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 : 31 octobre 2017

   5.2. Adoption de l'annexe par la Régie de l'énergie : 31 octobre 2017

5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : 1er janvier 2018

Norme	Date de mise en application au Québec		
	Entités visées par la version 1 des normes CIP adoptées par la Régie	Entités exemptées de l'application de la version 1 des normes CIP en vertu des dispositions particulières associées à ces normes	Entités qui possèdent des installations de production à vocation industrielle
CIP-010-2	2018-01-01	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

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	Intervention	Suivi des modifications
0	31 octobre 2017	Nouvelle annexe.	Nouvelle