Normes de fiabilité (version française)

A. Introduction

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

2. **Numéro :** CIP-005-7

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

4. **Applicabilité :**

   4.1. Entités fonctionnelles : Dans le contexte de la présente norme, les entités fonctionnelles indiquées ci-après sont appelées collectivement « entités responsables ». Si certaines exigences visent plus spécifiquement une entité fonctionnelle ou un sous-ensemble d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

   4.1.1. ***Responsable de l'équilibrage***

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

   4.1.2.1. Système de délestage de *charge* en sous-fréquence (DSF) ou 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 des délestages automatiques de *charge* de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

   4.1.2.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une *norme de fiabilité* de la NERC ou de l'*entité régionale*.

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

   4.1.2.4. *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 de la fiabilité***

   4.1.6. ***Exploitant de réseau de transport***

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

4.2. ***Installations*** **:** Dans le contexte de la présente norme, les systèmes, *installations* et équipements suivants détenus par une entité responsable indiquée à la section 4.1 sont visés par les exigences. Si certaines exigences visent plus spécifiquement un type ou un sous-ensemble de systèmes, d'*installations* ou d'équipements, ceux-ci sont précisés explicitement.

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

4.2.1.1. 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 des délestages de *charge* automatiques de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

4.2.1.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

4.2.1.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une *norme de fiabilité* de la NERC ou de l'*entité régionale*.

4.2.1.4. *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-005-7 :

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

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

4.2.3.3. Les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme 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 ont déterminé n'avoir aucun *système électronique BES* classé dans les catégories « impact élevé » ou « impact moyen » selon le processus d'inventaire et de catégorisation prescrit dans la norme CIP-002.

5. Date d'entrée en vigueur :

Voir le plan de mise en œuvre du projet 2019-03.

6. Contexte :

La norme CIP-005 fait partie d'une série de normes CIP sur la cybersécurité qui exigent l'inventaire et la catégorisation initiales des *systèmes électroniques BES*, ainsi qu'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 le 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 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 de DSF et de DST. Ce seuil particulier de 300 MW pour les systèmes de DSF et de DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes de DST et de DSF, qui constituent des efforts de dernier

recours pour sauver le *système de production-transport d'électricité*. Un examen des tolérances des systèmes de 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 de 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. L'équipe de rédaction (SDT) CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

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

- ***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.

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-005-7) – *Périmètre de sécurité électronique*.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation et exploitation le même jour]

M1. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-005-7) – *Périmètre de sécurité électronique*, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-005-7) – *Périmètre de sécurité électronique*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.1	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : • les *PCA* associés.	Tous les *actifs électroniques* visés qui sont reliés à un réseau au moyen d'un protocole routable doivent être situés à l'intérieur d'un *ESP* défini.	Exemple non limitatif de pièce justificative : liste de tous les *ESP* avec tous les *actifs électroniques* visés à identifiant unique qui sont reliés au moyen d'un protocole routable dans chaque *ESP*.
1.2	*Systèmes électroniques BES* à impact élevé à *connectivité externe routable* et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : • les *PCA* associés.	Toute *connectivité externe routable* doit s'effectuer par l'intermédiaire d'un *point d'accès électronique* (*EAP*) identifié.	Exemples non limitatifs de pièces justificatives : schémas de réseau montrant tous les chemins de communication routables externes et les *EAP* identifiés.
1.3	*Points d'accès électronique* associés à des *systèmes électroniques BES* à impact élevé. *Points d'accès électronique* associés à des *systèmes électroniques BES* à impact moyen.	Exiger des autorisations pour les accès entrants et sortants, y compris la raison pour donner l'accès, et refuser tout autre accès par défaut.	Exemple non limitatif de pièce justificative : liste de règles (coupe-feu, liste des droits d'accès, etc.) démontrant que seuls les accès autorisés sont permis et que chaque règle d'accès est justifiée, documentation à l'appui.

Tableau E1 (CIP-005-7) – *Périmètre de sécurité électronique*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.4	*Systèmes électroniques BES* à impact élevé à *connectivité par lien commuté* et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité par lien commuté* et : • les *PCA* associés.	Lorsque techniquement faisable, effectuer l'authentification lors de l'établissement de la *connectivité par lien commuté* avec les *actifs électroniques* visés.	Exemple non limitatif de pièce justificative : processus documenté décrivant la méthode utilisée par l'entité responsable afin d'assurer l'authentification des accès effectués pour chaque connexion par lien commuté.
1.5	*Points d'accès électronique* associés à des *systèmes électroniques BES* à impact élevé. *Points d'accès électronique* associés à des *systèmes électroniques BES* à impact moyen situés dans des *centres de contrôle*.	Avoir un ou plusieurs moyens de détection des communications entrantes et sortantes malveillantes avérées ou présumées.	Exemple non limitatif de pièce justificative : documentation attestant la mise en œuvre de moyens de détection des communications malveillantes (système de détection des intrusions, pare-feu au niveau de la couche application, etc.).

E2. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, et lorsque c'est techniquement faisable, couvrent tous les alinéas applicables du tableau E2 (CIP-005-7) – Gestion des accès distants. *[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation et exploitation le même jour]*

M2. Les pièces justificatives doivent comprendre les processus documentés qui, collectivement, traitent de chacun des alinéas applicables du tableau E2 (CIP-005-7) – Gestion des accès distants, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-005-7) – Gestion des accès distants			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : • les *PCA* associés.	Pour tous les *accès distants interactifs*, utiliser un *système intermédiaire* de façon que l'*actif électronique* qui commande l'*accès distant interactif* n'ait pas directement accès à l'*actif électronique* visé.	Exemples non limitatifs de pièces justificatives : schémas de réseau ou documents sur l'architecture.
2.2	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : • les *PCA* associés.	Pour toutes les sessions d'*accès distant interactif*, utiliser un cryptage se terminant à un *système intermédiaire*.	Exemple non limitatif de pièce justificative : documents sur l'architecture qui indiquent les points où commence et où se termine le cryptage.

Tableau E2 (CIP-005-7) – Gestion des accès distants			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.3	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : • les *PCA* associés.	Exiger l'authentification multifactorielle pour toutes les sessions d'*accès distant interactif*.	Exemple non limitatif de pièce justificative : documents sur l'architecture décrivant les facteurs d'authentification utilisés. Exemples non limitatifs de facteurs d'authentification : • ce que l'utilisateur sait, comme un mot de passe ou un NIP. Ceci n'inclut pas les identifiants d'utilisateur ; • ce que l'utilisateur possède, comme un jeton, un certificat numérique ou une carte intelligente ; ou • une caractéristique biométrique de l'utilisateur, comme ses empreintes digitales ou le motif de son iris.
2.4	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et : • les *PCA* associés.	Disposer d'une ou de plusieurs méthodes permettant de déterminer les sessions actives d'accès distant par des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système).	Exemples non limitatifs de pièces justificatives : documentation des méthodes utilisées pour déterminer les sessions actives d'accès distant par des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système), par exemple : • méthodes d'accès aux informations journalisées ou de surveillance pour déterminer les

Tableau E2 (CIP-005-7) – Gestion des accès distants			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
			sessions actives d'accès distant par des fournisseurs ; • méthodes de surveillance de l'activité (par exemple, tableaux des connexions ou compteurs de règles dans un pare-feu, ou surveillance de l'activité des utilisateurs) ou des ports ouverts (par exemple, commandes netstat ou connexes pour afficher les ports en activité) permettant de déterminer les sessions actives d'accès distant de système à système ; ou • méthodes de contrôle des accès distants commandés par les fournisseurs, par exemple l'exigence que ceux-ci téléphonent pour demander un deuxième facteur d'identification afin d'établir un accès distant.

Tableau E2 (CIP-005-7) – Gestion des accès distants			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
2.5	*Systèmes électroniques BES* à impact élevé et : • les *PCA* associés. *Systèmes électroniques BES* à impact moyen à *connectivité externe routable* et leurs : • les *PCA* associés.	Disposer d'une ou de plusieurs méthodes permettant de désactiver les accès distants actifs des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système).	Exemples non limitatifs de pièces justificatives : documentation des méthodes utilisées pour désactiver les accès distants actifs des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système), par exemple : • méthodes permettant de désactiver l'accès distant des fournisseurs au *point d'accès électronique* applicable dans le cas d'un accès distant de système à système ; ou • méthodes permettant de désactiver l'*accès distant interactif* des fournisseurs au *système intermédiaire* applicable.

E3. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent les alinéas applicables du tableau E3 (CIP-005-7) – Gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS*.
[Facteur de risque de non-conformité : Moyen] [Horizon : planification de l'exploitation et exploitation le même jour]

M3. Les pièces justificatives doivent comprendre les processus documentés qui, collectivement, traitent de chacun des alinéas applicables du tableau E3 (CIP-005-7) – Gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS*, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E3 (CIP-005-7) – Gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*EACMS* et *PACS* associés à des *systèmes électroniques BES* à impact élevé *EACMS* et *PACS* associés à des *systèmes électroniques BES* à impact moyen à *connectivité externe routable*	Disposer d'une ou de plusieurs méthodes pour déterminer les connexions à distance authentifiées commandées par des fournisseurs.	Exemples non limitatifs de pièces justificatives : documentation des méthodes utilisées pour déterminer les connexions à distance authentifiées commandées par des fournisseurs, notamment : • méthodes d'accès aux informations journalisées ou de surveillance pour déterminer les connexions à distance authentifiées commandées par des fournisseurs.

Tableau E3 (CIP-005-7) – Gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS*			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*EACMS* et *PACS* associés à des *systèmes électroniques BES* à impact élevé *EACMS* et *PACS* associés à des *systèmes électroniques BES* à impact moyen à *connectivité externe routable*	Disposer d'une ou de plusieurs méthodes pour interrompre les connexions à distance authentifiées commandées par des fournisseurs, et pour contrôler la possibilité de reconnexion.	Exemples non limitatifs de pièces justificatives : documentation des méthodes utilisées pour interrompre les connexions à distance authentifiées commandées par des fournisseurs avec les systèmes visés. Par exemple, interrompre un outil, un processus ou une session actif commandé par un fournisseur, ou abandonner au niveau du pare-feu une connexion active commandée par un fournisseur. Les méthodes permettant de contrôler la possibilité de reconnexion, si nécessaire, pourraient être par exemple : désactiver un compte Active Directory ; désactiver un jeton de sécurité ; restreindre au niveau du pare-feu des adresses IP en provenance de fournisseurs ; ou débrancher physiquement un câble réseau afin d'empêcher la reconnexion.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Le terme « *responsable des mesures pour assurer la conformité* » (*CEA*) désigne la NERC ou l'*entité régionale*, ou toute entité désignée par un organisme gouvernemental pertinent, dans leurs rôles respectifs visant à surveiller et à assurer la conformité avec les *normes de fiabilité* obligatoires et exécutoires de la NERC dans leurs territoires respectifs.

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 visée 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 visée doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité visée 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 dossiers de l'audit le plus récent ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Programme de surveillance de la conformité et d'application des normes

Selon la définition des règles de procédure de la NERC, l'expression « programme de surveillance de la conformité et d'application des normes » désigne la liste des processus qui serviront à évaluer les données ou l'information afin de déterminer les résultats de conformité avec la *norme de fiabilité*.

Niveaux de gravité de la non-conformité (VSL)

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E1.			L'entité responsable n'avait pas un moyen de détection des communications entrantes et sortantes malveillantes. (1.5)	L'entité responsable n'avait pas documenté un ou plusieurs processus pour le tableau E1 (CIP-005-7) – *Périmètre de sécurité électronique*. (E1) OU Tous les *actifs électroniques* visés de l'entité responsable qui sont reliés à un réseau au moyen d'un protocole routable n'étaient pas à l'intérieur d'un *périmètre de sécurité électronique* (*ESP*) défini. (1.1) OU La *connectivité externe routable* à travers l'*ESP* n'était pas effectuée par l'intermédiaire d'un *EAP* identifié. (1.2) OU L'entité responsable n'a pas exigé d'autorisations pour les accès entrants et sortants et refusé tout autre accès par défaut. (1.3) OU L'entité responsable n'a pas effectué l'authentification lors de l'établissement de la connectivité par lien commuté avec les *actifs*

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	**VSL modéré**	**VSL élevé**	**VSL critique**
				électroniques visés, lorsque techniquement faisable. (1.4)
E2.	L'entité responsable n'a pas de processus documentés pour un ou plusieurs des éléments visés des alinéas 2.1 à 2.3.	L'entité responsable n'a pas mis en œuvre de processus pour un des éléments visés des alinéas 2.1 à 2.3.	L'entité responsable n'a pas mis en œuvre de processus pour deux des éléments visés des alinéas 2.1 à 2.3. OU L'entité responsable ne disposait pas : soit d'une ou de plusieurs méthodes permettant de déterminer les sessions actives d'accès distant par des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système) (2.4) ; soit d'une ou de plusieurs méthodes permettant de désactiver les accès distants actifs des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système (2.5).	L'entité responsable n'a pas mis en œuvre de processus pour trois des éléments visés des alinéas 2.1 à 2.3. OU L'entité responsable ne disposait : ni d'une ou de plusieurs méthodes permettant de déterminer les sessions actives d'accès distant par des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système) (2.4) ; ni d'une ou de plusieurs méthodes permettant de désactiver les accès distants actifs des fournisseurs (y compris les *accès distants interactifs* et les accès distants de système à système) (2.5).
E3.	L'entité responsable n'a pas documenté un ou plusieurs processus spécifiés au tableau E3 (CIP-005-7) – Gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS*. (E3)	L'entité responsable disposait d'une ou de plusieurs méthodes spécifiées à l'alinéa 3.1 pour les *EACMS*, mais ne disposait d'aucune méthode pour déterminer les connexions à distance authentifiées	L'entité responsable n'a pas mis en œuvre de processus pour l'alinéa 3.1 ou 3.2. (E3) OU L'entité responsable disposait d'une ou de plusieurs méthodes spécifiées à l'alinéa 3.1 pour les *PACS*, mais ne disposait d'aucune	L'entité responsable n'a mis en œuvre aucun processus du tableau E3 (CIP-005-7) – Gestion des accès distants des fournisseurs pour les *EACMS* et les *PACS*. (E3) OU

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
		commandées par des fournisseurs pour les *PACS*. (3.1) OU L'entité responsable disposait d'une ou de plusieurs méthodes spécifiées à l'alinéa 3.2 pour les *EACMS*, mais ne disposait d'aucune méthode pour interrompre les connexions à distance authentifiées commandées par des fournisseurs pour les *PACS*. (3.2)	méthode pour déterminer les connexions à distance authentifiées commandées par des fournisseurs pour les *EACMS*. (3.1) OU L'entité responsable disposait d'une ou de plusieurs méthodes spécifiées à l'alinéa 3.2 pour les *PACS*, mais ne disposait d'aucune méthode pour interrompre les connexions à distance authentifiées commandées par des fournisseurs ou pour contrôler la possibilité de reconnexion pour les *EACMS*. (3.2)	L'entité responsable ne disposait d'aucune des méthodes spécifiées aux alinéas 3.1 et 3.2. (E3)

D. Différences régionales

Aucune.

E. Documents connexes

- Plan de mise en œuvre du projet 2019-03.
- Justification technique de la norme CIP-005-7.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	16 janvier 2006	E3.2 — Remplacement de « Control Center » par « control center ».	24 mars 2006
2	30 septembre 2009	Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes. Suppression de la mention sur la prise en compte des considérations d'affaires. Remplacement de l'organisation régionale de fiabilité par l'*entité régionale* comme entité responsable. Reformulation de la date d'entrée en vigueur. Remplacement de « Responsabilité de la surveillance de la conformité » par « *Responsable des mesures pour assurer la conformité* ».	
3	16 décembre 2009	Changement du numéro de version de -2 à -3. Approbation par le Conseil d'administration de la NERC.	
3	31 mars 2010	Approbation par la FERC.	
4	30 décembre 2010	Ajout de critères précis pour l'identification des actifs critiques.	Mise à jour
4	24 janvier 2011	Approbation par le Conseil d'administration de la NERC.	Mise à jour
5	26 novembre 2012	Adoption par le Conseil d'administration de la NERC.	Modifiée en coordination avec les autres normes CIP et révision du format selon le gabarit RBS.
5	22 novembre 2013	Ordonnance de la FERC approuvant la norme CIP-005-5.	
6	20 juillet 2017	Modifications visant à répondre à certaines directives de l'Ordonnance 829 de la FERC.	Révision
6	10 août 2017	Adoption par le Conseil d'administration de la NERC.	

6	18 octobre 2018	Ordonnance de la FERC approuvant la norme CIP-005-6. Dossier RM17-13-000.	
7	1er août 2019	Modifications visant à répondre à certaines prescriptions de l'Ordonnance 850 de la FERC.	Révision
7	5 novembre 2020	Adoption par le Conseil d'administration de la NERC.	

A. Introduction

1. **Titre :** Cybersécurité — Gestion des changements de configuration et analyses de vulnérabilité

2. **Numéro :** CIP-010-4

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 de la présente norme, les entités fonctionnelles indiquées ci-après sont appelées collectivement « entités responsables ». Si certaines exigences visent plus spécifiquement une entité fonctionnelle ou un sous-ensemble d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

   4.1.1. ***Responsable de l'équilibrage***

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

   4.1.2.1. Système de délestage de *charge* en sous-fréquence (DSF) ou 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 des délestages automatiques de *charge* de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

   4.1.2.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

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

   4.1.2.4. *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 de la fiabilité***

   4.1.6. ***Exploitant de réseau de transport***

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

4.2.*Installations* : Dans le contexte de la présente norme, les systèmes, *installations* et équipements suivants détenus par une entité responsable indiquée à la section 4.1 sont visés par les exigences. Si certaines exigences visent plus spécifiquement un type ou un sous-ensemble de systèmes, d'*installations* ou d'équipements, ceux-ci sont précisés explicitement.

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

4.2.1.1. 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 des délestages de *charge* automatiques de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

4.2.1.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

4.2.1.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

4.2.1.4. *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-010-4 :

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 électronique* 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 ont déterminent n'avoir aucun *système électroniques BES* classé dans les catégories « impact élevé » ou « impact moyen » selon le processus d'inventaire et de catégorisation de la norme CIP-002.

5. Date d'entrée en vigueur : Voir le plan de mise en œuvre du projet 2019-03.

6. Contexte :

La norme CIP-010 fait partie d'une série de normes CIP sur la cybersécurité qui exigent l'inventaire et la catégorisation initiales des *systèmes électroniques BES* ainsi qu'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 de DSF et de DST. Ce seuil particulier de 300 MW pour les systèmes de DSF et de DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes de DST et de DSF, qui constituent des efforts de dernier recours pour sauver le *BES*. Un examen des tolérances des systèmes de 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 de 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. L'équipe de rédaction (SDT) CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- ***Systèmes électroniques BES* à impact élevé –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon les processus d'inventaire et de catégorisation de la norme CIP-002.
- ***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.
- ***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 physiques* 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-010-4) – Gestion des changements de configuration.
[Facteur de risque de 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-010-4) – Gestion des changements de configuration ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-010-4) – 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 : 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 éléments suivants : 1.1.1. le ou les systèmes d'exploitation (y compris la version), ou tout 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 appliqué.	Exemples non limitatifs de pièces justificatives : • feuille de calcul indiquant les éléments de configuration de référence requis pour chaque *actif électronique*, individuellement ou par groupe ; ou • enregistrement dans un système de gestion d'actifs indiquant les éléments de configuration de référence requis pour chaque *actif électronique*, individuellement ou par groupe.

Tableau E1 (CIP-010-4) – Gestion des changements de configuration			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.2	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Autoriser et documenter tout changement par rapport à la configuration de référence existante.	Exemples non limitatifs de pièces justificatives : • pour chaque changement, l'enregistrement dans un système de gestion des changements de la demande de changement et de l'autorisation électronique correspondante (accordée par une personne ou un groupe dûment habilité) ; 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 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Pour tout changement par rapport à la configuration de référence existante, mettre à jour la configuration de référence dans les 30 jours civils suivant l'exécution du changement.	Exemple non limitatif de pièce justificative : documentation de la configuration de référence avec mise à jour datée d'au plus 30 jours civils après la date d'exécution du changement.

Tableau E1 (CIP-010-4) – Gestion des changements de configuration			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.4	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; 2. les *PACS* associés ; et 3. les *PCA* associés.	Pour 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 qui pourraient être touchés par le changement ; 1.4.2. après le changement, vérifier que les mécanismes de cybersécurité déterminés en 1.4.1 ne sont pas dégradés ; et 1.4.3. documenter les résultats de la vérification.	Exemple non limitatif de pièce justificative : liste de mécanismes de cybersécurité vérifiés ou mis à l'essai, avec résultats d'essai datés.

Tableau E1 (CIP-010-4) – Gestion des changements de configuration			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.5	*Systèmes électroniques BES* à impact élevé.	Pour chaque changement par rapport à la configuration de référence existante, dans la mesure où c'est techniquement faisable : 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 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 : 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-010-4) – Gestion des changements de configuration			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
1.6	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 2. les *PACS* associés. *Systèmes électroniques BES* à impact moyen et : 1. les *EACMS* associés ; et 2. les *PACS* associés. Remarque : La mise en œuvre d'un plan n'oblige pas l'entité responsable à renégocier ou à résilier des contrats existants (y compris les modifications aux ententes-cadres ou les bons de commande). En outre, la partie 1.6 ne s'étend pas : 1) aux modalités mêmes d'un contrat d'approvisionnement ; et 2) à l'exécution et au respect du contrat par le fournisseur.	Avant tout changement touchant les éléments de la configuration de référence spécifiés aux alinéas 1.1.1, 1.1.2 et 1.1.5 par rapport à la configuration existante, dans la mesure où la source d'un logiciel met les méthodes appropriées à la disposition de l'entité responsable : 1.6.1. vérifier l'identité de la source du logiciel ; et 1.6.2. vérifier l'intégrité du logiciel obtenu de la source du logiciel.	Exemples non limitatifs de pièces justificatives : enregistrement d'une demande de changement qui atteste que l'identité de la source du logiciel et l'intégrité du logiciel ont été vérifiées avant le changement à la configuration de référence ; ou processus qui documente les mécanismes en place pour assurer la vérification automatique de l'identité de la source du logiciel et de l'intégrité du logiciel.

E2. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-010-4) – Surveillance de la configuration.
[Facteur de risque de 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-010-4) – Surveillance de la configuration ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-010-4) – 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 à 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-010-4) – Analyses de vulnérabilité.
[Facteur de risque de 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-010-4) – Analyses de vulnérabilité ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E3 (CIP-010-4) – 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-010-4) – Analyses de vulnérabilité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*Systèmes électroniques BES* à impact élevé.	Au moins une fois tous les 36 mois civils, dans la mesure où c'est techniquement faisable : 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-010-4) – Analyses de vulnérabilité			
Alinéa	**Systèmes visés**	**Exigences**	**Mesures**
3.3	*Systèmes électroniques BES* à impact élevé et : 1. les *EACMS* associés ; et 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 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

Le terme « *responsable des mesures pour assurer la conformité* » (*CEA*) désigne la NERC ou l'*entité régionale*, ou toute entité désignée par un organisme gouvernemental pertinent, dans leurs rôles respectifs visant à surveiller et à assurer la conformité avec les normes de fiabilité obligatoires et exécutoires de la NERC dans leurs territoires respectifs.

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 visée 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 visée doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité visée 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 dossiers de l'audit le plus récent ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Programme de surveillance de la conformité et d'application des normes

Selon la définition des règles de procédure de la NERC, l'expression « programme de surveillance de la conformité et d'application des normes » désigne la liste des processus qui serviront à évaluer les données ou l'information afin de déterminer les résultats de conformité avec la norme de fiabilité.

Niveaux de gravité de la non-conformité (VSL)

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E1.	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) OU L'entité responsable a un processus conforme à l'alinéa 1.6 pour vérifier l'identité de la source du logiciel (1.6.1), mais n'a pas de processus conforme à l'alinéa 1.6 pour vérifier l'intégrité du logiciel obtenu de la source du logiciel alors que la méthode appropriée est mise à la disposition de l'entité responsable par la source du logiciel (1.6.2).	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 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

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
				L'entité responsable n'a pas de processus pour déterminer les mécanismes de sécurité exigés par les normes CIP-005 et CIP-007 qui pourraient être touchés par des 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 exigés par 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 exigés n'étaient pas dégradés par suite du changement. (1.4.2 et 1.4.3) OU L'entité responsable n'a pas de processus pour mettre à l'essai les changements dans un environnement qui simule la configuration de référence avant de mettre en œuvre un changement par rapport à la configuration de référence. (1.5.1) OU

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
				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) OU L'entité responsable n'a pas de processus conforme à l'alinéa 1.6 ni pour vérifier l'identité de la source du logiciel, ni pour vérifier l'intégrité du logiciel obtenu de la source du logiciel, alors que les méthodes appropriées sont mises à la disposition de l'entité responsable par la source du logiciel. (1.6)
E2.	Sans objet	Sans objet	Sans objet	L'entité responsable n'a pas documenté ou 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 à la configuration de référence, pour documenter ceux-ci et pour faire enquête. (2.1)
E3.	L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun 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,	L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses *systèmes électroniques BES* visés,	L'entité responsable n'a mis en œuvre aucun processus d'analyse de vulnérabilité pour un de ses

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
	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. (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 suivant la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2)	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. (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 suivant la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2)	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. (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 suivant la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2)	*systèmes électroniques BES* visés. (E3) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses *systèmes électroniques BES* visés, mais elle a effectué une analyse de vulnérabilité plus de 24 mois suivant la 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 suivant la dernière analyse active de l'un de ses *systèmes électroniques BES* visés. (3.2) OU L'entité responsable a mis en œuvre et documenté un ou plusieurs processus d'analyse de vulnérabilité pour chacun de ses *systèmes électroniques BES* visés, mais elle n'a pas effectué l'analyse

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
				de vulnérabilité active d'une manière qui simule une configuration de référence existante de ses *systèmes électroniques BES* visés. (3.3) OU L'entité responsable a mis en œuvre un ou plusieurs processus documentés d'analyse de vulnérabilité pour chacun de ses *systèmes électroniques BES* visés, mais elle n'a pas documenté les résultats des analyses de vulnérabilité, les plans d'action pour 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.	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'exigence E4 de la norme CIP-010-4. (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 applicables aux *supports de stockage amovibles* conformément à la section 3 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-4. (E4)	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 complémentaire à l'exigence E4 de la norme CIP-010-4. (E4) OU	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-010-4. (E4)

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
	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-010-4. (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 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-010-4. (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-010-4. (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	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 de l'annexe 1 complémentaire à l'exigence E4 de la norme CIP-010-4. (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 l'exigence E4 de la norme CIP-010-4. (E4)	

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
		complémentaire à l'exigence E4 de la norme CIP-010-4. (E4)		

D. Différences régionales

Aucune.

E. Documents connexes

- Plan de mise en œuvre du projet 2019-03.
- Justification technique de la norme CIP-010-4.

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.
2	21 janvier 2016	Ordonnance de la FERC approuvant la norme CIP-010-3. Dossier RM15-14-000.	
3	20 juillet 2017	Modifications visant à répondre à certaines directives de l'Ordonnance 829 de la FERC.	Révision
3	10 août 2017	Adoption par le Conseil d'administration de la NERC.	
3	18 octobre 2018	Ordonnance de la FERC approuvant la norme CIP-010-3. Dossier RM17-13-000.	

Version	Date	Intervention	Suivi des modifications
4	1er août 2019	Modifications visant à répondre à certaines prescriptions de l'Ordonnance 850 de la FERC	Révision
4	5 novembre 2020	Adoption par le Conseil d'administration de la NERC.	

CIP-010-4 – 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 avec les 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 :

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

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

1.1.3. 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 de 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 de stockage 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-010-4 – 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.

A. Introduction

1. **Titre :** Cybersécurité – Gestion des risques dans la chaîne d'approvisionnement

2. **Numéro :** CIP-013-2

3. **Objet :** Atténuer les risques de cybersécurité susceptibles de menacer la fiabilité du *système de production-transport d'électricité* (*BES*) en établissant des contrôles de sécurité axés sur la gestion des risques dans la chaîne d'approvisionnement des *systèmes électroniques BES*.

4. **Applicabilité :**

   4.1. Entités fonctionnelles : Dans le contexte de la présente norme, les entités fonctionnelles indiquées ci-après sont appelées collectivement « entités responsables ». Si certaines exigences visent plus spécifiquement une entité fonctionnelle ou un sous-ensemble d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

   4.1.1. ***Responsable de l'équilibrage***

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

   4.1.2.1. Système de délestage de *charge* en sous-fréquence (DSF) ou 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 des délestages automatiques de *charge* de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

   4.1.2.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

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

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

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

   4.1.5. ***Coordonnateur de la fiabilité***

   4.1.6. ***Exploitant de réseau de transport***

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

4.2. ***Installations*** **:** Dans le contexte de la présente norme, les systèmes, *installations* et équipements suivants détenus par une entité responsable indiquée à la section 4.1 sont visés par les exigences. Si certaines exigences visent plus spécifiquement un type ou un sous-ensemble de systèmes, d'*installations* ou d'équipements, ceux-ci sont précisés explicitement.

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

4.2.1.1. 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 des délestages de *charge* automatiques de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

4.2.1.2. *Automatisme de réseau* (*RAS*) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

4.2.1.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.

4.2.1.4. *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-013-2 :

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 *périmètres de sécurité électronique* (*ESP*) distincts.

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

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

4.2.3.5. Les entités responsables qui ont déterminé n'avoir aucun *système électronique BES* classé dans les catégories « impact élevé » ou « impact moyen » selon le processus d'inventaire et de catégorisation de la norme CIP-002 ou toute version postérieure.

5. **Date d'entrée en vigueur :** Voir le plan de mise en œuvre du projet 2019-03.

B. Exigences et mesures

E1. Chaque entité responsable doit établir un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement pour les *systèmes électroniques BES* à impact moyen ou élevé ainsi que les *systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*) et les *systèmes de contrôle des accès physiques* (*PACS*) associés. Ce ou ces plans doivent comprendre les éléments suivants :
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]

1.1. Un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* liés aux produits ou services de fournisseurs, résultant : i) de l'acquisition et de l'installation d'équipements et de logiciels de fournisseurs ; et ii) d'une transition entre fournisseurs.

1.2. Un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés, qui prévoient les mesures suivantes, selon le cas :

1.2.1. la notification par le fournisseur des incidents constatés par celui-ci relativement aux produits ou services livrés à l'entité responsable et qui présentent pour celle-ci un risque de cybersécurité ;

1.2.2. la coordination des réponses aux incidents constatés par le fournisseur relativement aux produits ou services livrés à l'entité responsable et qui présentent pour celle-ci un risque de cybersécurité ;

1.2.3. la notification par le fournisseur lorsqu'il n'y a plus lieu d'accorder à ses représentants un accès distant ou local ;

1.2.4. la divulgation par le fournisseur de vulnérabilités connues touchant des produits ou services livrés à l'entité responsable ;

1.2.5. la vérification de l'intégrité et de l'authenticité de tous les logiciels et correctifs livrés par le fournisseur et destinés à un *système électronique BES* ainsi qu'aux *EACMS* et aux *PACS* associés; et

1.2.6. la coordination des contrôles visant les accès distants commandés par un fournisseur.

M1. Les pièces justificatives doivent comprendre un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, conformément à l'exigence.

E2. Chaque entité responsable doit mettre en œuvre le ou les plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement prescrits à l'exigence E1.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]

Remarque : La mise en œuvre d'un plan n'oblige pas l'entité responsable à renégocier ou à résilier des contrats existants (y compris les modifications aux ententes-cadres ou les bons de commande). En outre, l'exigence E2 ne s'étend pas : 1) aux modalités mêmes d'un contrat d'approvisionnement ; et 2) à l'exécution et au respect du contrat par le fournisseur.

M2. Les pièces justificatives doivent comprendre une documentation attestant la mise en œuvre du ou des plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement. Exemples non limitatifs de pièces justificatives : documents de correspondance, de politique ou de travail témoignant de l'utilisation de tels plans.

E3. Chaque entité responsable doit réexaminer et faire approuver par le *cadre supérieur CIP* ou son délégataire, au moins une fois tous les 15 mois civils, le ou les plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement prescrits à l'exigence E1.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]

M3. Les pièces justificatives doivent comprendre le ou les plans datés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement approuvés par le *cadre supérieur CIP* ou son délégataire ainsi que des pièces justificatives supplémentaires attestant le réexamen de ce ou ces plans. Exemples non limitatifs de pièces justificatives : documents de politique, historique de révisions, dossiers de réexamen ou preuves de flux de travail provenant d'un système de gestion documentaire attestant que chaque plan de gestion des risques de cybersécurité dans la chaîne d'approvisionnement a fait l'objet d'un réexamen au moins une fois tous les 15 mois civils, ainsi que l'approbation documentée par le *cadre supérieur CIP* ou son délégataire.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Le terme « *responsable des mesures pour assurer la conformité* » (*CEA*) désigne la NERC ou l'*entité régionale*, ou toute entité désignée par un organisme gouvernemental pertinent, dans leurs rôles respectifs visant à surveiller et à assurer la conformité avec les normes de fiabilité obligatoires et exécutoires de la NERC dans leurs territoires respectifs.

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 afin de démontrer sa conformité. Dans les cas où la période de conservation 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.

Chaque 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 dossiers de l'audit le plus récent ainsi que tous les dossiers d'audit demandés et soumis par la suite.

1.3. Programme de surveillance de la conformité et d'application des normes

Selon la définition des règles de procédure de la NERC, l'expression « programme de surveillance de la conformité et d'application des normes » désigne la liste des processus qui serviront à évaluer les données ou l'information afin de déterminer les résultats de conformité avec la norme de fiabilité.

Niveaux de gravité de la non-conformité (VSL)

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E1.	L'entité responsable a établi un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, qui comprennent un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1, et comprenant un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés conformément à l'alinéa 1.2, mais ce ou ces plans omettent une des prescriptions des alinéas 1.2.1 à 1.2.6.	L'entité responsable a établi un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, qui comprennent un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1, et comprenant un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés conformément à l'alinéa 1.2, mais ce ou ces plans omettent au moins deux des prescriptions des alinéas 1.2.1 à 1.2.6.	L'entité responsable a établi un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, mais ce ou ces plans ne comprennent pas de processus utilisé dans la planification de l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1, ou ne comprennent pas de processus utilisé dans l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés conformément à l'alinéa 1.2.	L'entité responsable a établi un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, mais ce ou ces plans ne comprennent pas de processus utilisé dans la planification de l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1, et ne comprennent pas non plus de processus utilisé dans l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés conformément à l'alinéa 1.2. OU L'entité responsable n'a établi aucun plan documenté de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, en contravention avec l'exigence.

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E2.	L'entité responsable a mis en œuvre son ou ses plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, comprenant un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1 de l'exigence E1, et comprenant un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés conformément à l'alinéa 1.2 de l'exigence E1, mais cette mise en œuvre a omis une des prescriptions des alinéas 1.2.1 à 1.2.6.	L'entité responsable a mis en œuvre son ou ses plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, comprenant un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1 de l'exigence E1, et comprenant un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés conformément à l'alinéa 1.2 de l'exigence E1, mais cette mise en œuvre a omis au moins deux des prescriptions des alinéas 1.2.1 à 1.2.6.	L'entité responsable a mis en œuvre son ou ses plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, mais sans mettre en œuvre un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1 de l'exigence E1, ou sans mettre en œuvre un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés conformément à l'alinéa 1.2 de l'exigence E1.	L'entité responsable a mis en œuvre son ou ses plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, mais sans mettre en œuvre un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* conformément à l'alinéa 1.1 de l'exigence E1, et sans non plus mettre en œuvre un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés conformément à l'alinéa 1.2 de l'exigence E1. OU L'entité responsable n'a mis en œuvre aucun plan documenté de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, en contravention avec l'exigence.

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E3.	L'entité responsable a réexaminé et fait approuver par le *cadre supérieur CIP* ou son délégataire son ou ses plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, mais dans un délai de plus de 15 mois civils et d'au plus 16 mois civils suivant le réexamen précédent.	L'entité responsable a réexaminé et fait approuver par le *cadre supérieur CIP* ou son délégataire son ou ses plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, mais dans un délai de plus de 16 mois civils et d'au plus 17 mois civils suivant le réexamen précédent.	L'entité responsable a réexaminé et fait approuver par le *cadre supérieur CIP* ou son délégataire son ou ses plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, mais dans un délai de plus de 17 mois civils et d'au plus 18 mois civils suivant le réexamen précédent.	L'entité responsable n'a pas réexaminé et fait approuver par le *cadre supérieur CIP* ou son délégataire son ou ses plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement dans un délai de 18 mois civils suivant le réexamen précédent.

D. Différences régionales

Aucune.

E. Documents connexes

- Plan de mise en œuvre du projet 2019-03.
- Justification technique de la norme CIP-013-2.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	20 juillet 2017	Mise en œuvre de l'Ordonnance 829 de la FERC.	
1	10 août 2017	Approbation par le Conseil d'administration de la NERC.	
1	18 octobre 2018	Ordonnance de la FERC approuvant la norme CIP-013-1. Dossier RM17-13-000.	
2	1er août 2019	Modifications visant à répondre à certaines prescriptions de l'Ordonnance 850 de la FERC.	Révision
2	5 novembre 2020	Adoption par le Conseil d'administration de la NERC.	