivent documenter et mettre en œuvre leurs processus d'atténuation du risque lié à l'introduction de programmes malveillants, en adoptant une ou plusieurs des mesures de protection indiquées. Ces mesures doivent tenir compte des capacités de chaque dispositif. Comme pour la gestion des vulnérabilités logicielles, il convient de reconnaître la grande diversité des types de dispositifs qui peuvent servir d'*actifs électroniques temporaires* ainsi que les progrès réalisés dans la protection contre les programmes malveillants. L'entité responsable doit adopter des mesures pour bloquer, détecter ou prévenir les programmes malveillants. Si un programme malveillant est détecté, il faut le supprimer ou le neutraliser afin qu'il ne puisse pas être introduit dans un *actif électronique BES* ou un *système électronique BES*. L'entité doit aussi déterminer si la détection du programme malveillant constitue un *incident de cybersécurité*.

- Un logiciel antivirus, avec mises à jour manuelles ou systématiques des signatures ou des séquences de code, offre la même souplesse que l'application de correctifs. On peut ainsi gérer les *actifs électroniques temporaires* en déployant des logiciels antivirus ou des outils de sécurité des points terminaux qui assurent une mise à jour programmée des signatures ou des séquences de code. Par ailleurs, pour les dispositifs dont la connexion non régulière ne leur permet pas de recevoir des mises à jour programmées, l'entité peut choisir de balayer l'*actif électronique temporaire* avant son raccordement afin de confirmer l'absence de programme malveillant.
- La liste blanche d'applications consiste à autoriser seulement les applications et les processus nécessaires pour l'*actif électronique temporaire*. Cela réduit d'autant la possibilité pour un programme malveillant de devenir résident, et encore moins de se propager à partir de l'*actif électronique temporaire* vers l'*actif électronique BES* ou le *système électronique BES*.

- On peut limiter les communications aux seuls échanges de données entre un *actif électronique temporaire* géré et les *actifs électroniques* auxquels il est connecté, en restreignant ou en désactivant les communications série ou réseau (y compris sans fil) de l'*actif électronique temporaire*, afin de réduire au minimum les occasions d'introduire un programme malveillant dans celui-ci pendant qu'il n'est pas connecté à un *système électronique BES*. Le dispositif est alors incapable de communiquer avec des dispositifs autres que celui auquel il doit être connecté.
- Si elle opte pour des moyens autres que ceux qui sont suggérés pour l'atténuation du risque lié à l'introduction de programmes malveillants, l'entité doit établir une documentation qui indique comment ces moyens réalisent l'objectif d'atténuer le risque en question.

Section 1.5 : Les entités doivent documenter et mettre en œuvre leurs processus de protection et d'évaluation des *actifs électroniques temporaires* visant à atténuer le risque qu'une utilisation non autorisée de ceux-ci peut présenter pour les *systèmes électroniques BES*. La préoccupation à laquelle répond cette section est la possibilité qu'un *actif électronique temporaire* puisse être manipulé de façon inappropriée ou être exposé à des logiciels malveillants pendant qu'il n'est pas utilisé aux fins prévues par une personne autorisée. La sécurité physique de l'*actif électronique temporaire* est assurément une mesure qui atténue ce risque, mais d'autres outils et techniques sont aussi envisageables. La liste d'exemples ci-après présente différentes possibilités suggérées.

- Les restrictions d'accès physique consistent à maintenir l'*actif électronique temporaire* à l'intérieur d'un *périmètre de sécurité physique* ou d'un autre lieu ou enceinte physique dont les accès physiques sont contrôlés afin de protéger l'*actif électronique temporaire*.
- Le cryptage de disque intégral avec authentification est une option qui permet de protéger un *actif électronique temporaire* contre toute utilisation non autorisée ; il est toutefois important qu'une authentification soit exigée avant le décryptage. Par exemple, l'authentification avant le démarrage ou à la mise sous tension sécurise le système d'exploitation en constituant autour de lui une couche d'authentification externe. Les données du disque dur ne peuvent pas être lues tant que l'utilisateur n'a pas confirmé son identité au moyen d'un mot de passe ou d'autres éléments d'authentification. En imposant une authentification avant le décryptage du système et le démarrage, on réduit le risque qu'une personne non autorisée puisse manipuler l'*actif électronique temporaire*.
- L'authentification multifactorielle sert à confirmer l'identité de la personne qui accède au dispositif. L'authentification multifactorielle atténue aussi le risque qu'une personne non autorisée puisse manipuler l'*actif électronique temporaire*.
- Outre les mécanismes d'authentification et de sécurité physique pure, d'autres possibilités existent. Certaines solutions de sécurisation en cas de vol permettent de géolocaliser l'*actif électronique temporaire*, de détecter tout accès, d'effacer le contenu à distance et de verrouiller le système, limitant ainsi la menace potentielle

liée à une utilisation non autorisée si l'*actif électronique temporaire* était par la suite connecté à un *actif électronique BES*. D'autres solutions plus rudimentaires peuvent aussi être efficaces pour atténuer le risque lié à l'utilisation d'un *actif électronique temporaire* falsifié, par exemple des étiquettes ou des sceaux d'inviolabilité dont l'intégrité est vérifiée au moyen d'une procédure spéciale avant l'utilisation du dispositif.

- Si elle opte pour des moyens autres que ceux qui sont suggérés pour atténuer le risque lié aux utilisations non autorisées, l'entité doit établir une documentation qui indique comment ces moyens réalisent l'objectif d'atténuer le risque en question.

Exigence E4, section 2 de l'annexe 1 – *Actifs électroniques temporaires* gérés par une tierce partie autre que l'entité responsable

Cette annexe reconnaît également que l'entité responsable n'a aucun contrôle direct sur les *actifs électroniques temporaires* qui sont gérés par une tierce partie. L'entité responsable est néanmoins tenue de s'assurer que des moyens ont été déployés pour bloquer, détecter ou prévenir l'introduction de programmes malveillants dans les *actifs électroniques temporaires* qui ne relèvent pas de sa gestion. Les exigences ci-après indiquent aux entités comment procéder au mieux à l'examen des actifs afin de remplir leurs obligations.

Afin d'assurer un contrôle adéquat, les entités responsables peuvent choisir de conclure des ententes avec des tierces parties pour la prestation de services de soutien des *systèmes électroniques BES* et des *actifs électroniques BES* qui peuvent nécessiter l'utilisation d'*actifs électroniques temporaires*. Les entités pourront juger avantageux d'adopter les clauses normalisées du département de l'Énergie des États-Unis pour les contrats de cybersécurité dans le domaine de la fourniture d'énergie (*Cybersecurity Procurement Language for Energy Delivery Systems*[1], avril 2014). Ces clauses d'approvisionnement peuvent aider à harmoniser les actions de l'entité responsable et des tierces parties chargées du soutien des *systèmes électroniques BES* et des *actifs électroniques BES*. Les attributs du programme de protection des infrastructures essentielles (CIP), y compris les rôles et responsabilités, les contrôles d'accès, la surveillance, la journalisation, la gestion des vulnérabilités et celle des correctifs ainsi que les interventions en cas d'incident et la récupération des sauvegardes, peuvent faire partie des prestations confiées à une tierce partie. Les entités pourront s'inspirer des chapitres General Cybersecurity Procurement Language et The Supplier's Life Cycle Security Program du document précité pour la rédaction des ententes-cadres de services, des contrats et des processus et contrôles du programme CIP.

Section 2.1 – Les entités doivent documenter et mettre en œuvre leurs processus d'atténuation du risque lié aux vulnérabilités logicielles, comportant une ou plusieurs des mesures de protection indiquées ci-après.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Procéder à un examen de l'*actif électronique temporaire* géré par une tierce partie autre que l'entité responsable afin de déterminer si la version des correctifs de sécurité du dispositif atténue adéquatement le risque de vulnérabilités logicielles avant la connexion de l'*actif électronique temporaire* à un système visé.

- Procéder à un examen de la procédure d'application de correctifs de la tierce partie. Cet examen peut être fait lors de l'entente contractuelle, ou au plus tard avant de connecter l'*actif électronique temporaire* à un système visé. Tout comme pour l'examen de la version des correctifs de sécurité du dispositif, le choix de ce moyen vise à confirmer que l'entité responsable a atténué le risque lié aux vulnérabilités logicielles pour les systèmes visés.
- Procéder à un examen d'autres processus adoptés par la tierce partie pour atténuer le risque lié aux vulnérabilités logicielles, par exemple le renforcement du système d'exploitation, les listes blanches d'applications, les machines virtuelles, etc.
- Si elle opte pour des moyens autres que ceux qui sont suggérés pour atténuer le risque lié aux vulnérabilités logicielles, l'entité doit établir une documentation qui indique comment ces moyens réalisent l'objectif d'atténuer le risque en question.

Section 2.2 – Les entités doivent documenter et mettre en œuvre leurs processus d'atténuation du risque lié à l'introduction des programmes malveillants, comportant une ou plusieurs des mesures d'atténuation indiquées ci-après.

- Procéder à un examen des niveaux de tenue à jour des logiciels antivirus ainsi que des signatures ou des séquences de code afin de s'assurer que ces niveaux permettent à l'entité responsable d'atténuer adéquatement le risque lié à l'introduction de programmes malveillants dans un système visé.
- Procéder à un examen des processus antivirus ou de sécurisation des points terminaux de la tierce partie afin de s'assurer que ces processus permettent à l'entité responsable d'atténuer adéquatement le risque lié à l'introduction de programmes malveillants dans un système visé.
- Procéder à un examen de l'utilisation par la tierce partie de listes blanches d'applications pour atténuer le risque lié à l'introduction de programmes malveillants dans un système visé.
- Procéder à un examen de l'utilisation de systèmes d'exploitation ou de logiciels exécutables uniquement à partir de supports non inscriptibles afin de s'assurer que les supports eux-mêmes sont exempts de tout programme malveillant. Les entités doivent examiner les processus de préparation des supports non inscriptibles ainsi que les supports eux-mêmes.
- Procéder à un examen des pratiques adoptées par la tierce partie pour le renforcement du système d'exploitation afin de s'assurer que les ports, services, applications et autres éléments inutiles ont été désactivés ou retirés, ce qui limite le risque d'introduction de programmes malveillants dans un système visé.

Section 2.3 – Déterminer si des mesures d'atténuation supplémentaires sont nécessaires, et exécuter ces mesures avant de connecter l'*actif électronique temporaire* géré par une tierce partie. Cette section vise à faire en sorte que si, après les examens effectués conformément aux sections 2.1 et 2.2, des lacunes subsistent par rapport à la posture de sécurité de l'entité responsable, la tierce partie soit tenue d'exécuter des mesures d'atténuation supplémentaires avant de connecter ses dispositifs à un système visé.

Exigence E4, section 3 de l'annexe 1 – *Supports de stockage amovibles*

Les entités ont un degré de contrôle élevé sur les *supports de stockage amovibles* destinés à être connectés à leurs *actifs électroniques BES*.

Section 3.1 – Les entités doivent documenter et mettre en œuvre leurs processus d'autorisation de l'utilisation des *supports de stockage amovibles*. Les *supports de stockage amovibles* peuvent être inscrits individuellement ou par type.

- Documenter les utilisateurs (individuellement, par groupe ou par rôle) autorisés à utiliser les *supports de stockage amovibles*. On peut inscrire à cette fin le nom de la personne, le nom d'un service ou le titre d'un poste. L'autorisation s'étend au personnel de l'entité ainsi qu'aux fournisseurs. Attention : il faut déterminer si ces utilisateurs doivent aussi avoir un accès électronique autorisé au système pertinent conformément à la norme CIP-004.
- Documenter les emplacements où les *supports de stockage amovibles* sont autorisés. On peut inscrire à cette fin un emplacement particulier ou un groupe d'emplacements.

Section 3.2 – Les entités doivent documenter et mettre en œuvre leurs processus d'atténuation du risque lié à l'introduction de programmes malveillants, comportant un ou plusieurs moyens de détecter tout programme malveillant sur les *supports de stockage amovibles* avant leur connexion à un *actif électronique BES*. La détection de programmes malveillants doit normalement se faire à partir d'un système qui ne fait pas partie d'un *système électronique BES*, afin d'atténuer le risque lié à la propagation de programmes malveillants dans le réseau des *systèmes électroniques BES* ou dans un des *actifs électroniques BES*. Si un programme malveillant est détecté, il faut le supprimer ou le neutraliser afin qu'il ne puisse pas être introduit dans un *actif électronique BES* ou un *système électronique BES*. L'entité doit aussi déterminer si la détection du programme malveillant constitue un *incident de cybersécurité*. La fréquence et le choix du moment d'utilisation des moyens de détection des programmes malveillants ont été intentionnellement exclus de l'exigence, car il existe de multiples scénarios temporels possibles pour un plan d'atténuation du risque lié à l'introduction de programmes malveillants. Les entités doivent procéder à la détection des programmes malveillants sur les *supports de stockage amovibles* avant qu'ils soient connectés à l'*actif électronique BES*. Un choix judicieux du moment des interventions de détection, documenté dans le plan de l'entité, devrait réduire le risque d'introduction de programmes malveillants dans l'*actif électronique BES* ou l'*actif électronique protégé*.

Pour la détection des programmes malveillants, les entités peuvent choisir d'utiliser des *supports de stockage amovibles* auxquels sont intégrés des outils de détection de programmes malveillants. Dans ce cas, les outils de détection intégrés au support d'information amovible

doivent quand même être utilisés en combinaison avec un *actif électronique*. La section 3.2.1 précise que l'*actif électronique* utilisé pour la détection de programmes malveillants doit être situé à l'extérieur d'un *système électronique BES* ou d'un *actif électronique protégé*.

Justification

Pendant l'élaboration de cette norme, des zones de texte ont été incorporées à celle-ci pour exposer la justification de ses diverses parties. Après l'approbation par le Conseil d'administration, le contenu de ces zones de texte a été transféré ci-après.

Justification de l'exigence E1 :

Les processus de gestion des changements de configuration visent à empêcher les modifications non autorisées aux *systèmes électroniques BES*.

Justification de l'exigence E2 :

Les processus de surveillance de la configuration visent à détecter les modifications non autorisées aux *systèmes électroniques BES*.

Justification de l'exigence 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.

Justification de l'exigence E4 :

L'exigence E4 met en œuvre les prescriptions des paragraphes 6 et 136 de l'ordonnance 791 de la FERC, qui concernent les questions de sécurité associées aux *actifs électroniques temporaires* et aux *supports de stockage amovibles* utilisés pendant une durée limitée pour des tâches comme le transfert de données, l'analyse de vulnérabilité, la maintenance ou le dépannage. Ces outils sont des vecteurs potentiels d'introduction de programmes malveillants dans une installation et, de là, dans des *actifs électroniques* ou des *systèmes électroniques BES*. Afin d'atténuer les risques associés à de tels outils, l'exigence E4 a été élaborée en fonction des objectifs de sécurité suivants :

- empêcher tout accès non autorisé ou toute transmission de logiciels malveillants aux *systèmes électroniques BES* par des *actifs électroniques temporaires* ou des *supports de stockage amovibles* ; et
- empêcher tout accès non autorisé à l'information de *système électronique BES* au moyen d'*actifs électroniques temporaires* ou de *supports de stockage amovibles*.

L'exigence E4 intègre les concepts d'autres exigences des normes CIP-010-2 et CIP-007-6 afin d'aider à définir les exigences applicables aux actifs électroniques temporaires et aux *supports de stockage amovibles*.

Résumé des changements – Toutes les exigences relatives aux *actifs électroniques temporaires* et aux *supports de stockage amovibles* sont regroupées dans la norme CIP-010. En raison de la nouveauté de la définition de ces types d'actifs et des exigences qui s'y appliquent, la SDT a jugé que le regroupement de ces exigences dans une seule et même

norme aiderait les entités à reconnaître rapidement les exigences applicables à ces types d'actifs. La création d'une norme séparée pour ces exigences a été envisagée ; cependant, la SDT a déterminé que l'utilisation de ces types d'actifs est connexe aux processus de gestion des changements et d'analyse de vulnérabilité, et qu'il est en somme préférable de regrouper le tout dans la norme qui encadre déjà ces processus.

Annexe QC-CIP-010-2
Dispositions particulières de la norme CIP-010-2 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-010-2

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

   4.1. Entités fonctionnelles

   Aucune disposition particulière

   4.2. Installations

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

   Exemptions additionnelles

   Sont exemptés de l'application de la présente norme :

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

5. **Date d'entrée en vigueur 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 :

Norme	Révision CIPv6	Date d'entrée en vigueur proposée au Québec		
		Entités visées par la version 1 des normes CIP adoptées par la Régie	Entités ne possédant pas d'installations de production à vocation industrielle et non visées par la version 1 des normes CIP	Entités qui possèdent des installations de production à vocation industrielle
CIP-010-2	Élimination de la formulation « détecter, évaluer et corriger » car elle est vague et sujette à de multiples interprétations	2017-10-01	2018-10-01	2019-04-01
CIP-010-2, E4	Nouvelle exigence pour les *actifs électronique transitoires* (TCA) et les *supports d'information de stockage* (RM)	2017-10-01	2018-10-01	2019-04-01

Les ajouts et modifications proposés au glossaire pour les termes suivants doivent être approuvés et en vigueur en même temps que la norme : [1]

- « *actif électronique transitoire* » ;
- « actifs électroniques BES » ;
- « *actifs électroniques protégés* ».

6. Contexte

Aucune disposition particulière

[1] Cette section sera retirée suivant l'adoption de la norme par la Régie.

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et de mise en application des normes

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

Annexe 1

Aucune disposition particulière

Annexe 2

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Justification

Aucune disposition particulière

Historique des versions

Révision	Date d'adoption	Intervention	Suivi des modifications
0	29 juillet 2016	Nouvelle annexe.	Nouvelle

A. Introduction

1. Titre : Cybersécurité — Protection de l'information

2. Numéro : CIP-011-2

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 système de production-transport d'électricité (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* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale; et

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

4.1.2.2 Chaque *automatisme de réseau* ou *plan de défense* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

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

4.1.2.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des 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* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale; et

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

4.2.1.2 Chaque *automatisme de réseau* ou *plan de défense* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les *distributeurs* :

Toutes les *installations* du *BES*.

4.2.3 Exemptions : Sont exemptés de la norme CIP-011-2 :

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 composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme au règlement CFR 10, section 73.54;

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

4.2.3.5 les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* classés dans les catégories « impact élevé » ou « impact moyen » selon le processus de désignation et de catégorisation de la norme CIP-002-5.1.

5. Dates de mise en vigueur

Voir le plan de mise en œuvre de la norme CIP-011-2.

6. Contexte :

La norme CIP-011 fait partie d'une série de normes CIP sur la cybersécurité qui exigent la détermination et la catégorisation initiales des *systèmes électroniques BES*. Ces normes exigent aussi un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.

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

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité doit inclure tout ce qu'elle juge nécessaire dans ses processus documentés, en s'assurant de bien couvrir les exigences pertinentes.

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

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation

du personnel sont des exemples qui figurent dans les normes. La mise en œuvre complète des normes de fiabilité CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

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

Les mesures auxquelles renvoie l'énoncé initial de l'exigence correspondent simplement aux processus documentés eux-mêmes. La colonne « Mesures » présente des exemples de pièces justificatives attestant la documentation et la mise en œuvre des éléments pertinents dans les processus documentés; ces exemples sont présentés à titre indicatif, et leur liste ne doit pas être considérée comme exhaustive.

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

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes 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 *BES*. Un examen des tolérances des 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. La SDT (équipe de rédaction) CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- ***Systèmes électroniques BES* à impact élevé –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.

- ***Systèmes électroniques BES* à impact moyen –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.
- ***Systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*) –** Désigne tout *système de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d’authentification et systèmes de surveillance de registre d’événements et d’alerte.
- ***Systèmes de contrôle des accès physiques* (*PACS*) –** Désigne tout *système de contrôle des accès physique*s associés 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 un ou plusieurs programmes documentés de protection de l'information qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-011-2) – Protection de l'information. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]*

M1. Les pièces justificatives du programme de protection de l'information doivent couvrir toutes les parties applicables du tableau E1 (CIP-011-2) – Protection de l'information; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

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

Tableau E1 (CIP-011-2) – Protection de l'information			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
			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.
1.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés; et 2. les *PACS* associés.	Procédures 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, couvrent tous les alinéas applicables du tableau E2 (CIP-011-2) – 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, couvrent toutes les parties applicables du tableau E2 (CIP-011-2) – Réutilisation et élimination des *actifs électroniques BES*; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-011-2) – Réutilisation et élimination des actifs électroniques BES			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés; 2. les *PACS* associés; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés; 2. les *PACS* associés; et 3. les *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* stockée sur le support de stockage 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-011-2) – Réutilisation et élimination des actifs électroniques BES			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés; 2. les *PACS* associés; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés; 2. les *PACS* associés; et *3.* les *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* stockée sur 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 des mesures pour assurer la conformité

Selon la définition des règles de procédure de la NERC, le terme « *responsable des mesures pour assurer la conformité* » (CEA) désigne la NERC ou l’entité régionale dans leurs rôles respectifs de surveillance de la conformité aux normes de fiabilité de la NERC.

1.2. Conservation des pièces justificatives

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

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

- Chaque entité 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 de mise en application des normes

Audits de conformité

Déclarations sur la conformité

Contrôles ponctuels

Enquêtes de conformité

Déclarations de non-conformité

Plaintes

1.4. Autres informations sur la conformité

Aucune.

2. Tableau des éléments de conformité

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-011-2)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1	**Planification de l'exploitation**	**Moyen**	Sans objet	Sans objet	Sans objet	L'entité responsable n'a pas documenté ou mis en œuvre un programme de protection de l'*information de système électronique BES.* (E1)
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 d'*information de système électronique BES* à partir de l'*actif électronique BES.* (2.1)	L'entité responsable a mis en œuvre un ou plusieurs processus documentés, mais n'a pas inclus de processus d'élimination ou de destruction de support afin d'empêcher la récupération non autorisée d'*information de système électronique BES* à partir de l'*actif électronique BES.* (2.2)	L'entité responsable n'a documenté ou mis en œuvre aucun processus pour les alinéas applicables du tableau E2 (CIP-011-2) – Réutilisation et élimination des *actifs électroniques BES.* (E2)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Principes directeurs et fondements techniques (ci-joints)

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	Ordonnance de la FERC approuvant CIP-011-1 (L'ordonnance entre en vigueur le 3 février 2014)	
2	13 novembre 2014	Adoption par le conseil d'administration de la NERC	Mise en œuvre de deux prescriptions de l'ordonnance 791 de la FERC concernant l'obligation de « détecter, évaluer et corriger » ainsi que les réseaux de communication.

Version	Date	Intervention	Suivi des modifications
2	12 février 2015	Adoption par le conseil d'administration de la NERC	Remplace la version adoptée par le conseil d'administration le 13 novembre 2014. La version à jour met en œuvre des prescriptions en instance de l'ordonnance 791 relativement aux actifs temporaires et aux *systèmes électroniques BES* à impact faible.
6	21 janvier 2016	Ordonnance de la FERC émise approuvant CIP-003-6. Dossier no. RM15-14-000	

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) présente 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, les normes CIP sur la cybersécurité de la NERC s'y appliquent. Il est à noter qu'en ce qui concerne les *distributeurs*, la section 4.1 limite l'applicabilité 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 qui, selon la section 4.1, est visée par les exigences de la norme. Comme il est indiqué à la section d'exemption 4.2.3.5, la présente norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou moyen selon la catégorisation de la norme CIP-002-5.1. 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* » dans le glossaire de la NERC indique déjà qu'il s'agit d'*éléments* du *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 aide à clarifier 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*.

La 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 électroniques et papiers. 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. Ces procédures s'appliquent aussi à l'information qui peut se trouver sur des *actifs électroniques transitoires*ou des *supports amovibles*.

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.

Justification

Pendant l'élaboration de cette norme, des zones de texte ont été incorporées à celle-ci pour exposer la justification de ses diverses parties. Après l'approbation par le Conseil d'administration, le contenu de ces zones de texte a été transféré ci-après.

Justification de l'exigence 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*.

Justification de l'exigence 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.

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-011-2

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

4.1. Entités fonctionnelles

Aucune disposition particulière

4.2. Installations

Installations

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

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

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

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

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

Norme	Révision CIPv6	Date d'entrée en vigueur proposée au Québec		
		Entités visées par la version 1 des normes CIP adoptées par la Régie	Entités ne possédant pas d'installations de production à vocation industrielle et non visées par la version 1 des normes CIP	Entités qui possèdent des installations de production à vocation industrielle
CIP-011-2	Informations stockées sur *actifs électronique transitoires* (TCA) et les *supports d'information de stockage* (RM) référencées dans les principes directeurs et fondement techniques	2017-10-01	2018-10-01	2019-04-01

Les ajouts et modifications proposés au glossaire pour les termes suivants doivent être approuvés et en vigueur en même temps que la norme : [1]

- « *actifs électroniques BES* »;
- « *actifs électroniques protégés* ».

6. Contexte : Aucune disposition particulière

[1] Cette section sera retirée suivant l'adoption de la norme par la Régie.

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et de mise en application des normes

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

1.5. 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

Justification

Aucune disposition particulière

Historique des versions

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

A. Introduction

1. **Titre :** **Sécurité physique**

2. **Numéro :** **CIP-014-2**

3. **Objet :** Désigner et protéger les postes de *transport* et les centres de contrôle principaux connexes qui, s'ils devenaient inopérants ou étaient endommagés par suite d'une attaque physique, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*.

4. **Applicabilité :**

   4.1. Entités fonctionnelles :

   4.1.1 *Propriétaire d'installation de transport* ayant un poste de *transport* qui répond à un des critères suivants :

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

   4.1.1.2 *Installations* de *transport* exploitées entre 200 et 499 kV dans un seul et même poste, celui-ci étant raccordé à 200 kV ou plus à au moins trois autres postes de *transport* et ayant une « valeur pondérée combinée » de plus de 3 000 selon le tableau ci-dessous. La « valeur pondérée combinée » d'un poste est la somme des « valeurs pondérées par ligne » respectives, indiquées au tableau, des *lignes de transport* d'arrivée et de départ qui font partie du *BES* et qui relient ce poste à un autre poste de *transport*. Aux fins de ce critère, le jeu de barres collectrices d'une centrale 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

4.1.1.3 *Installations* de *transport* d'un même poste, désignées par leur *coordonnateur de la fiabilité*, leur *responsable de la planification* ou leur *planificateur de réseau de transport* comme déterminantes dans le calcul des *limites d'exploitation pour la fiabilité de l'Interconnexion* (*IROL*) et des contingences qui y sont associées.

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

4.1.2 *Exploitant de réseau de transport.*

Exemptions : La présente norme ne s'applique pas aux *installations* situées dans une « zone protégée », selon la définition de la section 73.2 du titre 10 du *Code of Federal Regulations*, et visées par un plan de sécurité approuvé ou accepté par la U.S. Nuclear Regulatory Commission, non plus qu'aux *installations* visées par un plan de sécurité approuvé ou accepté par la Commission canadienne de sûreté nucléaire.

5. Date d'entrée en vigueur :

Voir le plan de mise en œuvre pour la CIP-014-2.

6. Contexte :

La présente norme de fiabilité répond aux prescriptions de l'Ordonnance de la FERC du 7 mars 2014, *Reliability Standards for Physical Security Measures, 146 FERC ¶61,166 (2014)*, qui demande à la NERC d'établir une ou des normes de fiabilité relatives à la sécurité physique afin que soient désignées et protégées les installations qui, si elles devenaient inopérantes ou étaient endommagées, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*.

B. Exigences et mesures

E1. Chaque *propriétaire d'installation de transport* doit effectuer une évaluation des risques initiale ainsi que des évaluations des risques subséquentes pour ses postes de *transport* (existants ou devant entrer en service dans les 24 mois suivants) qui répondent aux critères de l'alinéa 4.1.1 de la section Applicabilité. Les évaluations des risques initiale et subséquentes doivent consister en des analyses du réseau de transport visant à désigner les postes de *transport* qui, s'ils devenaient inopérants ou étaient endommagés, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*.
[Facteur de risque (VRF) : élevé] [Horizon : planification à long terme]

1.1. Les évaluations des risques subséquentes doivent être effectuées :

- au moins une fois tous les 30 mois civils pour un *propriétaire d'installation de transport* dont l'évaluation des risques précédente (après vérification selon

l'exigence E2) a désigné un ou plusieurs postes de *transport* qui, s'ils devenaient inopérants ou étaient endommagés, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion* ; ou

- au moins une fois tous les 60 mois civils pour un *propriétaire d'installation de transport* dont l'évaluation des risques précédente (après vérification selon l'exigence E2) n'a désigné aucun poste de *transport* qui, s'il devenait inopérant ou était endommagé, pourrait entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*.

1.2. Le *propriétaire d'installation de transport* doit également désigner le centre de contrôle principal qui exerce le contrôle opérationnel sur chaque poste de transport désigné dans l'évaluation des risques prescrite à l'exigence E1.

M1. Exemples non limitatifs de preuve adéquate : documentation datée (en version papier ou électronique) de l'évaluation des risques pour les postes de *transport* (existants et devant entrer en service dans les 24 mois suivants) qui répondent aux critères de l'alinéa 4.1.1 de la section Applicabilité de l'exigence E1. Autres exemples non limitatifs de preuve adéquate : documentation datée (en version papier ou électronique) de la désignation du centre de contrôle principal qui exerce le contrôle opérationnel sur chaque poste de *transport* désigné dans l'évaluation des risques, selon l'alinéa 1.2 de l'exigence E1.

E2. Chaque *propriétaire d'installation de transport* doit faire vérifier par un tiers indépendant l'évaluation des risques effectuée selon l'exigence E1. Cette vérification peut avoir lieu pendant ou après l'évaluation en question.
[Facteur de risque (VRF) : moyen] [Horizon : planification à long terme]

2.1. Chaque *propriétaire d'installation de transport* doit mandater une entité vérificatrice indépendante, qui doit être :

- un *coordonnateur de la planification*, *planificateur de réseau de transport* ou *coordonnateur de la fiabilité* inscrit au registre ; ou
- une entité ayant de l'expérience en planification ou en analyse du transport de l'électricité.

2.2. L'entité vérificatrice indépendante doit vérifier l'évaluation des risques effectuée par le *propriétaire d'installation de transport* selon l'exigence E1, et peut recommander l'ajout ou le retrait de postes de *transport*. Le *propriétaire d'installation de transport* doit veiller à ce que la vérification soit terminée dans les 90 jours civils suivant la fin de l'évaluation effectuée selon l'exigence E1.

2.3. Si l'entité vérificatrice indépendante recommande au *propriétaire d'installation de transport* d'ajouter ou de retirer un ou plusieurs postes de *transport* dans la désignation effectuée selon l'exigence E1, le *propriétaire d'installation de transport* doit, dans les 60 jours civils suivant la fin de la vérification, pour chaque ajout ou retrait de poste de *transport* recommandé :

- modifier, conformément à la recommandation, la désignation effectuée selon l'exigence E1; ou
- documenter la justification technique de son refus d'apporter la modification recommandée.

2.4. Chaque *propriétaire d'installation de transport* doit adopter des procédures (ententes de non-divulgation, etc.) afin de protéger les informations sensibles ou confidentielles accessibles à l'entité vérificatrice indépendante, ainsi que de soustraire à la divulgation publique toute information sensible ou confidentielle produite dans le cadre de l'application de la présente norme de fiabilité.

M2. Exemples non limitatifs de preuve adéquate : documentation datée (en version papier ou électronique) attestant que le *propriétaire d'installation de transport* a fait vérifier par un tiers indépendant l'évaluation effectuée selon l'exigence E1 et qu'il a respecté toutes les dispositions applicables de l'exigence E2, y compris, le cas échéant, la documentation de son refus de modifier la désignation selon l'alinéa 2.3. Autres exemples non limitatifs de preuve adéquate : documentation (en version papier ou électronique) des procédures visant à protéger l'information selon l'alinéa 2.4.

E3. Pour tout centre de contrôle principal désigné par le *propriétaire d'installation de transport*, selon l'alinéa 1.2 de l'exigence E1, a) comme exerçant le contrôle opérationnel sur un poste de *transport* désigné et vérifié selon l'exigence E2, mais b) comme n'étant pas sous le contrôle opérationnel du *propriétaire d'installation de transport*, ce dernier doit, dans les sept jours civils suivant la fin de la vérification selon l'exigence E2, aviser l'*exploitant de réseau de transport* qui exerce le contrôle opérationnel sur le centre de contrôle principal en question pour lui signaler la désignation du poste et la date de fin de la vérification selon l'exigence E2. *[Facteur de risque (VRF) : faible] [Horizon : planification à long terme]*

3.1. Si un poste de *transport* désigné selon l'exigence E1 et confirmé selon l'exigence E2 se voit retirer sa désignation lors d'une évaluation des risques subséquente effectuée selon l'exigence E1 ou d'une vérification de celle-ci selon l'exigence E2, le *propriétaire d'installation de transport* doit, dans les sept jours civils suivant l'évaluation ou la vérification en cause, aviser de ce retrait l'*exploitant de réseau de transport* qui exerce le contrôle opérationnel sur le centre de contrôle principal.

M3. Exemples non limitatifs de preuve adéquate : notifications ou communications datées (en version papier ou électronique) attestant que le *propriétaire d'installation de transport* a avisé chaque *exploitant de réseau de transport*, selon le cas, conformément à l'exigence E3.

E4. Chaque *propriétaire d'installation de transport* qui a désigné un poste de *transport* ou un centre de contrôle principal selon l'exigence E1 et qui a fait vérifier cette désignation selon l'exigence E2, ainsi que chaque *exploitant de réseau de transport* avisé par un *propriétaire d'installation de transport* selon l'exigence E3, doit effectuer une évaluation des menaces potentielles d'attaque physique et des vulnérabilités à de telles attaques pour chacun de leurs postes de *transport* et centres de contrôle principaux désignés selon l'exigence E1 et vérifiés selon l'exigence E2. Cette évaluation doit porter sur les éléments suivants :
[Facteur de risque (VRF) : moyen] [Horizon : exploitation en temps différé et planification à long terme]

- **4.1.** caractéristiques particulières des postes de *transport* et centres de contrôle principaux désignés et vérifiés ;
- **4.2.** historique des attaques d'installations semblables, avec prise en compte de la fréquence, de la proximité géographique et de la gravité des incidents de sécurité physique antérieurs ; et
- **4.3.** renseignements ou menaces transmis notamment par les autorités policières, l'organisation de fiabilité du service d'électricité (ERO), l'Electricity Sector Information Sharing and Analysis Center (ES-ISAC), des agences fédérales des États-Unis ou des organismes publics du Canada, ou leurs remplaçants éventuels.

M4. Exemples non limitatifs de preuve adéquate : documentation datée (en version papier ou électronique) attestant que le *propriétaire d'installation de transport* ou l'*exploitant de réseau de transport* a effectué une évaluation des menaces potentielles et vulnérabilités pour son ou ses postes de transport et centres de contrôle principaux visés, selon l'exigence E4.

E5. Chaque *propriétaire d'installation de transport* qui a désigné un poste de *transport* ou un centre de contrôle principal selon l'exigence E1 et qui a fait vérifier cette désignation selon l'exigence E2, ainsi que chaque *exploitant de réseau de transport* avisé par un *propriétaire d'installation de transport* selon l'exigence E3, doivent élaborer et mettre en place un ou des plans de sécurité physique documentés pour leurs postes de *transport* et centres de contrôle principaux visés. Chaque plan de sécurité physique doit être préparé dans les 120 jours civils suivant la fin de la vérification selon l'exigence E2, et être mis en place dans les délais prescrits dans ce plan. Chaque plan de sécurité physique doit comporter les éléments suivants:
[Facteur de risque (VRF) : élevé] [Horizon : planification à long terme]

- **5.1.** mesures de résilience ou de sécurité conçues collectivement pour prévenir, détecter, retarder, évaluer, communiquer et contrer les menaces et vulnérabilités physiques potentielles inventoriées selon l'exigence E4 ;
- **5.2.** informations de contact des autorités policières et de coordination avec celles-ci ;

5.3. délais d'exécution des mesures de renforcement de la sécurité physique et autres modifications énoncées dans le plan de sécurité physique ;

5.4. dispositions prévoyant un suivi de l'évolution des menaces physiques pour les postes de *transport* ou les centres de contrôle principaux, ainsi que des mesures de sécurité correspondantes.

M5. Exemples non limitatifs de preuve adéquate : documentation datée (en version papier ou électronique) attestant qu'un plan de sécurité physique conforme à l'exigence E5 a été élaboré pour chacun des postes de *transport* et centres de contrôle principaux désignés et vérifiés, et une preuve supplémentaire attestant la mise en place du plan de sécurité physique dans les délais qui y sont prescrits.

E6. Chaque *propriétaire d'installation de transport* qui a désigné un poste de *transport* ou un centre de contrôle principal selon l'exigence E1 et qui a fait vérifier cette désignation selon l'exigence E2, ainsi que chaque *exploitant de réseau de transport* avisé par un *propriétaire d'installation de transport* selon l'exigence E3, doivent faire examiner par un tiers indépendant l'évaluation effectuée selon l'exigence E4 et le ou les plans de sécurité élaborés selon l'exigence E5. Cet examen peut avoir lieu pendant ou après l'évaluation effectuée selon l'exigence E4 et l'élaboration du ou des plans de sécurité selon l'exigence E5.
[Facteur de risque (VRF) : moyen] [Horizon : planification à long terme]

6.1. Chaque *propriétaire d'installation de transport* et *exploitant de réseau de transport* visé doit mandater une entité examinatrice indépendante, qui doit être :

- une entité ou organisation ayant de l'expérience en matière de sécurité physique dans l'industrie électrique, et dont le personnel d'examen compte au moins un titulaire de certification CPP (Certified Protection Professional) ou PSP (Physical Security Professional) ;
- une entité ou organisation agréée par l'organisation de fiabilité du service d'électricité (ERO) ;
- un organisme gouvernemental ayant de l'expertise en sécurité physique ; ou
- une entité ou organisation ayant une expertise confirmée en sécurité physique dans un cadre policier, gouvernemental ou militaire.

6.2. Le *propriétaire d'installation de transport* ou l'*exploitant de réseau de transport* doit veiller à ce que l'entité examinatrice ait terminé son examen dans les 90 jours civils suivant la fin de l'élaboration du ou des plans de sécurité selon l'exigence E5. L'examen peut facultativement recommander des changements à l'évaluation effectuée selon l'exigence E4 ou aux plans de sécurité élaborés selon l'exigence E5.

6.3. Si l'entité examinatrice recommande des changements à l'évaluation effectuée selon l'exigence E4 ou aux plans de sécurité élaborés selon l'exigence E5, le *propriétaire d'installation de transport* ou l'*exploitant de réseau de transport* doit, dans les 60 jours civils suivant la fin de l'examen par l'entité examinatrice, pour chaque recommandation :

- modifier son évaluation ou son plan de sécurité selon la recommandation ; ou
- documenter les raisons qui motivent son refus d'apporter la modification demandée.

6.4. Chaque *propriétaire d'installation de transport* et *exploitant de réseau de transport* doit adopter des procédures (ententes de non-divulgation, etc.) afin de protéger les informations sensibles ou confidentielles accessibles à l'entité examinatrice indépendante, ainsi que de soustraire à la divulgation publique toute information sensible ou confidentielle produite dans le cadre de l'application de la présente norme de fiabilité.

M6. Exemples non limitatifs de preuve adéquate : documentation (en version papier ou électronique) attestant que le *propriétaire d'installation de transport* ou l'*exploitant de réseau de transport* a fait examiner par un tiers indépendant, selon l'exigence E6, l'évaluation effectuée selon l'exigence E4 et le ou les plans de sécurité élaborés selon l'exigence E5, y compris, le cas échéant, la documentation de son refus de modifier l'évaluation ou le ou les plans de sécurité selon l'alinéa 6.3. Autres exemples non limitatifs de preuve adéquate : documentation (en version papier ou électronique) des procédures visant à protéger l'information selon l'alinéa 6.4.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Selon la définition des règles de procédure de la NERC, le terme « responsable des mesures pour assurer la conformité » (CEA) désigne la NERC ou l'entité régionale dans leurs rôles respectifs de surveillance de la conformité aux normes de fiabilité de la NERC.

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 indiquée est plus courte que le temps écoulé depuis l'audit le plus récent, le CEA peut demander à l'entité de fournir d'autres pièces justificatives pendant une visite sur place afin d'attester sa conformité pendant la période complète écoulée depuis l'audit le plus récent.

Le *propriétaire d'installation de transport* et l'*exploitant de réseau de transport* doivent conserver les données ou les pièces justificatives suivantes attestant la conformité, à moins que leur CEA leur ordonne, dans le cadre d'une enquête, de conserver certains éléments de pièces justificatives plus longtemps.

Les entités responsables doivent conserver les pièces justificatives documentaires pendant trois ans.

Si une entité responsable est jugée non conforme à une exigence, 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, sous réserve des exigences de confidentialité de la section 1500 des règles de procédure de la NERC et des dispositions de la section 1.4 ci-après.

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

Audits de conformité

Déclarations sur la conformité

Contrôle ponctuel

Enquêtes sur les non-conformités

Déclarations volontaires

Plaintes

1.4. Autres informations sur la conformité

Confidentialité : Afin de protéger la confidentialité et de respecter la nature sensible des pièces justificatives de conformité à la présente norme, tout élément de preuve sera conservé dans les installations du *propriétaire d'installation de transport* et de l'*exploitant de réseau de transport*.

2. Tableau des éléments de conformité

	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-014-1)			
			VSL faible	VSL modérée	VSL élevée	VSL critique
E1	**Planification à long terme**	**Élevé**	Le *propriétaire d'installation de transport* a effectué une évaluation des risques initiale, mais avec un retard d'au plus deux mois civils par rapport à la date prescrite pour cette évaluation dans le plan de mise en œuvre. OU Le *propriétaire d'installation de transport* dont l'évaluation des risques précédente a désigné un ou plusieurs postes de transport qui, s'ils devenaient inopérants ou étaient endommagés, pourraient entraîner une instabilité, une séparation fortuite ou	Le *propriétaire d'installation de transport* a effectué une évaluation des risques initiale, mais avec un retard de plus de deux mois civils et d'au plus quatre mois civils par rapport à la date prescrite pour cette évaluation dans le plan de mise en œuvre. OU Le *propriétaire d'installation de transport* dont l'évaluation des risques précédente a désigné un ou plusieurs postes de transport qui, s'ils devenaient inopérants ou étaient endommagés, pourraient entraîner une instabilité, une	Le *propriétaire d'installation de transport* a effectué une évaluation des risques initiale, mais avec un retard de plus de quatre mois civils et d'au plus six mois civils par rapport à la date prescrite pour cette évaluation dans le plan de mise en œuvre. OU Le *propriétaire d'installation de transport* dont l'évaluation des risques précédente a désigné un ou plusieurs postes de transport qui, s'ils devenaient inopérants ou étaient endommagés, pourraient entraîner une instabilité, une	Le *propriétaire d'installation de transport* a effectué une évaluation des risques initiale, mais avec un retard de plus de six mois civils par rapport à la date prescrite pour cette évaluation dans le plan de mise en œuvre. OU Le *propriétaire d'installation de transport* n'a pas effectué une évaluation des risques initiale. OU Le propriétaire d'installation de transport dont l'évaluation des risques précédente a désigné un ou plusieurs postes

	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-014-1)			
			VSL faible	VSL modérée	VSL élevée	VSL critique
			des *déclenchements en cascade* dans une *Interconnexion*, a effectué une évaluation des risques subséquente dans un délai de plus de 30 mois civils et d'au plus 32 mois civils. OU Le *propriétaire d'installation de transport* dont l'évaluation des risques précédente n'a désigné aucun poste de transport qui, s'il devenait inopérant ou était endommagé, pourrait entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*, a effectué une évaluation des risques	séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*, a effectué une évaluation des risques subséquente dans un délai de plus de 32 mois civils et d'au plus 34 mois civils. OU Le *propriétaire d'installation de transport* dont l'évaluation des risques précédente n'a désigné aucun poste de transport qui, s'il devenait inopérant ou était endommagé, pourrait entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*, a effectué une évaluation	séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*, a effectué une évaluation des risques subséquente dans un délai de plus de 34 mois civils et d'au plus 36 mois civils. OU Le *propriétaire d'installation de transport* dont l'évaluation des risques précédente n'a désigné aucun poste de transport qui, s'il devenait inopérant ou était endommagé, pourrait entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*, a effectué une évaluation	de transport qui, s'ils devenaient inopérants ou étaient endommagés, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*, a effectué une évaluation des risques subséquente dans un délai de plus de 36 mois civils. OU Le *propriétaire d'installation de transport* dont l'évaluation des risques précédente a désigné un ou plusieurs postes de transport qui, s'ils devenaient inopérants ou étaient endommagés, pourraient entraîner

	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-014-1)			
			VSL faible	**VSL modérée**	**VSL élevée**	**VSL critique**
			subséquente dans un délai de plus de 60 mois civils et d'au plus 62 mois civils.	des risques subséquente dans un délai de plus de 62 mois civils et d'au plus 64 mois civils.	des risques subséquente dans un délai de plus de 64 mois civils et d'au plus 66 mois civils. OU Le *propriétaire d'installation de transport* a effectué une évaluation des risques, mais en omettant l'alinéa 1.2.	une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*, n'a pas effectué d'évaluation des risques subséquente. OU Le *propriétaire d'installation de transport* dont l'évaluation des risques précédente n'a désigné aucun poste de transport qui, s'il devenait inopérant ou était endommagé, pourrait entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*, a effectué une évaluation des risques subséquente dans un

	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-014-1)			
			VSL faible	VSL modérée	VSL élevée	VSL critique
						délai de plus de 66 mois civils. OU Le *propriétaire d'installation de transport* dont l'évaluation des risques précédente n'a désigné aucun poste de transport qui, s'il devenait inopérant ou était endommagé, pourrait entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*, n'a pas effectué d'évaluation des risques subséquente.
E2	**Planification à long terme**	**Moyen**	Le *propriétaire d'installation de transport* a fait vérifier par un tiers indépendant	Le *propriétaire d'installation de transport* a fait vérifier par un tiers indépendant	Le *propriétaire d'installation de transport* a fait vérifier par un tiers indépendant	Le *propriétaire d'installation de transport* a fait vérifier par un tiers indépendant

	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-014-1)			
			VSL faible	VSL modérée	VSL élevée	VSL critique
			l'évaluation des risques effectuée selon l'exigence E1, mais dans un délai de plus de 90 jours civils et d'au plus 100 jours civils suivant la fin de cette évaluation. OU Le *propriétaire d'installation de transport* a fait vérifier par un tiers indépendant l'évaluation des risques effectuée selon l'exigence E1 et a modifié sa désignation découlant de l'exigence E1 ou documenté la justification technique de son refus de le faire, selon l'alinéa 2.3, mais dans un délai de plus de 60 jours civils et d'au plus 70 jours civils	l'évaluation des risques effectuée selon l'exigence E1, mais dans un délai de plus de 100 jours civils et d'au plus 110 jours civils suivant la fin de cette évaluation. OU Le *propriétaire d'installation de transport* a fait vérifier par un tiers indépendant l'évaluation des risques effectuée selon l'exigence E1 et a modifié sa désignation découlant de l'exigence E1 ou documenté la justification technique de son refus de le faire, selon l'alinéa 2.3, mais dans un délai de plus de 70 jours civils et d'au plus 80 jours civils	l'évaluation des risques effectuée selon l'exigence E1, mais dans un délai de plus de 110 jours civils et d'au plus 120 jours civils suivant la fin de cette évaluation. OU Le *propriétaire d'installation de transport* a fait vérifier par un tiers indépendant l'évaluation des risques effectuée selon l'exigence E1 et a modifié sa désignation découlant de l'exigence E1 ou documenté la justification technique de son refus de le faire, selon l'alinéa 2.3, mais dans un délai de plus de 80 jours civils suivant la fin de la	l'évaluation des risques effectuée selon l'exigence E1, mais dans un délai de plus de 120 jours civils suivant la fin de cette évaluation. OU Le *propriétaire d'installation de transport* n'a pas fait vérifier par un tiers indépendant l'évaluation des risques effectuée selon l'exigence E1. OU Le *propriétaire d'installation de transport* a fait vérifier par un tiers indépendant l'évaluation des risques effectuée selon l'exigence E1, mais n'a pas adopté de

	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-014-1)			
			VSL faible	VSL modérée	VSL élevée	VSL critique
			suivant la fin de la vérification.	suivant la fin de la vérification.	vérification. OU Le *propriétaire d'installation de transport* a fait vérifier par un tiers indépendant l'évaluation des risques effectuée selon l'exigence E1, mais n'a ni modifié sa désignation découlant de l'exigence E1, ni documenté la justification technique de son refus de le faire, selon l'alinéa 2.3.	procédures de protection des informations conformément à l'alinéa 2.4.
E3	**Planification à long terme**	**Faible**	Le *propriétaire d'installation de transport* a avisé conformément à l'exigence E3 un *exploitant de réseau de transport* qui exploite un centre de contrôle principal, mais	Le *propriétaire d'installation de transport* a avisé conformément à l'exigence E3 un *exploitant de réseau de transport* qui exploite un centre de contrôle principal, mais	Le *propriétaire d'installation de transport* a avisé conformément à l'exigence E3 un *exploitant de réseau de transport* qui exploite un centre de contrôle principal, mais	Le *propriétaire d'installation de transport* a avisé conformément à l'exigence E3 un *exploitant de réseau de transport* qui exploite un centre de contrôle principal, mais

	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-014-1)			
			VSL faible	VSL modérée	VSL élevée	VSL critique
			dans un délai de plus de 7 jours civils et d'au plus 9 jours civils suivant la fin de la vérification selon l'exigence E2. OU Le *propriétaire d'installation de transport* a avisé l'*exploitant de réseau de transport* qui exploite un centre de contrôle principal pour lui signaler son retrait dans la désignation selon l'exigence E1, mais dans un délai de plus de 7 jours civils et d'au plus 9 jours civils suivant la fin de l'évaluation ou de la vérification en cause.	dans un délai de plus de 9 jours civils et d'au plus 11 jours civils suivant la fin de la vérification selon l'exigence E2. OU Le *propriétaire d'installation de transport* a avisé l'*exploitant de réseau de transport* qui exploite un centre de contrôle principal pour lui signaler son retrait dans la désignation selon l'exigence E1, mais dans un délai de plus de 9 jours civils et d'au plus 11 jours civils suivant la fin de l'évaluation ou de la vérification en cause.	dans un délai de plus de 11 jours civils et d'au plus 13 jours civils suivant la fin de la vérification selon l'exigence E2. OU Le *propriétaire d'installation de transport* a avisé l'*exploitant de réseau de transport* qui exploite un centre de contrôle principal pour lui signaler son retrait dans la désignation selon l'exigence E1, mais dans un délai de plus de 11 jours civils et d'au plus 13 jours civils suivant la fin de l'évaluation ou de la vérification en cause.	dans un délai de plus de 13 jours civils suivant la fin de la vérification selon l'exigence E2. OU Le *propriétaire d'installation de transport* n'a pas avisé un *exploitant de réseau de transport* qui exploite un centre de contrôle principal désigné selon l'exigence E1. OU Le *propriétaire d'installation de transport* a avisé un *exploitant de réseau de transport* qui exploite un centre de contrôle principal pour lui signaler son retrait dans la désignation selon l'exigence E1,

	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-014-1)			
			VSL faible	VSL modérée	VSL élevée	VSL critique
						mais dans un délai de plus de 13 jours civils suivant la fin de l'évaluation ou de la vérification en cause. OU Le *propriétaire d'installation de transport* n'a pas avisé un *exploitant de réseau de transport* qui exploite un centre de contrôle principal pour lui signaler son retrait dans la désignation selon l'exigence E1.
E4	**Planification de l'exploitation, planification à long terme**	**Moyen**	S. O.	L'entité responsable a effectué une évaluation des menaces potentielles d'attaque physique et des vulnérabilités à de telles attaques pour chacun de ses postes de *transport* et centres de contrôle principaux	L'entité responsable a effectué une évaluation des menaces potentielles d'attaque physique et des vulnérabilités à de telles attaques pour chacun de ses postes de *transport* et centres de contrôle principaux	L'entité responsable n'a pas effectué d'évaluation des menaces potentielles d'attaque physique et des vulnérabilités à de telles attaques pour chacun de ses postes de *transport* et centres de contrôle principaux

	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-014-1)			
			VSL faible	VSL modérée	VSL élevée	VSL critique
				désignés selon l'exigence E1, mais a omis un des alinéas 4.1 à 4.3 dans son évaluation.	désignés selon l'exigence E1, mais a omis deux des alinéas 4.1 à 4.3 dans son évaluation.	désignés selon l'exigence E1. OU L'entité responsable a effectué une évaluation des menaces potentielles d'attaque physique et des vulnérabilités à de telles attaques pour chacun de ses postes de *transport* et centres de contrôle principaux désignés selon l'exigence E1, mais a omis les alinéas 4.1 à 4.3 dans son évaluation.
E5	**Planification à long terme**	**Élevé**	L'entité responsable a élaboré et mis en place un ou des plans de sécurité physique documentés pour ses postes de *transport* et centres de contrôle principaux désignés	L'entité responsable a élaboré et mis en place un ou des plans de sécurité physique documentés pour ses postes de *transport* et centres de contrôle principaux désignés	L'entité responsable a élaboré et mis en place un ou des plans de sécurité physique documentés pour ses postes de *transport* et centres de contrôle principaux désignés	L'entité responsable a élaboré et mis en place un ou des plans de sécurité physique documentés pour ses postes de *transport* et centres de contrôle principaux désignés

	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-014-1)			
			VSL faible	VSL modérée	VSL élevée	VSL critique
			selon l'exigence E1, mais dans un délai de plus de 120 jours civils et d'au plus 130 jours civils suivant la fin de la vérification selon l'exigence E2. OU L'entité responsable a élaboré et mis en place un ou des plans de sécurité physique documentés pour ses postes de *transport* et centres de contrôle principaux désignés selon l'exigence E1 et vérifiés selon l'exigence E2, mais a omis un des alinéas 5.1 à 5.4 dans son ou ses plans.	selon l'exigence E1, mais dans un délai de plus de 130 jours civils et d'au plus 140 jours civils suivant la fin de la vérification selon l'exigence E2. OU L'entité responsable a élaboré et mis en place un ou des plans de sécurité physique documentés pour ses postes de *transport* et centres de contrôle principaux désignés selon l'exigence E1 et vérifiés selon l'exigence E2, mais a omis deux des alinéas 5.1 à 5.4 dans son ou ses plans.	selon l'exigence E1, mais dans un délai de plus de 140 jours civils et d'au plus 150 jours civils suivant la fin de la vérification selon l'exigence E2. OU L'entité responsable a élaboré et mis en place un ou des plans de sécurité physique documentés pour ses postes de *transport* et centres de contrôle principaux désignés selon l'exigence E1 et vérifiés selon l'exigence E2, mais a omis trois des alinéas 5.1 à 5.4 dans son ou ses plans.	selon l'exigence E1, mais dans un délai de plus de 150 jours civils suivant la fin de la vérification selon l'exigence E2. OU L'entité responsable n'a ni élaboré ni mis en place de plan de sécurité physique documenté pour ses postes de *transport* et centres de contrôle principaux désignés selon l'exigence E1 et vérifiés selon l'exigence E2. OU L'entité responsable a élaboré et mis en place un ou des plans de sécurité physique documentés pour ses postes de *transport* et centres de contrôle

	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-014-1)			
			VSL faible	VSL modérée	VSL élevée	VSL critique
						principaux désignés selon l'exigence E1 et vérifiés selon l'exigence E2, mais a omis les alinéas 5.1 à 5.4 dans son ou ses plans.
E6	**Planification à long terme**	**Moyen**	L'entité responsable a fait examiner par un tiers indépendant l'évaluation effectuée selon l'exigence E4 et le ou les plans de sécurité élaborés selon l'exigence E5, mais dans un délai de plus de 90 jours civils et d'au plus 100 jours civils. OU L'entité responsable a fait examiner par un tiers indépendant l'évaluation effectuée selon l'exigence E4 et le ou les plans de sécurité	L'entité responsable a fait examiner par un tiers indépendant l'évaluation effectuée selon l'exigence E4 et le ou les plans de sécurité élaborés selon l'exigence E5, mais dans un délai de plus de 100 jours civils et d'au plus 110 jours civils. OU L'entité responsable a fait examiner par un tiers indépendant l'évaluation effectuée selon l'exigence E4 et le ou les plans de sécurité	L'entité responsable a fait examiner par un tiers indépendant l'évaluation effectuée selon l'exigence E4 et le ou les plans de sécurité élaborés selon l'exigence E5, mais dans un délai de plus de 110 jours civils et d'au plus 120 jours civils. OU L'entité responsable a fait examiner par un tiers indépendant l'évaluation effectuée selon l'exigence E4 et le ou les plans de sécurité	L'entité responsable n'a pas fait examiner par un tiers indépendant l'évaluation effectuée selon l'exigence E4 et le ou les plans de sécurité élaborés selon l'exigence E5, dans un délai de plus de 120 jours civils. OU L'entité responsable n'a pas fait examiner par un tiers indépendant l'évaluation effectuée selon l'exigence E4 et le ou les plans de sécurité

	Horizon	VRF	Niveau de gravité de la non-conformité (CIP-014-1)			
			VSL faible	VSL modérée	VSL élevée	VSL critique
			élaborés selon l'exigence E5, et a modifié ce ou ces plans ou documenté les raisons de son refus de le faire, conformément à l'alinéa 6.3, mais dans un délai de plus de 60 jours civils et d'au plus 70 jours civils suivant la fin de l'examen par l'entité examinatrice.	élaborés selon l'exigence E5, et a modifié ce ou ces plans ou documenté les raisons de son refus de le faire, conformément à l'alinéa 6.3, mais dans un délai de plus de 70 jours civils et d'au plus 80 jours civils suivant la fin de l'examen par l'entité examinatrice.	élaborés selon l'exigence E5, et a modifié ce ou ces plans ou documenté les raisons de son refus de le faire, conformément à l'alinéa 6.3, mais dans un délai de plus de 80 jours civils suivant la fin de l'examen par l'entité examinatrice. OU L'entité responsable a fait examiner par un tiers indépendant l'évaluation effectuée selon l'exigence E4 et le ou les plans de sécurité élaborés selon l'exigence E5, mais n'a pas documenté les raisons de son refus de modifier ce ou ces plans, conformément à l'alinéa 6.3.	élaborés selon l'exigence E5. OU L'entité responsable a fait examiner par un tiers indépendant l'évaluation effectuée selon l'exigence E4 et le ou les plans de sécurité élaborés selon l'exigence E5, mais n'a pas adopté de procédures de protection des informations conformément à l'alinéa 6.4.

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	1er octobre 2015	Date d'entrée en vigueur	Nouveau
2	16 avril 2015	Revisée pour répondre à l'ordonnace 802 de la FERC pour enlevé le mot « étendue »	Révision
2	7 mai 2015	Adoption par le Conseil d'administration de la NERC	
2	14 juillet 2015	Ordonnance de la FERC dans le dossier no. RD15-4-000 approuvant CIP-014-2	

Principes directeurs et justification technique

Section 4 – Applicabilité

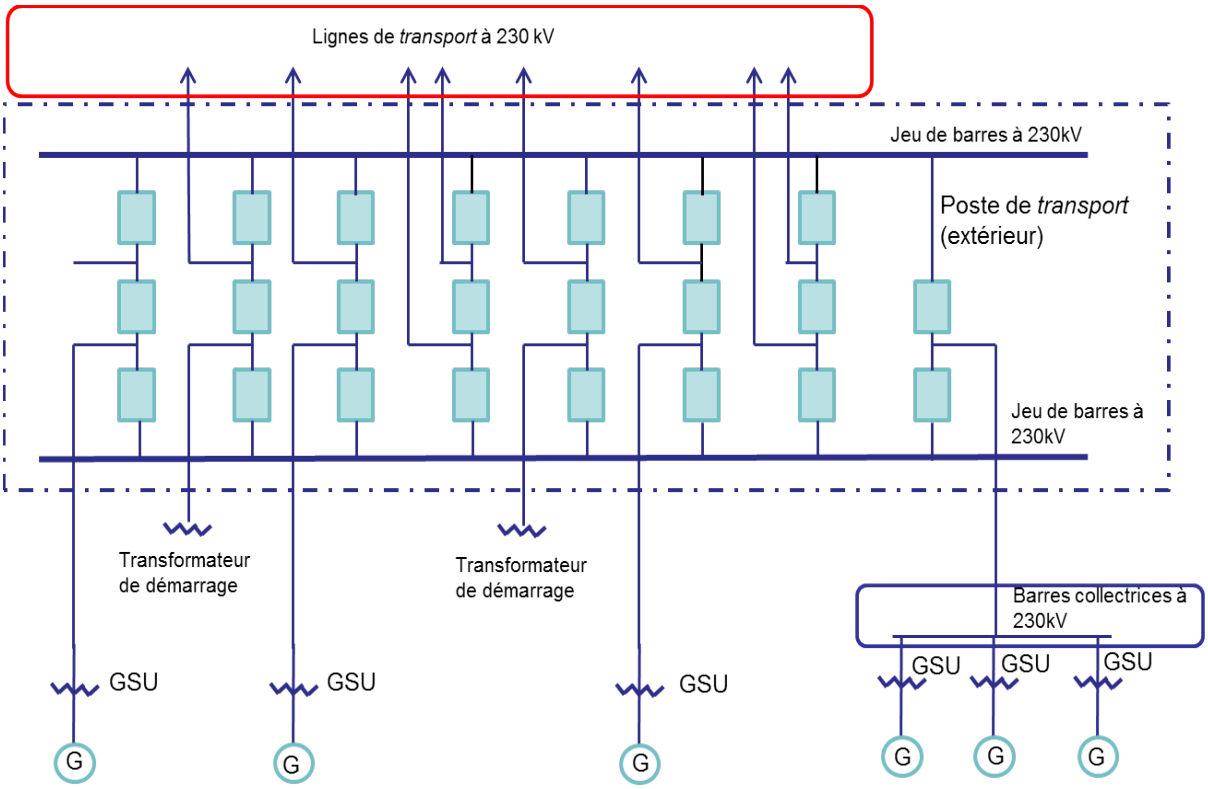
La norme de fiabilité CIP-014 vise la protection des postes de *transport* et des centres de contrôle principaux connexes qui, s'ils devenaient inopérants ou étaient endommagés par suite d'une attaque physique, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*. Afin de circonscrire correctement les entités qui possèdent ou exploitent de telles *installations*, la norme de fiabilité CIP-014 vise d'abord les *propriétaires d'installation de transport* dont certains *installations* répondent aux critères 4.1.1.1 à 4.1.1.4 de la section Applicabilité. Les *installations* définies par ces critères sont les mêmes que celles qui répondent aux critères d'« impact moyen » de l'annexe 1 de la norme de fiabilité CIP-002-5.1. Chaque *propriétaire d'installation de transport* dont certains *installations* de *transport* répondent aux critères 4.1.1.1 à 4.1.1.4 est tenu d'effectuer une évaluation des risques conformément à l'exigence E1 afin de désigner ceux de ces postes de *transport* et des centres de contrôle principaux connexes qui, s'ils devenaient inopérants ou étaient endommagés, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*. L'équipe de rédaction de la norme prévoit que les postes à évaluer seront peu nombreux et que beaucoup de *propriétaires d'installation de transport* visés par la présente norme ne désigneront en fin de compte aucune *installation*. Seuls les *propriétaires d'installation de transport* qui ont désigné un ou des postes de *transport* dans le cadre de l'évaluation des risques (après vérification selon l'exigence E2) sont assujettis aux exigences E3 à E6.

La norme s'applique aussi aux *exploitants de réseau de transport*. Un *exploitant de réseau de transport* n'est toutefois assujetti à la norme que si un *propriétaire d'installation de transport* l'avise, en vertu de l'exigence E3, que l'*exploitant de réseau de transport* exploite un centre de contrôle principal qui exerce le contrôle opérationnel sur un ou des postes de *transport* désignés par l'évaluation des risques de l'exigence E1. Un centre de contrôle principal exerce le contrôle opérationnel sur un poste de *transport* si les actions électroniques du centre de contrôle peuvent commander une action physique directe (par exemple l'ouverture d'un disjoncteur) au poste de *transport* désigné, par opposition à un centre de contrôle qui ne ferait que recevoir de l'information du poste de *transport* et qui devrait coordonner une action directe par l'entremise d'une autre entité. Seuls les *exploitants de réseau de transport* auxquels on notifie qu'ils exercent le contrôle opérationnel sur un ou des centres de contrôle principaux en vertu de la présente norme sont assujettis aux exigences E4 à E6. En somme, un centre de contrôle principal n'est visé par la présente norme que s'il s'agit du centre de contrôle que le *propriétaire d'installation de transport* ou l'*exploitant de réseau de transport*, selon le cas, utilise comme site principal, occupé en permanence par du personnel, pour commander physiquement un poste de *transport* désigné selon l'exigence E1 (après vérification selon l'exigence E2). Les centres de contrôle qui ont un rôle de relève ne sont pas visés, car ils constituent une mesure de résilience et sont volontairement redondants.

L'équipe de rédaction a envisagé plusieurs options pour les critères explicites d'applicabilité permettant de constituer un seuil initial pour définir l'ensemble des postes de *transport* qui correspondent aux prescriptions de l'Ordonnance de la FERC sur la sécurité physique (c'est-à-

dire ceux qui pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*). Selon l'équipe de rédaction, les critères des *installations* de *transport* à impact moyen de l'annexe 1 de la norme CIP-002-5.1 constitueraient un seuil prudent pour définir quels postes de *transport* doivent être soumis à l'évaluation des risques prescrite à l'exigence E1 de la norme CIP-014. L'équipe de rédaction a conclu en outre que l'adoption des critères de la catégorie « impact moyen » de la norme CIP-002-5.1 est appropriée puisque ces critères ont été approuvés par les parties concernées, par la NERC et par la FERC, et que leur utilisation représente une base techniquement solide pour déterminer quels *propriétaires d'installation de transport* doivent procéder à l'évaluation des risques. Comme l'indique la norme CIP-002-5.1, la défaillance d'un poste de *transport* qui appartient à la catégorie « impact moyen » pourrait entraîner le dépassement d'une ou de plusieurs *limites d'exploitation pour la fiabilité de l'Interconnexion* (*IROL*). L'équipe de rédaction reconnaît que l'adoption de ces critères pour déterminer l'applicabilité peut faire en sorte que certains *propriétaires d'installation de transport* devront effectuer des évaluations des risques selon l'exigence E1 pour finalement conclure qu'aucun de leurs postes de *transport* ne représente un risque d'instabilité, de séparation fortuite ou de *déclenchements en cascade* dans une *Interconnexion*. L'équipe de rédaction considère toutefois qu'un critère plus restrictif ne garantirait pas l'inclusion de tous les postes de *transport* et centres de contrôle principaux connexes qui, s'ils devenaient inopérants ou étaient endommagés, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*. D'autres indications et justifications techniques concernant les critères des *installations* à impact moyen figurent dans la section « Principes directeurs et justification technique » de la norme CIP-002-5.1.

En outre, l'équipe de rédaction a jugé inutile d'étendre l'application de la norme de fiabilité aux *exploitants d'installation de production* et aux *propriétaires d'installation de production*. Premièrement, les postes de *transport* servant au raccordement des installations de production sont visés par les critères d'applicabilité ; les *propriétaires d'installation de transport* tiendront donc compte des postes de *transport* situés du côté haute tension des transformateurs élévateurs de groupe de production (GSU) dans le contexte des alinéas 4.1.1.1 et 4.1.1.2 de la section Applicabilité. Par exemple, un poste de *transport* désigné comme une installation de *propriétaire d'installation de transport* qui sert à raccorder des sources de production sera soumis à l'évaluation des risques prescrite à l'exigence E1 s'il est exploité à 500 kV ou plus ou s'il est raccordé entre 200 kV et 499 kV à au moins trois autres postes de *transport* et s'il a une « valeur pondérée combinée » de plus de 3 000 selon le tableau de l'alinéa 4.1.1.2 de la section Applicabilité. Deuxièmement, l'analyse du réseau de *transport* ou les analyses effectuées selon l'exigence E1 devraient tenir compte de l'impact de la perte de la production raccordée aux postes de *transport* visés. En outre, l'Ordonnance de la FERC ne mentionne pas explicitement les actifs de production, et l'on peut raisonnablement comprendre qu'elle vise essentiellement les *installations* de *transport* les plus critiques. Le schéma ci-dessous montre un exemple de poste.



Il est à noter que dans l'expression « postes de *transport* », l'équipe de rédaction utilise le mot « poste » pour recouvrir à la fois le champ sémantique les termes anglais « station » et « substation » (Le terme « substation » est souvent utilisé dans l'industrie pour désigner un emplacement qui contient au moins un autotransformateur. Il existe des emplacements qui ne contiennent pas d'autotransformateur, et de nombreuses entités de l'industrie se réfèrent à ces endroits avec le terme « station » (poste électriques sans autotransformateur). Par conséquent, l'équipe de rédaction a choisi d'utiliser à la fois « station » et « substation » pour désigner les endroits où existent des installations de transport.

Pour ce qui est des situations de propriété commune, l'équipe de rédaction considère que cet enjeu n'est pas exclusif à la norme CIP-014 ; elle s'attend à ce que les *propriétaires d'installation de transport* et les *exploitants de réseau de transport* en cause, lorsqu'il y a propriété commune, établissent entre eux des protocoles d'entente, des inscriptions coordonnées au registre des entités visées, des procédures ou d'autres ententes afin d'établir les responsabilités dans le cadre de la norme CIP-014, comme le font déjà de nombreuses entités dans le cadre d'autres normes de fiabilité.

Le texte de la section applicabilité concernant le jeu de barres collectrices est repris directement tel quel de l'annexe 1 de la norme CIP-002-5.1, et n'a pas de signification supplémentaire dans le contexte de la norme CIP-014.

Exigence E1

L'évaluation des risques initiale prescrite à l'exigence E1 doit être terminée au plus tard à la date d'entrée en vigueur de la norme. Les évaluations des risques subséquentes doivent être

effectuées à intervalles de 30 ou de 60 mois, d'après les résultats de l'évaluation des risques précédente, comme l'indique l'alinéa 1.1 de l'exigence E1. Avant d'entreprendre l'évaluation des risques prescrite à l'exigence E1, le *propriétaire d'installation de transport* doit d'abord déterminer quels sont les postes de *transport* visés, selon les critères de l'alinéa 4.1.1 de la section Applicabilité. L'évaluation des risques consiste ensuite à analyser le réseau de transport afin de déterminer si certains des postes de *transport* visés, s'ils devenaient inopérants ou étaient endommagés, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*. L'exigence ne consiste pas à exiger la désignation d'un poste de *transport* – et par conséquent ne vise pas à assujettir celui-ci à la norme – à moins que le *propriétaire d'installation de transport* visé n'ait déterminé (au moyen d'études et d'analyses techniques fondées sur une analyse objective, une expertise technique, l'historique d'exploitation et un jugement averti) que la perte de cette installation, si celle-ci devenait inopérante ou était endommagée, aurait des conséquences graves sur le fonctionnement de l'*interconnexion*. Dans son ordonnance du 20 novembre 2014, la FERC a réitéré que « seule une instabilité ayant des "conséquences graves sur le fonctionnement de l'interconnexion" justifie que l'installation ayant causé cette instabilité soit désignée selon l'exigence E1 ». Le *propriétaire d'installation de transport* peut déterminer ce qui constitue une conséquence grave en ayant recours, entre autres, aux critères suivants :

- les critères ou la méthodologie utilisés par les *planificateurs de réseau de transport* ou les *responsables de la planification* en vertu de l'exigence E6 de la norme TPL-001-4 ;
- les critères de déclaration selon la norme NERC EOP-004-2 ;
- l'étendue ou l'importance des conséquences.

La norme n'impose pas une méthode d'analyse particulière pour l'évaluation des risques ; le *propriétaire d'installation de transport* est libre de choisir la méthode qui lui convient le mieux, par exemple une analyse de transit de puissance et une analyse de stabilité à divers niveaux de charge.

Exécution de l'évaluation des risques

Le *propriétaire d'installation de transport* est libre de choisir la méthode d'analyse du réseau de transport qui convient le mieux à sa situation et aux particularités de son réseau. L'imposition d'une méthode particulière n'est pas techniquement souhaitable, et pourrait en fait empêcher de prendre en compte adéquatement les particularités régionales et topologiques ainsi que le contexte d'exploitation du réseau. Les indications qui suivent ne sont qu'un exemple de la manière dont un *propriétaire d'installation de transport* peut effectuer une analyse de transit de puissance ou de stabilité afin de désigner les postes de *transport* qui, s'ils devenaient inopérants ou étaient endommagés par suite d'une attaque physique, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*. Ainsi, l'entité pourrait simuler le débranchement de toutes les lignes, quel que soit leur niveau de tension, à un poste de *transport* donné, puis évaluer le comportement du réseau afin de déterminer s'il risque d'en résulter des *déclenchements en cascade* d'*installations* de *transport*, une séparation fortuite ou encore une instabilité en tension ou en fréquence dans une portion importante de l'*Interconnexion*. En s'appuyant sur son meilleur jugement technique,

le *propriétaire d'installation de transport* (éventuellement en consultation avec les comités régionaux de planification ou d'exploitation ou avec le comité pertinent de son centre d'exploitation indépendant ou organisme de transport régional) devrait établir des critères (par exemple un défaut près du poste de *transport* débranché) permettant de définir une contingence ou des paramètres qui entraîneraient une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*. Une consultation régionale sur ces questions serait sans doute utile et instructive, puisque les avis sur l'évaluation des risques et sur les traits qui caractérisent une instabilité, une séparation fortuite ou des déclenchements en cascade dans une Interconnexion varieront probablement d'une région à l'autre ou d'un centre d'exploitation indépendant à l'autre selon la topologie, les caractéristiques et la configuration du réseau. Les critères utilisés pourraient aussi comprendre des charges postcontingences supérieures à une certaine caractéristique assignée en situation d'urgence ou la non-convergence d'un scénario de transit de puissance. Les automatismes de réseau présents, le cas échéant, pourraient être mis à contribution pour déterminer si le réseau éprouve des instabilités supplémentaires pouvant entraîner une séparation fortuite. Exemples de critères utilisables :

(a) surcharges thermiques supérieures aux caractéristiques assignées en situation d'urgence des installations ;

(b) écart de tension au-delà de ±10 % ; ou

(c) interruptions ou effondrements de tension en cascade ; ou

(d) baisse de fréquence en deçà des seuils de délestage en sous-fréquence.

Périodicité

Un *propriétaire d'installation de transport* qui détermine qu'un ou plusieurs de ses postes de *transport* (après vérification selon l'exigence E2), s'ils devenaient inopérants ou étaient endommagés par suite d'une attaque physique, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*, doit effectuer une évaluation des risques au moins une fois tous les 30 mois ; avec une telle périodicité, l'évaluation des risques demeure à jour par rapport aux conditions et aux configurations projetées dans le réseau planifié. Ces évaluations des risques subséquentes, tout comme l'évaluation initiale, doivent englober les postes de *transport* dont l'entrée en service est prévue au cours des 24 mois suivants. L'intervalle de 30 mois s'harmonise avec le délai de mise en service de 24 mois, car il donne au *propriétaire d'installation de transport* la latitude voulue pour faire mieux concorder ces dates, selon son cycle de planification et la fréquence à laquelle il peut projeter de construire de nouveaux postes de *transport*. La périodicité prescrite est d'au moins une fois tous les 30 mois ; ainsi, si un *propriétaire d'installation de transport* juge plus approprié d'effectuer une évaluation des risques à intervalles de 24 mois compte tenu de son cycle de planification, il a la latitude pour le faire.

Les *propriétaires d'installation de transport* qui n'ont pas désigné (après vérification selon l'exigence E2) de postes de *transport* qui, s'ils devenaient inopérants ou étaient endommagés par suite d'une attaque physique, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*, ne constateront probablement pas

de changement dans leur évaluation des risques sur l'*horizon de planification à court terme*. C'est pourquoi la périodicité des évaluations des risques subséquentes est de 60 mois dans leur cas.

Désignation du centre de contrôle principal

Une fois terminée l'évaluation des risques selon l'exigence E1, il importe de connaître le centre de contrôle principal qui exerce le contrôle opérationnel sur chaque poste de *transport* qui, s'il devenait inopérant ou était endommagé par suite d'une attaque physique, pourrait entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*. Un centre de contrôle principal « exerce le contrôle opérationnel » sur un poste de *transport* si ses actions électroniques peuvent commander des actions physiques directes au poste de *transport* désigné, par exemple l'ouverture d'un disjoncteur.

Exigence E2

Cette exigence stipule que l'évaluation des risques effectuée selon l'exigence E1 doit être vérifiée par une entité autre que le propriétaire ou l'exploitant qui a effectué l'évaluation des risques en question.

La vérification de l'évaluation des risques par un tiers indépendant, selon l'exigence E2, pourrait porter sur les points suivants :

1. Confirmation que l'évaluation des risques effectuée selon l'exigence E1 portait bien sur tous les postes de *transport* qui répondent aux critères de l'alinéa 4.1.1 de la section Applicabilité.
2. Examen du modèle utilisé pour l'évaluation des risques afin de confirmer qu'il contient des données de topologie de réseau suffisantes pour permettre de désigner les postes de *transport* qui, s'ils devenaient inopérants ou étaient endommagés par suite d'une attaque physique, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*.
3. Examen de la méthodologie de l'évaluation des risques selon l'exigence E1.

Cette exigence offre au *propriétaire d'installation de transport* la liberté de choisir parmi des entités indépendantes, inscrites ou non au registre, ayant de l'expérience en planification ou en analyse du transport de l'électricité, pour vérifier l'évaluation des risques effectuée selon l'exigence E1. Le mot « indépendant » signifie que l'entité vérificatrice ne peut pas être une société affiliée (elle ne doit pas être une entité qui contrôle le *propriétaire d'installation de transport*, qui est contrôlée par celui-ci ou qui est sous contrôle commun). L'entité vérificatrice ne peut pas non plus être une division du *propriétaire d'installation de transport* qui est exploitée à la manière d'une unité fonctionnelle.

L'interdiction imposée aux entités inscrites au registre de choisir une société affiliée pour la vérification n'interdit cependant pas à une entité gouvernementale (ville, municipalité, agence fédérale américaine de commercialisation d'électricité ou toute autre subdivision politique d'un gouvernement fédéral, d'État ou provincial au Canada ou aux États-Unis) de choisir comme entité vérificatrice une autre entité gouvernementale à l'intérieur de la même subdivision

politique. Par exemple, une agence fédérale américaine de commercialisation d'électricité peut choisir comme entité vérificatrice une autre agence fédérale américaine, pourvu que celle-ci ait de l'expérience en planification ou en analyse du transport de l'électricité. De même, un *propriétaire d'installation de transport* qui est la propriété d'une province canadienne peut choisir un autre organisme de la même province pour effectuer la vérification. L'entité vérificatrice doit néanmoins être une entité bien distincte ; elle ne peut pas être une division de l'entité inscrite au registre qui est exploitée à la manière d'une unité fonctionnelle.

L'exigence E2 stipule aussi que la « vérification peut avoir lieu pendant ou après l'évaluation en question ». Cette disposition vise à donner au *propriétaire d'installation de transport* la possibilité de travailler avec l'entité vérificatrice tout au long de l'évaluation des risques (donc simultanément à celle-ci), ce qui, pour certains *propriétaires d'installation de transport*, peut être plus commode et plus efficace. Autrement dit, le *propriétaire d'installation de transport* pourrait collaborer avec son entité vérificatrice indépendante pour effectuer l'évaluation des risques de manière à satisfaire en même temps aux exigences E1 et E2. L'exigence E2 vise essentiellement à ce qu'une entité autre que le propriétaire ou l'exploitant de l'installation soit associée au processus d'évaluation des risques et ait l'occasion de donner son avis. Cette exigence laisse aux entités la liberté de choisir entre un processus en deux étapes successives (le *propriétaire d'installation de transport* évalue les risques lui-même, puis l'entité indépendante procède à la vérification) ou en une seule étape (les deux entités collaborent à l'évaluation des risques).

Les critères du choix de l'entité vérificatrice seraient notamment les suivants :

- *entité visée* inscrite au registre pour les fonctions de planification et de fiabilité pertinentes ;
- expérience en matière d'études et de planification de réseau électrique ;
- compréhension des normes MOD, des normes TPL et des caractéristiques assignées d'installation dans le contexte des études de planification ;
- familiarité avec l'*Interconnexion* dans laquelle le *propriétaire d'installation de transport* est situé.

Quant à l'exigence faite aux *propriétaires d'installation de transport* d'adopter des procédures pour protéger les informations sensibles ou confidentielles, le *propriétaire d'installation de transport* pourrait avoir une méthode permettant de désigner les documents qui doivent faire l'objet d'un traitement confidentiel. Un mécanisme possible pour protéger les informations sensibles ou confidentielles consisterait à interdire de les sortir des locaux du *propriétaire d'installation de transport*. Ce dernier pourrait incorporer une telle interdiction à une entente de non-divulgation signée par l'entité vérificatrice.

Une étude de faisabilité technique n'est pas exigée, dans le cadre de l'exigence E2, pour justifier le refus de modifier la désignation selon la recommandation de l'entité vérificatrice.

Afin de préciser la différence entre l'entité vérificatrice de l'exigence E2 et l'entité examinatrice de l'exigence E6, l'équipe de rédaction indique que l'entité vérificatrice a pour mandat de confirmer que l'évaluation des risques est conforme à l'exigence E1 (notamment pour le

nombre de postes de *transport* désignés), tandis que l'entité examinatrice de l'exigence E6 porte un jugement expert sur la manière dont l'évaluation des menaces prescrite à l'exigence E4 a été effectuée ainsi que sur le plan de sécurité physique prescrit à l'exigence E5. Dans le contexte de l'exigence E6, il n'est pas question de vérifier une analyse technique, mais plutôt de faire jouer expérience et expertise afin de fournir des indications ou des recommandations si nécessaire.

Les alinéas 2.4 et 6.4 exigent que des procédures soient adoptées pour protéger les informations sensibles ou confidentielles. Ces procédures peuvent comprendre les éléments suivants :

1. contrôler et conserver sur place l'information consultable par l'entité vérificatrice ou examinatrice ;
2. restreindre l'information aux personnes qui ont vraiment besoin d'en prendre connaissance ;
3. marquer les documents comme étant confidentiels ;
4. tenir l'information en lieu sûr et la détruire lorsqu'elle n'est plus nécessaire ;
5. ne pas laisser l'information sortir des locaux de l'entité sans l'approbation du chef des Services juridiques, par exemple.

Exigence E3

La norme impose à certains *exploitants de réseau de transport* des obligations à l'endroit de certains centres de contrôle principaux. Ces obligations sont cependant conditionnelles aux conclusions de l'évaluation des risques effectuée par le *propriétaire d'installation de transport* selon l'exigence E1, puis vérifiée selon l'exigence E2. L'exigence E3 stipule qu'un *exploitant de réseau de transport* qui exerce le contrôle opérationnel sur un centre de contrôle principal désigné selon l'exigence E1 doit en être avisé afin de pouvoir s'acquitter des obligations énoncées aux exigences E4 à E6. Comme ces obligations prévoient des délais qui commencent à courir après l'étape de l'exigence E2, le *propriétaire d'installation de transport* doit aussi préciser dans sa notification la date de fin de la vérification selon l'exigence E2. De même, le *propriétaire d'installation de transport* doit aviser l'*exploitant de réseau de transport* de tout retrait d'un poste de la désignation par suite d'une évaluation des risques subséquents selon l'exigence E1 ou de sa vérification selon l'exigence E2.

Exigence E4

Cette exigence demande aux propriétaires et aux exploitants d'installations désignées par l'évaluation des risques effectuée selon l'exigence E1 et vérifiée selon l'exigence E2 d'effectuer une évaluation des menaces potentielles et des vulnérabilités relatives aux postes de *transport* et aux centres de contrôle principaux ainsi désignés, compte tenu des particularités de chaque installation. Les menaces et les vulnérabilités peuvent varier d'une installation à l'autre selon divers facteurs, par exemple l'emplacement, la taille, la fonction, les protections de sécurité physique existantes et l'attractivité de l'installation comme cible.

Dans le cadre de l'analyse des menaces et vulnérabilités, le propriétaire de l'installation est souvent le mieux placé pour déterminer les vulnérabilités propres au site ; par contre, la détermination de l'origine et de l'évolution des menaces relève davantage d'autres intervenants dans les domaines du renseignement et de la police. Le texte de la norme mentionne diverses ressources, mais il en existe beaucoup d'autres, et les propriétaires d'installations ont toute liberté pour s'adresser à celles de leur choix. Autres ressources possibles : les centres de fusion locaux ou d'État, le département de la Sécurité intérieure des États-Unis, le FBI, Sécurité publique Canada, la Gendarmerie royale du Canada et les chapitres InfraGard coordonnés par le FBI.

L'entité responsable doit prendre en compte certains facteurs, énoncés aux alinéas 4.1 à 4.3, afin d'effectuer une évaluation des risques conforme à l'exigence E4.

Afin d'aider à déterminer les menaces courantes applicables à une installation et à évaluer leur probabilité, il convient d'étudier l'historique des attaques visant des installations ayant une protection semblable.

Les ressources suivantes pourront être utiles pour l'analyse des menaces et vulnérabilités :

- *NERC Security Guideline for the Electricity Sector: Physical Securit ;*
- *NERC Security Guideline: Physical Security Response* ;
- ASIS International *General Risk Assessment Guideline* ;
- ASIS International *Facilities Physical Security Measures Guideline* ;
- ASIS International *Security Management Standard: Physical Asset Protection* ;
- *Whole Building Design Guide: Threat/Vulnerability Assessments.*

Exigence E5

Cette exigence demande d'élaborer et de mettre en place un ou des plans de sécurité visant à protéger contre les attaques les installations désignées selon l'exigence E1, d'après l'évaluation effectuée selon l'exigence E4.

L'exigence E5 spécifie les éléments suivants à intégrer au plan de sécurité physique :

- *Mesures de résilience ou de sécurité conçues collectivement pour prévenir, détecter, retarder, évaluer, communiquer et contrer les menaces et vulnérabilités physiques potentielles inventoriées selon l'exigence E4*.

  Les mesures de résilience peuvent comprendre notamment :

  a. des changements dans la topologie du réseau ;

  b. des équipements de relève ;

  c. la construction d'un nouveau poste de *transport*.

  Bien que la plupart des mesures de sécurité agissent collectivement pour sécuriser l'ensemble du site, certaines mesures peuvent cibler des composants critiques particuliers. Par exemple, si une protection contre les tirs d'arme à feu est jugée

nécessaire, on peut limiter cette protection aux composants critiques plutôt que de l'aménager pour l'ensemble du site.

- *Informations de contact des autorités policières et de coordination avec celles-ci.*

  Exemples de telles informations : affichages 9-1-1 pour les appels d'urgence et formation en sécurité des postes électriques pour les autorités policières locales et fédérales, les services d'incendie et les services médicaux d'urgence.

- *Délais d'exécution des mesures de renforcement de la sécurité physique et autres modifications énoncées dans le plan de sécurité physique.*

  Les entités sont libres de prioriser (en fonction du risque, des ressources ou d'autres facteurs) la mise en œuvre des diverses améliorations à la résilience et à la sécurité définies dans leur plan de sécurité. Les délais à spécifier dans le plan de sécurité physique selon l'alinéa 5.3 pour l'exécution des mesures de renforcement de la sécurité physique et autres modifications ne sont pas liés au délai de 120 jours prescrit pour l'élaboration du plan ; les délais d'exécution peuvent dépasser 120 jours, selon l'ampleur des travaux à effectuer.

- *Dispositions prévoyant un suivi de l'évolution des menaces physiques pour les postes de* transport *ou les centres de contrôle principaux, ainsi que des mesures de sécurité correspondantes.*

  Le plan de sécurité physique d'une entité inscrite au registre doit prévoir des processus et des responsabilités pour le suivi des alertes, renseignements et avis de menace provenant de diverses sources, par exemple l'organisation de fiabilité du service d'électricité, l'ES-ISAC et des organismes fédéraux du Canada ou des agences fédérales des États-Unis. L'ensemble de ces informations servira à réévaluer, en vue de les modifier éventuellement, le plan de sécurité élaboré selon l'exigence E5 ainsi que les mesures de sécurité correspondantes.

  Les changements apportés au plan de sécurité physique, au fur et à mesure, avant l'examen indépendant suivant selon l'exigence E6 ne nécessitent pas d'examen supplémentaire par un tiers.

Exigence E6

Cette exigence stipule que l'évaluation effectuée selon l'exigence E4 et le ou les plans de sécurité élaborés selon l'exigence E5 doivent être examinés par une entité autre que le *propriétaire d'installation de transport* ou l'*exploitant de réseau de transport*, et que cette entité doit avoir une expertise appropriée. De même que pour l'exigence E2, le mot « indépendant » signifie que l'entité examinatrice indépendante ne peut pas être une société affiliée (l'entité examinatrice indépendante ne doit pas être une entité qui contrôle l'*exploitant de réseau de transport*, qui est contrôlé par celui-ci ou qui est sous contrôle commun). L'entité vérificatrice indépendante ne peut pas non plus être une division de l'*exploitant de réseau de transport* qui est exploitée à la manière d'une unité fonctionnelle.

De même que pour l'exigence E2, l'interdiction imposée aux entités inscrites au registre de choisir une société affiliée pour l'examen n'interdit cependant pas à une entité gouvernementale de choisir comme entité examinatrice indépendante une autre entité gouvernementale à l'intérieur de la même subdivision politique. Par exemple, une ville ou une municipalité peut recourir aux services de police locaux, pourvu que ceux-ci répondent aux critères de l'exigence E6. L'entité examinatrice doit néanmoins être une entité bien distincte ; elle ne peut pas être une division de l'entité inscrite au registre qui est exploitée à la manière d'une unité fonctionnelle.

L'entité responsable peut choisir l'entité examinatrice parmi plusieurs entités possibles :

- *Une entité ou organisation ayant de l'expérience en matière de sécurité physique dans l'industrie électrique, et dont le personnel d'examen compte au moins un titulaire de certification CPP (Certified Protection Professional) ou PSP (Physical Security Professional).*

  Si les certifications CPP ou PSP sont exigées dans le cadre de la norme, c'est que l'équipe de rédaction juge important que toute entité privée (par exemple une firme d'experts-conseils ou de sécurité) choisie pour effectuer l'examen par un tiers puisse démontrer de façon convaincante sa compétence pour réaliser un tel examen. Les compétences exigées comprennent de l'expérience en sécurité physique dans l'industrie électrique ainsi que l'une ou l'autre des certifications d'ASIS International les plus respectées dans l'industrie de la sécurité. Le programme de certification d'ASIS a été créé en 1977 ; les titulaires de la certification CPP sont dûment certifiés en gestion de la sécurité, tandis que les titulaires de la certification PSP le sont en sécurité physique.

- *Une entité ou organisation agréée par l'organisation de fiabilité du service d'électricité (*ERO*).*

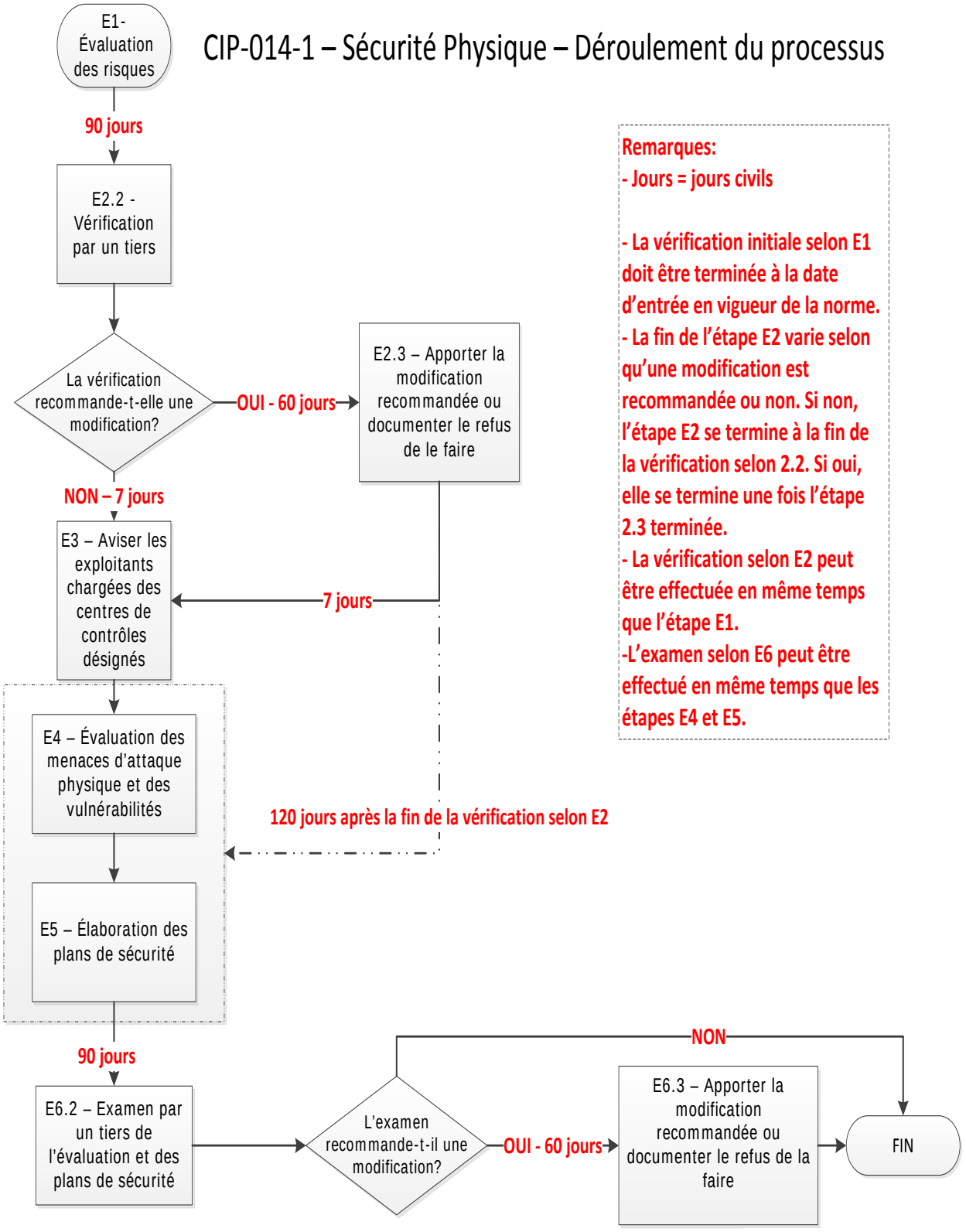
- *Un organisme gouvernemental ayant de l'expertise en sécurité physique.*

- *Une entité ou organisation ayant une expertise confirmée en sécurité physique dans un cadre policier, gouvernemental ou militaire.*

De même que pour l'exigence E2, l'exigence E6 stipule que l'« examen peut avoir lieu pendant ou après l'évaluation effectuée selon l'exigence E4 et l'élaboration du ou des plans de sécurité selon l'exigence E5 ». Cette disposition vise à donner au *propriétaire d'installation de transport* et à l'*exploitant de réseau de transport* la possibilité de travailler avec l'entité examinatrice tout au long de l'évaluation selon l'exigence E4 et de l'élaboration de plans de sécurité selon l'exigence E5 (donc simultanément à ces processus), ce qui, pour certaines entités responsables, peut être plus commode et plus efficace. Autrement dit, le *propriétaire d'installation de transport* ou l'*exploitant de réseau de transport* pourrait collaborer avec son entité examinatrice pour effectuer l'évaluation des menaces potentielles et vulnérabilités (exigence E4) et pour élaborer le ou les plans de sécurité (exigence E5) de manière à satisfaire en même temps aux exigences E4 à E6. L'exigence E6 vise essentiellement à ce qu'une entité autre que le propriétaire ou l'exploitant de l'installation soit associée aux processus d'évaluation selon l'exigence E4 et d'élaboration de plans de sécurité selon l'exigence E5 et ait l'occasion de donner son avis sur ces processus. L'exigence E6 laisse aux

entités la liberté de choisir entre un processus en deux étapes successives (le *propriétaire d'installation de transport* effectue l'évaluation et élabore le plan de sécurité lui-même, puis l'entité indépendante procède à la vérification) ou en une seule étape (les deux entités collaborent à l'évaluation et à l'élaboration du plan de sécurité).

Calendrier


CIP-014-1 – Sécurité Physique – Déroulement du processus
E1- Évaluation des risques
90 jours
E2.2 - Vérification par un tiers
La vérification recommande-t-elle une modification?
OUI - 60 jours
E2.3 – Apporter la modification recommandée ou documenter le refus de le faire
NON – 7 jours
E3 – Aviser les exploitants chargées des centres de contrôles désignés
7 jours
E4 – Évaluation des menaces d'attaque physique et des vulnérabilités
120 jours après la fin de la vérification selon E2
E5 – Élaboration des plans de sécurité
90 jours
E6.2 – Examen par un tiers de l'évaluation et des plans de sécurité
L'examen recommande-t-il une modification?
NON
OUI - 60 jours
E6.3 – Apporter la modification recommandée ou documenter le refus de la faire
FIN
Remarques:
- Jours = jours civils
- La vérification initiale selon E1 doit être terminée à la date d'entrée en vigueur de la norme.
- La fin de l'étape E2 varie selon qu'une modification est recommandée ou non. Si non, l'étape E2 se termine à la fin de la vérification selon 2.2. Si oui, elle se termine une fois l'étape 2.3 terminée.
- La vérification selon E2 peut être effectuée en même temps que l'étape E1.
-L'examen selon E6 peut être effectué en même temps que les étapes E4 et E5.

Justifications

Pendant l'élaboration de la norme, des zones de texte ont été incorporées à celle-ci pour exposer la justification de ses diverses parties. Après l'approbation par le Conseil d'administration, le contenu de ces zones de texte a été transféré ci-après.

Justification de l'exigence E1

Cette exigence répond à la prescription du paragraphe 6 de la directive du 7 mars 2014 de la FERC portant sur la sécurité physique, qui demande une évaluation des risques afin de désigner les installations qui, si elles devenaient inopérantes ou étaient endommagées par suite d'une attaque physique, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade*. L'exigence ne vise pas à assujettir un poste de *transport* à la norme à moins que le *propriétaire d'installation de transport* visé n'ait déterminé (au moyen d'études et d'analyses techniques fondées sur une analyse objective, une expertise technique, l'historique d'exploitation et un jugement averti) que la perte de cette installation, si celle-ci devenait inopérante ou était endommagée, aurait des conséquences graves sur le fonctionnement de l'*interconnexion*. Dans son ordonnance du 20 novembre 2014, la FERC a réitéré que « seule une instabilité ayant des "conséquences graves sur le fonctionnement de l'interconnexion" justifie que l'installation ayant causé cette instabilité soit désignée selon l'exigence E1 ». Le *propriétaire d'installation de transport* peut déterminer ce qui constitue une conséquence grave en ayant recours, entre autres, aux critères suivants :

- les critères ou la méthodologie utilisés par les *planificateurs de réseau de transport* ou les *responsables de la planification* en vertu de l'exigence E6 de la norme TPL-001-4 ;
- les critères de déclaration selon la norme NERC EOP-004-2 ;
- l'étendue ou l'importance des conséquences.

L'exigence E1 répond aussi à une prescription de la FERC qui demande une réévaluation périodique, en exigeant que l'évaluation des risques soit effectuée tous les 30 mois (ou tous les 60 mois pour une entité qui n'a pas désigné dans une évaluation des risques précédente de postes de *transport* qui, s'ils devenaient inopérants ou étaient endommagés par suite d'une attaque physique, pourraient entraîner une instabilité, une séparation fortuite ou des *déclenchements en cascade* dans une *Interconnexion*).

Après avoir désigné chaque poste de *transport* qui répond aux critères de l'exigence E1, il importe en outre de désigner le centre de contrôle principal qui exerce le contrôle opérationnel sur le poste de *transport* en question, c'est-à-dire le centre de contrôle dont les actions électroniques peuvent commander une action physique directe (par exemple l'ouverture d'un disjoncteur) au poste de *transport* désigné, par opposition à un centre de contrôle qui ne ferait que surveiller le poste de *transport* et qui devrait coordonner une action directe par l'entremise d'une autre entité.

Justification de l'exigence E2

Cette exigence répond à la prescription du paragraphe 11 de la directive de la FERC portant sur la sécurité physique, qui demande une vérification, par une entité autre que le propriétaire ou l'exploitant, de l'évaluation des risques effectuée selon l'exigence E1.

Cette exigence offre au *propriétaire d'installation de transport* la liberté de choisir parmi des entités (inscrites ou non au registre) ayant de l'expérience en planification ou en analyse du transport de l'électricité pour vérifier l'évaluation des risques effectuée selon l'exigence E1. Le mot « indépendant » signifie que l'entité vérificatrice ne peut pas être une société affiliée (entité qui contrôle le *propriétaire d'installation de transport*, qui est contrôlée par celui-ci ou qui est sous contrôle commun). L'entité vérificatrice ne peut pas non plus être une division du *propriétaire d'installation de transport* qui est exploitée à la manière d'une unité fonctionnelle. Le mot « indépendant » ne vise cependant pas à interdire à une entité gouvernementale de choisir une autre entité gouvernementale comme entité vérificatrice dans le cadre de l'exigence E2.

L'exigence E2 vise aussi à donner au *propriétaire d'installation de transport* la possibilité de travailler avec l'entité vérificatrice tout au long de l'évaluation des risques prescrite à l'exigence E1 – ce qui, pour certains *propriétaires d'installation de transport*, peut être plus commode et plus efficace. Autrement dit, le *propriétaire d'installation de transport* pourrait collaborer avec son entité vérificatrice pour effectuer l'évaluation des risques de manière à satisfaire en même temps aux exigences E1 et E2.

Le *coordonnateur de la planification* est une des entités fonctionnelles indiquées à l'alinéa 2.1. Il convient de rappeler que le *coordonnateur de la planification* et le *responsable de la planification* représentent la même entité, comme l'indique le « Glossaire des termes et des acronymes relatifs aux normes de fiabilité ».

Justification de l'exigence E3

La norme impose à certains *exploitants de réseau de transport* des obligations à l'endroit de certains centres de contrôle principaux. Cependant, le *propriétaire d'installation de transport* doit d'abord désigner les postes de *transport* en procédant à l'évaluation des risques prescrite à l'exigence E1, puis faire vérifier cette évaluation selon l'exigence E2. L'exigence E3 vise à faire en sorte qu'un *exploitant de réseau de transport* qui exerce le contrôle opérationnel sur un centre de contrôle principal désigné selon l'alinéa 1.2 de l'exigence E1 en soit avisé afin de pouvoir satisfaire aux exigences E4 à E6 dans les délais qui y sont prescrits. Comme ces délais commencent à courir après l'étape de l'exigence E2, le *propriétaire d'installation de transport* doit aussi préciser dans sa notification la date de fin de la vérification selon l'exigence E2. De même, le *propriétaire d'installation de transport* doit aviser l'*exploitant de réseau de transport* de tout retrait d'un poste de la désignation par suite d'une évaluation des risques subséquente selon l'exigence E1 ou de sa vérification selon l'exigence E2.

Justification de l'exigence E4

Cette exigence répond à la prescription du paragraphe 8 de la directive de la FERC portant sur la sécurité physique, qui demande une évaluation adaptée des menaces potentielles et des

vulnérabilités relatives aux installations désignées selon l'exigence E1, après vérification selon l'exigence E2. Les menaces et les vulnérabilités peuvent varier d'une installation à l'autre selon divers facteurs, par exemple l'emplacement, la taille et la fonction de l'installation, les protections existantes et l'attractivité de l'installation comme cible. C'est pourquoi l'exigence E4 n'impose pas une démarche uniforme, mais demande au contraire de tenir compte des particularités de chaque installation.

L'exigence E4 ne précise pas de délai pour l'évaluation des menaces et des vulnérabilités. Cependant, l'exigence E5 stipule que le ou les plans de sécurité, élaborés à partir de l'évaluation selon l'exigence E4, doivent être prêts dans les 120 jours civils suivant la fin de la vérification selon l'exigence E2. L'entité dispose donc d'une certaine latitude temporelle pour son évaluation selon l'exigence E4, pourvu que cette évaluation soit terminée à temps pour permettre d'élaborer le ou les plans de sécurité physique prescrits à l'exigence E5 dans le délai de 120 jours civils précité.

Justification de l'exigence E5

Cette exigence répond à la prescription du paragraphe 9 de la directive de la FERC portant sur la sécurité physique, qui demande l'élaboration et la mise en place de plans de sécurité visant à protéger contre les attaques les installations désignées selon l'exigence E1, d'après l'évaluation effectuée selon l'exigence E4.

Justification de l'exigence E6

Cette exigence répond à la prescription du paragraphe 11 de la directive de la FERC portant sur la sécurité physique, qui demande que l'évaluation effectuée selon l'exigence E4 et le ou les plans de sécurité élaborés selon l'exigence E5 soient examinés par un tiers indépendant du propriétaire ou de l'exploitant et ayant une expertise appropriée.

De même que pour l'exigence E2, l'exigence E6 offre au *propriétaire d'installation de transport* ou à l'*exploitant de réseau de transport* la possibilité de travailler avec l'entité examinatrice tout au long de l'évaluation effectuée selon l'exigence E4 et de l'élaboration de plans de sécurité selon l'exigence E5. Les entités pourraient ainsi satisfaire à l'exigence E6 en même temps qu'aux exigences E4 et E5.

Annexe QC-CIP-014-2
Dispositions particulières de la norme CIP-014-2 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 :** Sécurité Physique
2. **Numéro :** CIP-014-2
3. **Objet :** Aucune disposition particulière
4. **Applicabilité :**

4.1 Entités fonctionnelles

Aucune disposition particulière

4.2 Installations

La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) qui répondent aux critères établis dans la section « Applicabilité » de la norme. Toute référence au terme « BES » doit être remplacée par le terme « RTP ».

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

La date d'entrée en vigueur proposée est le premier jour du premier trimestre civil à survenir six mois après l'adoption de la norme par la Régie de l'énergie.

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

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

1.1. Responsable des mesures pour assurer la conformité

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

1.2. Conservation des pièces justificatives

Au Québec, le CEA est assujetti aux dispositions de confidentialité comme spécifiée dans les sections applicables du « Programme de surveillance de la conformité et d'application des normes de fiabilité du Québec (PSCAQ) ».

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 justification technique

Aucune disposition particulière

Justifications

Aucune disposition particulière

Historique des versions

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