

A. Introduction

1. **Titre :** Cybersécurité — Gestion de la sécurité des systèmes
2. **Numéro :** CIP-007-5
3. **Objet :** Gérer la sécurité des systèmes en établissant des exigences techniques, opérationnelles et administratives particulières afin de protéger les *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou une instabilité dans le BES.
4. **Applicabilité :**
 - 4.1. **Entités fonctionnelles :** Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.
 - 4.1.1 **Responsable de l'équilibrage**
 - 4.1.2 **Distributeur** qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du BES :
 - 4.1.2.1 Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :
 - 4.1.2.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et
 - 4.1.2.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.
 - 4.1.2.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.
 - 4.1.2.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.
 - 4.1.2.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.
 - 4.1.3 **Exploitant d'installation de production**
 - 4.1.4 **Propriétaire d'installation de production**

4.1.5 Coordonnateur des échanges ou Responsable des échanges**4.1.6 Coordonnateur de la fiabilité****4.1.7 Exploitant de réseau de transport****4.1.8 Propriétaire d'installation de transport**

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

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

4.2.1.1 Chaque système de DSF ou de DST qui :

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

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

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

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

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

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

- 4.2.3.2** les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électroniques* distincts ;
- 4.2.3.3** les systèmes, structures et composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme à la norme CFR 10, section 73.54 ;
- 4.2.3.4** dans le cas des distributeurs, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus ;
- 4.2.3.5** les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* catégorisés comme impact élevé ou impact moyen en conformité avec le processus d'identification et de catégorisation de la CIP-002-5.

5. Dates d'entrée en vigueur

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

6. Contexte :

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

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

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

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

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

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

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

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

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

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

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

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

Colonnes « Systèmes visés » des tableaux

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. Le SDT CS0706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

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

B. Exigences et mesures

- E1.** Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-007-5) – Ports et services. *[Facteur de risque de la non-conformité : moyen] [Horizon : exploitation du jour même]*
- M1.** Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-007-5) – Ports et services, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

| Tableau E1 (CIP-007-5) – Ports et services | | | |
|--|--|---|--|
| Partie | Systèmes visés | Exigences | Mesures |
| 1.1 | <p><i>Systèmes électroniques BES</i> à impact élevé et leurs :</p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES</i> à impact moyen à <i>connectivité externe routable</i> et leurs :</p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | <p>Lorsque techniquement faisable, activer uniquement les ports logiques accessibles par le réseau qui sont jugés nécessaires par l'entité responsable, y compris les plages de ports ou de services qui sont nécessaires pour la prise en charge de ports dynamiques. Si un dispositif ne permet pas la désactivation ou la restriction de ses ports logiques, tous les ports ouverts sont considérés comme nécessaires.</p> | <p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • documentation établissant la nécessité de tous les ports activés de tous les <i>actifs électroniques</i> et <i>points d'accès électronique</i> visés, pris individuellement ou collectivement ; • listes des ports à l'écoute des <i>actifs électroniques</i>, pris individuellement ou collectivement, provenant des fichiers de configuration des dispositifs, du résultat de commandes telles que netstat ou de balayages réseau des ports ouverts ; ou • fichiers de configuration des pare-feu de l'hôte ou de tout autre mécanisme intégré au matériel qui n'autorisent l'accès qu'aux ports nécessaires et qui le refusent à tous les autres. |

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

- E2.** Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-007-5) – Gestion des rustines de sécurité. [*Facteur de risque de la non-conformité : moyen*] [*Horizon : planification de l'exploitation*]
- M2.** Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-007-5) – Gestion des rustines de sécurité, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-007-5) – Gestion des rustines de sécurité

| Partie | Systèmes visés | Exigences | Mesures |
|--------|--|--|---|
| 2.1 | <p><i>Systèmes électroniques BES</i> à impact élevé et leurs :</p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés; et 3. PCA associés. | <p>Un processus de gestion des rustines portant sur le suivi, l'évaluation et l'installation des rustines de cybersécurité pour les <i>actifs électroniques</i> visés. Le suivi comprend la désignation de la ou des sources que l'entité responsable utilise pour faire le suivi de la publication de rustines de cybersécurité destinées aux <i>actifs électroniques</i> visés qui sont actualisables et pour lesquels il existe une source de rustines.</p> | <p>Exemples non limitatifs de pièces justificatives : documentation d'un processus de gestion des rustines et documentation ou listes de sources qui sont utilisées pour le suivi visant chacun des <i>systèmes électroniques BES</i> ou des <i>actifs électroniques BES</i>.</p> |

Tableau E2 (CIP-007-5) – Gestion des rustines de sécurité

| Partie | Systèmes visés | Exigences | Mesures |
|--------|---|---|--|
| 2.2 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | Au moins une fois tous les 35 jours civils, évaluer l'applicabilité des rustines de sécurité publiées par la ou les sources indiquées à la partie 2.1 depuis l'évaluation précédente. | Exemple non limitatif de pièce justificative : une évaluation effectuée ou citée par une entité responsable ou réalisée en son nom et portant sur les rustines de sécurité publiées par les sources documentées, et ce, au moins tous les 35 jours civils. |

Tableau E2 (CIP-007-5) – Gestion des rustines de sécurité

| Partie | Systèmes visés | Exigences | Mesures |
|--------|---|---|---|
| 2.3 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | <p>Pour les rustines jugées applicables selon la partie 2.2, prendre une des mesures suivantes dans les 35 jours civils après que l'évaluation soit terminée :</p> <ul style="list-style-type: none"> • appliquer les rustines applicables, • créer un plan de mitigation daté ou • réviser un plan de mitigation existant. <p>Les plans de mitigation doivent comprendre les mesures que l'entité responsable compte prendre pour mitiger les vulnérabilités visées par chaque rustine de sécurité, ainsi qu'un délai de mise en œuvre des mesures.</p> | <p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • Enregistrements d'installation des rustines (p. ex. rapport exporté d'un outil automatisé de gestion des rustines fournissant la date d'installation, validation de la version du logiciel des composants du <i>système électronique BES</i> ou exportation d'un registre indiquant que le logiciel a été installé) ; ou • plan daté indiquant à quel moment et de quelle façon la vulnérabilité sera corrigée, qui documente les mesures que l'entité responsable compte prendre pour mitiger les vulnérabilités visées par la rustine de sécurité et qui précise un délai d'exécution des mesures de mitigation. |

| Tableau E2 (CIP-007-5) – Gestion des rustines de sécurité | | | |
|---|--|--|---|
| Partie | Systèmes visés | Exigences | Mesures |
| 2.4 | <p><i>Systèmes électroniques BES à impact élevé et :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; 3. PCA associés. | Pour chaque plan de mitigation créé ou mis à jour à la partie 2.3, mettre le plan en œuvre dans le délai précisé, à moins qu’une révision du plan ou un prolongement du délai indiqué à la partie 2.3 ne soit approuvé par le <i>cadre supérieur CIP</i> ou son délégué. | Exemple non limitatif de pièce justificative : dossiers de mise en œuvre des plans de mitigation. |

- E3.** Chaque entité responsable doit mettre en œuvre, d’une manière permettant d’identifier, d’évaluer et de corriger les lacunes, un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d’exigence applicables du tableau E3 (CIP-007-5) – Protection contre les programmes malveillants. [*Facteur de risque de la non-conformité : moyen*] [*Horizon : exploitation du jour même*]
- M3.** Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d’exigence applicables du tableau E3(CIP-007-5) – Protection contre les programmes malveillants ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

| Tableau E3 (CIP-007-5) – Protection contre les programmes malveillants | | | |
|--|---|--|---|
| Partie | Systèmes visés | Exigences | Mesures |
| 3.1 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | Utiliser une ou des méthodes pour bloquer, détecter ou prévenir les programmes malveillants. | Exemple non limitatif de pièce justificative : suivis de la mise en œuvre de ces méthodes par l'entité responsable (au moyen des logiciels antivirus habituels, du renforcement des systèmes, de politiques, etc.). |

| Tableau E3 (CIP-007-5) – Protection contre les programmes malveillants | | | |
|--|---|--|---|
| Partie | Systèmes visés | Exigences | Mesures |
| 3.2 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | Mitiger la menace des programmes malveillants détectés. | <p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • registres des processus d'intervention en cas de détection de programmes malveillants ; • suivis de la mise en œuvre de ces processus lorsque des programmes malveillants sont détectés. |
| 3.3 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | Pour les méthodes indiquées à la partie 3.1 qui utilisent des signatures ou des séquences de code, avoir un processus de mise à jour des signatures et des séquences de code. Le processus doit traiter de l'essai et de l'installation des signatures et des séquences de code. | Exemple non limitatif de pièce justificative : documentation décrivant le processus de mise à jour des signatures et des séquences de code. |

- E4.** Chaque entité responsable doit mettre en œuvre, d’une manière permettant d’identifier, d’évaluer et de corriger les lacunes, un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d’exigence applicables du tableau E4 (CIP-007-5) – Surveillance des événements de sécurité. *[Facteur de risque de la non-conformité : moyen]*
[Horizon : exploitation du jour même et évaluation de l’exploitation]
- M4.** Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d’exigence applicables du tableau E4 (CIP-007-5) – Surveillance des événements de sécurité ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

| Tableau E4 (CIP-007-5) – Surveillance des événements de sécurité | | | |
|--|---|---|--|
| Partie | Systèmes visés | Exigences | Mesures |
| 4.1 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; 3. PCA associés. | <p>Journaliser les événements au niveau du <i>système électronique BES</i> (par fonction de <i>système électronique BES</i>) ou au niveau de l'<i>actif électronique</i> (par fonction d'<i>actif électronique</i>) permettant la détection des <i>incidents de cybersécurité</i> – et les enquêtes subséquentes à leur sujet – qui comprennent au minimum chacun des types d’événements suivants :</p> <ol style="list-style-type: none"> 4.1.1. toute tentative détectée d’ouverture de session ayant réussi ; 4.1.2. toute tentative détectée d’accès ou d’ouverture de session ayant échoué ; 4.1.3. tout programme malveillant détecté. | <p>Exemples non limitatifs de pièces justificatives : liste des types d’événements que le <i>système électronique BES</i> est en mesure de détecter, générée manuellement ou par le système lui-même, et, le cas échéant, qu’il est configuré pour journaliser. Cette liste doit comprendre les types d’événements obligatoires.</p> |

| Tableau E4 (CIP-007-5) – Surveillance des événements de sécurité | | | |
|--|---|---|--|
| Partie | Systèmes visés | Exigences | Mesures |
| 4.2 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; 3. PCA associés. | <p>Générer des alertes pour les événements de sécurité qui, selon l'entité responsable, nécessitent une alerte, y compris au minimum chacun des types d'événements suivants (par fonction de l'<i>actif électronique</i> ou du <i>système électronique BES</i>) :</p> <ol style="list-style-type: none"> 4.2.1. programmes malveillants détectés conformément à la partie 4.1 ; 4.2.2. échec détecté de la journalisation des événements définis à la partie 4.1. | <p>Exemples non limitatifs de pièces justificatives : liste, générée manuellement ou par le système, des événements de sécurité qui, selon l'entité responsable, nécessitent des alertes, y compris une liste, générée manuellement ou par le système, indiquant la configuration des alertes.</p> |

| Tableau E4 (CIP-007-5) – Surveillance des événements de sécurité | | | |
|--|--|---|---|
| Partie | Systèmes visés | Exigences | Mesures |
| 4.3 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen de centres de contrôle et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | Lorsque techniquement faisable, conserver les journaux des événements exigés à la partie 4.1 pendant au moins 90 jours civils consécutifs, sauf dans des <i>circonstances CIP exceptionnelles</i> . | Exemples non limitatifs de pièces justificatives : documentation du processus de conservation des journaux des événements et rapports générés manuellement ou par le système qui indiquent que la configuration de conservation des journaux est réglée à 90 jours ou plus. |
| 4.4 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PCA associés. | Passer en revue un résumé ou un échantillon des événements journalisés, tels que définis par l'entité responsable, à des intervalles d'un maximum de 15 jours civils, afin de repérer les <i>incidents de cybersécurité</i> non détectés. | Exemples non limitatifs de pièces justificatives : document décrivant l'examen et ses constatations éventuelles, et document daté démontrant que l'examen a eu lieu. |

- E5.** Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un ou plusieurs processus documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E5 (CIP-007-5) – Contrôle des accès aux systèmes. [*Facteur de risque de la non-conformité : moyen*] [*Horizon : planification de l'exploitation*]
- M5.** Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E5 (CIP-007-5) – Contrôle des accès aux systèmes, ainsi que des pièces justificatives additionnelles attestant la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E5 (CIP-007-5) – Contrôle des accès aux systèmes

| Partie | Systèmes visés | Exigences | Mesures |
|--------|--|---|--|
| 5.1 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen de centres de contrôle et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | Avoir une ou plusieurs méthodes pour imposer l'authentification de tout accès utilisateur interactif, lorsque techniquement faisable. | Exemple non limitatif de pièce justificative : documentation décrivant le mode d'authentification des accès. |

Tableau E5 (CIP-007-5) – Contrôle des accès aux systèmes

| Partie | Systèmes visés | Exigences | Mesures |
|--------|---|--|---|
| 5.2 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | Identifier et répertorier par système, par groupe de systèmes, par emplacement ou par type de système tous les comptes par défaut ou autres comptes génériques qui sont connus et activés. | Exemple non limitatif de pièce justificative : liste de comptes indiquant les types de comptes activés ou génériques utilisés pour le <i>système électronique BES</i> . |
| 5.3 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | Identifier toutes les personnes ayant un accès autorisé à des comptes partagés. | Exemple non limitatif de pièce justificative : liste des comptes partagés et des personnes qui y ont un accès autorisé. |

Tableau E5 (CIP-007-5) – Contrôle des accès aux systèmes

| Partie | Systèmes visés | Exigences | Mesures |
|--------|---|---|--|
| 5.4 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | Changer les mots de passe par défaut connus par fonction de <i>l'actif électronique</i> . | <p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • documentation d'une procédure selon laquelle les mots de passe sont changés lorsque de nouveaux dispositifs sont mis en service ; ou • mention dans les manuels des systèmes ou dans d'autres documents de leurs fournisseurs selon laquelle les mots de passe par défaut ont été générés de façon pseudo-aléatoire et sont donc exclusifs à chaque dispositif. |

Tableau E5 (CIP-007-5) – Contrôle des accès aux systèmes

| Partie | Systèmes visés | Exigences | Mesures |
|--------|---|--|--|
| 5.5 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | <p>En ce qui concerne l'authentification par mot de passe uniquement de l'accès utilisateur interactif, imposer les paramètres suivants par des moyens techniques ou procéduraux :</p> <p>5.5.1. une longueur de mot de passe d'au moins huit caractères ou de la longueur maximale permise par l'<i>actif électronique</i>, selon la moindre des deux ;</p> <p>5.5.2. une complexité minimale du mot de passe d'au moins trois types différents de caractères (lettres majuscules et minuscules, chiffres, caractères non alphanumériques) ou du maximum permis par l'<i>actif électronique</i>, selon la moindre des deux.</p> | <p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • rapports générés par le système ou captures d'écran montrant les paramètres de mot de passe appliqués par le système, y compris la longueur et la complexité ; ou • attestations comportant un renvoi aux procédures documentées ayant été suivies. |

Tableau E5 (CIP-007-5) – Contrôle des accès aux systèmes

| Partie | Systèmes visés | Exigences | Mesures |
|--------|---|--|--|
| 5.6 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen à connectivité externe routable et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | <p>Lorsque techniquement faisable, en ce qui concerne l'authentification par mot de passe uniquement de l'accès utilisateur interactif, imposer par des moyens techniques ou procéduraux les changements de mot de passe ou l'obligation de changer le mot de passe au moins une fois tous les 15 mois civils.</p> | <p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • rapports générés par le système ou captures d'écran montrant la fréquence de changement du mot de passe appliquée par le système ; ou • attestations comportant un renvoi aux procédures documentées ayant été suivies. |
| 5.7 | <p><i>Systèmes électroniques BES à impact élevé et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. <p><i>Systèmes électroniques BES à impact moyen de centres de contrôle et leurs :</i></p> <ol style="list-style-type: none"> 1. EACMS associés ; 2. PACS associés ; et 3. PCA associés. | <p>Lorsque techniquement faisable, soit :</p> <ul style="list-style-type: none"> • limiter le nombre de tentatives d'authentification échouées ou • générer des alertes après un certain nombre de tentatives d'authentification échouées. | <p>Exemples non limitatifs de pièces justificatives :</p> <ul style="list-style-type: none"> • documentation des paramètres de verrouillage de compte ; ou • règles de configuration des alertes indiquant comment le système avise des personnes après un nombre défini de tentatives d'ouverture de session. |

C. Conformité

1. Processus de surveillance de la conformité

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

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

1.2. Conservation des pièces justificatives

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

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

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

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

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

1.4. Autres informations sur la conformité

- Aucune.

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

2. Tableau des éléments de conformité

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Principes directeurs et fondements techniques

Section 4 – Portée de l'applicabilité des normes CIP sur la cybersécurité

La section « 4 Applicabilité » des normes présente de l'information importante pour aider les entités responsables à déterminer la portée d'application des exigences CIP sur la cybersécurité.

La section « 4.1. Entités fonctionnelles » est la liste des entités fonctionnelles de la NERC auxquelles s'applique la norme. Si l'entité est enregistrée au titre d'une ou de plusieurs des entités fonctionnelles énumérées à la section 4.1, alors les normes CIP sur la cybersécurité de la NERC s'appliquent. Il est à noter qu'il y a une restriction à la section 4.1 qui limite l'applicabilité dans le cas des distributeurs à ceux qui détiennent certains types de systèmes et d'équipements énumérés à la section 4.2.

La section « 4.2. Installations » définit la portée des *installations*, systèmes et équipements détenus par l'entité responsable qualifiée à la section 4.1, qui est visée par les exigences de la norme. Tel qu'indiqué à la section exemption 4.2.3.5, cette norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou à impact moyen selon la catégorisation de la CIP-002-5. Outre l'ensemble des *installations* du BES, des *centres de contrôle* et des autres systèmes et équipements, la liste comprend l'ensemble des systèmes et équipements détenus par les distributeurs. Bien que le terme « *installations* » du glossaire de la NERC comprenne déjà la caractéristique BES, l'utilisation additionnelle du terme « BES » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité. Cela établit quels sont les *installations*, systèmes et équipements visés par les normes.

Exigence E1

L'exigence E1 a pour but de réduire la surface d'attaque des *actifs électroniques* en obligeant les entités à désactiver les ports non nécessaires. L'intention du SDT est de faire en sorte que l'entité sache quels ports et services connexes sont accessibles (« ports à l'écoute ») sur ses actifs et systèmes et s'ils sont nécessaires au fonctionnement de l'*actif électronique*, et qu'elle désactive tous les autres ports ou limite l'accès à ceux-ci.

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

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

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

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

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

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

Exigence E2

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

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

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

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

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

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

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

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

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

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

Exigence E3

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

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

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

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

Exigence E4

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

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

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

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

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

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

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

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

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

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

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

Exigence E5

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

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

5.1 Voir la justification de l'exigence.

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

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

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

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

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

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

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

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

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

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

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

Raisonnement :

Pendant l'élaboration de cette norme, les références aux versions antérieures des normes CIP et le raisonnement derrière les exigences et leurs parties étaient intégrés à même la norme. Sur approbation du BOT, cette information a été déplacée à la présente section.

Raisonnement pour E1 :

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

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

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

Justification de la modification : (Partie 1.1)

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

Référence à une version précédente : (Partie 1.2) Nouveau

Justification de la modification : (Partie 1.2)

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

Raisonnement pour E2 :

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

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

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

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

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

Justification des modifications : (Partie 2.1)

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

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

Justification des modifications : (Partie 2.2)

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

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

Justification des modifications : (Partie 2.3)

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

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

Justification des modifications : (Partie 2.4)

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

Raisonnement pour E3 :

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

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

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

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

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

Justification des modifications : (Partie 3.1)

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

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

Justification des modifications : (Partie 3.2)

Voir le sommaire des modifications.

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

Justification des modifications : (Partie 3.3)

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

Raisonnement pour E4 :

La surveillance des événements de sécurité a pour but la détection des accès non autorisés, des activités de reconnaissance et d'autres actes malveillants ciblant les *systèmes électroniques BES*. Elle comprend les activités liées à la constitution, au traitement et à la conservation des journaux de sécurité ainsi que les alertes. Ces journaux peuvent à la fois (1) permettre la détection d'un incident et (2) fournir une preuve utile à l'enquête sur un incident. La conservation des journaux de sécurité est destinée à étayer l'analyse des données post-événement.

Cette exigence ne pénalise pas les échecs de journalisation ; elle précise plutôt les processus à mettre en place pour surveiller les échecs de journalisation et en aviser le personnel.

Sommaire des modifications : À partir des paragraphes 525 et 628 de son ordonnance 706, la FERC demande que l'examen manuel des journaux d'événements de sécurité soit effectué plus régulièrement. La présente exigence combine l'exigence E5 de la norme CIP 005-4 et l'exigence E6 de la norme CIP 007-4 dans une perspective globale. Le principal commentaire reçu à propos de cette exigence au cours de la période de consultation informelle portait sur l'imprécision des termes « événement de sécurité » et « surveillance ».

Les termes « événement de sécurité » et « événements touchant la cybersécurité » sont problématiques parce qu'ils ne s'appliquent pas systématiquement à l'ensemble des plateformes et des applications. Pour clarifier ce terme, le libellé de l'exigence est semblable à celui de la publication 800 53 du NIST, en ce que l'entité doit définir les événements de sécurité pertinents pour le système. Pour quelques événements, il est indiqué explicitement que si un *actif électronique* ou un *système électronique BES* peut les journaliser, alors il doit le faire.

En outre, cette exigence établit des paramètres de surveillance et d'examen des processus. Il est rarement faisable ou productif d'examiner chaque journal des événements de sécurité d'un système. Cette réalité est prise en considération dans le paragraphe 629 de l'ordonnance 706 de la FERC, où un examen manuel des journaux est prescrit. Par conséquent, selon cette exigence, l'examen manuel peut consister en un échantillonnage ou en un résumé des événements de sécurité survenus depuis le dernier examen.

Référence à une version précédente : (Partie 4.1) CIP-005-4, E3 ; CIP-007-4, E5, E5.1.2, E6.1 et E6.3

Justification de la modification : (Partie 4.1)

Cette exigence est dérivée de l'alinéa AU-2 de la publication 800-53, version 3, du NIST, qui oblige les organisations à déterminer quels événements systèmes journaliser à des fins d'intervention en cas d'incident. Selon les commentaires officiels reçus au sujet de la norme CIP-011, l'industrie a indiqué une certaine confusion face au terme « événements systèmes touchant la cybersécurité ». Les journaux des accès de l'ESP prescrits à l'exigence E3 de la

norme CIP-005-4 et les journaux des accès et des activités des utilisateurs prescrits à l'exigence E5 de la norme CIP-007-5 sont également visés ici.

Référence à une version précédente : (Partie 4.2) CIP-005-4, E3.2 ; CIP-007-4, E6.2

Justification de la modification : (Partie 4.2)

Cette exigence est dérivée des exigences relatives aux alertes, soit l'exigence E3.2 de la norme CIP-005-4 et l'exigence E6.2 de la norme CIP-007-4, en plus de l'alinéa AU-6 de la publication 800-53, version 3, de la NIST. Les versions antérieures des normes CIP exigeaient des alertes en cas de tentatives d'accès non autorisé et de détection d'*incidents de cybersécurité*, qui peuvent être très nombreux et difficiles à déterminer au jour le jour. Les modifications à cette exigence permettent à l'entité de déterminer quels événements nécessitent une intervention.

Référence à une version précédente : (Partie 4.3) CIP-005-4, E3.2 ; CIP-007-4, E6.4

Justification des modifications : (Partie 4.3)

Aucune modification importante.

Référence à une version précédente : (Partie 4.4) CIP-005-4, E3.2 ; CIP-007-4, E6.5

Justification de la modification : (Partie 4.4)

À partir des paragraphes 525 et 628 de son ordonnance 706, la FERC demande que l'examen manuel des journaux des événements de sécurité soit effectué plus régulièrement et suggère un examen hebdomadaire. Dans cette ordonnance, la FERC reconnaît qu'il est rarement faisable d'examiner tous les journaux systèmes. En effet, l'examen des journaux est un processus dynamique qui doit s'améliorer avec le temps et à la lumière de nouveaux renseignements sur les menaces. Selon les modifications à la présente exigence, un examen d'un résumé ou d'un échantillon des journaux peut être effectué environ toutes les deux semaines.

Raisonnement pour E5 :

Faire en sorte qu'aucune personne autorisée ne puisse obtenir un accès électronique à un *système électronique BES* à moins d'être authentifiée, c'est-à-dire sans que ses renseignements d'authentification n'aient été validés. L'exigence E5 cherche aussi à réduire le risque que des mots de passe statiques utilisés comme facteur d'authentification soient compromis.

L'exigence 5.1 vise à assurer que tout *système électronique BES* et tout *actif électronique* authentifie les personnes pouvant modifier l'information de configuration. Cette exigence porte notamment sur la configuration de l'authentification. L'autorisation des personnes est aussi abordée ailleurs dans les normes CIP sur la cybersécurité. L'accès utilisateur interactif exclut l'accès à de l'information en lecture seule pour lequel la configuration de l'*actif électronique* ne peut être changée (afficheur intégré, rapports Web, etc.). Si un dispositif n'est pas en mesure d'assurer l'authentification, pour des raisons techniques ou opérationnelles, l'entité doit démontrer que tous les chemins d'accès utilisateur interactif distants et locaux sont configurés

de manière à assurer l'authentification. La sécurité physique est suffisante comme configuration des accès locaux si elle est en mesure d'enregistrer l'identité des personnes qui se trouvent dans le *périmètre de sécurité physique* à tout moment.

L'exigence 5.2 porte sur les comptes par défaut et autres comptes génériques. Le fait que l'entité consigne quelle l'utilisation est faite des comptes par défaut et autres comptes génériques pouvant causer des vulnérabilités a l'avantage de faire en sorte qu'elle comprenne le risque éventuel représenté par ces comptes pour le *système électronique BES*. Cette partie d'exigence évite de prescrire une intervention sur ces comptes parce que la solution la plus efficace dépend de chaque situation et que la suppression ou la désactivation du compte pourrait nuire à la fiabilité.

L'exigence 5.3 porte sur les personnes ayant accès aux comptes communs. L'objectif est de neutraliser le risque d'accès non autorisé par l'intermédiaire de comptes communs. Cette exigence est différente de celles d'autres normes CIP sur la cybersécurité visant l'autorisation de l'accès. Une entité peut autoriser l'accès sans savoir qui a accès à un compte partagé. L'entité qui n'aurait pas la liste des personnes ayant accès aux comptes communs pourrait difficilement retirer ces droits d'accès à quiconque n'en a plus besoin. Le terme « autorisé » est employé dans l'exigence pour préciser que le fait qu'une personne enregistre ou perde un mot de passe ou qu'elle le partage sans autorisation ne constitue pas une non-conformité en vertu de cette exigence.

L'exigence 5.4 porte sur les mots de passe par défaut. Leur modification élimine une vulnérabilité facilement exploitable de nombreux systèmes et applications. Les mots de passe pseudo-aléatoires générés par le système ne sont pas considérés comme des mots de passe par défaut.

En ce qui concerne l'authentification des utilisateurs par mot de passe, l'utilisation de mots de passe forts et leur modification périodique contribuent à atténuer le risque de réussite des attaques de craquage de mots de passe ainsi que le risque de divulgation accidentelle de mots de passe à des personnes non autorisées. L'équipe de rédaction a envisagé plusieurs approches pour rendre cette exigence assez efficace et flexible pour permettre aux entités responsables de prendre les bonnes décisions en matière de sécurité. L'une des approches envisagées consistait à exiger une entropie minimale pour les mots de passe ; or, le calcul de la véritable entropie d'information est beaucoup plus complexe et se fonde sur plusieurs hypothèses concernant le choix de mots de passe par les utilisateurs. Ces derniers peuvent choisir des mots de passe faibles dont l'entropie est nettement inférieure au minimum calculé.

L'équipe de rédaction a aussi choisi de ne pas exiger d'exceptions liées à la faisabilité technique pour les dispositifs qui ne respectent pas les paramètres de longueur et de complexité des mots de passe. L'objectif de cette exigence est d'appliquer une politique de mot de passe mesurable afin de prévenir les tentatives de craquage ; le remplacement de dispositifs simplement pour respecter une politique précise sur les mots de passe n'atteint pas cet objectif. Cependant, l'exigence a été renforcée de manière à exiger le verrouillage de comptes ou la génération d'alertes en cas d'échec d'ouverture de session, ce qui permet généralement de mieux atteindre l'objectif visé.

L'exigence de changement des mots de passe permet de contrer la situation où une tentative de craquage aurait réussi à décoder un mot de passe chiffré, ainsi que de remplacer tout rafraîchir tous les mots de passe qui auraient été divulgués accidentellement au fil du temps. L'exigence donne à l'entité le loisir de préciser quelle fréquence de changement des mots de passe permet d'atteindre l'objectif. En particulier, l'équipe de rédaction a jugé plus efficace que la fréquence soit déterminée en fonction de plusieurs facteurs plutôt que d'être fixée pour tous les *systèmes électroniques BES* visés par la norme. En général, les mots de passe servant à l'authentification des utilisateurs doivent être changés au moins une fois par année. Cette fréquence peut parfois être réduite : ainsi, des mots de passe d'applications longs et pseudo-aléatoires pourraient être changés très peu fréquemment. Par ailleurs, les mots de passe employés uniquement comme méthode d'authentification faible d'une application (par exemple, l'accès à la configuration d'un relais) pourraient n'être changés que dans le cadre de l'entretien de routine.

L'*actif électronique* doit appliquer automatiquement la politique sur les mots de passe aux comptes d'utilisateurs individuels. Toutefois, dans le cas des comptes communs pour lesquels il n'existe aucun mécanisme d'application de la politique sur les mots de passe, l'entité responsable peut recourir à des procédures ainsi qu'à une évaluation interne et à un audit.

L'exigence 5.7 aide à prévenir les attaques perpétrées en ligne visant les mots de passe en limitant le nombre de tentatives possible. Il s'agit soit de limiter le nombre de tentatives d'authentification, soit de générer une alerte après un certain nombre d'échecs. Les entités doivent user de prudence avant de limiter le nombre de tentatives d'authentification pour tous les comptes, car cela peut ouvrir la possibilité d'une attaque par déni de service visant le *système électronique BES*.

Sommaire des modifications (par rapport à E5) :

L'exigence E5.3 de la norme CIP 007-4 prescrit l'utilisation de mots de passe et précise une politique d'au moins six caractères combinant caractères alphanumériques et autres. Le niveau de détail dans ces exigences peut par contre limiter le recours à des mesures de sécurité plus efficaces. Ainsi, plusieurs l'ont interprété comme s'appliquant aux mots de passe de jetons ou de systèmes biométriques, ce qui a pu empêcher le recours à ces formes d'authentification plus fortes. En outre, l'utilisation de mots de passe plus longs peut réduire la nécessité d'imposer des règles de complexité. Les exigences relatives aux mots de passe ont été modifiées afin de permettre à l'entité de préciser les paramètres les plus efficaces en fonction de l'impact du *système électronique BES*, du mode d'utilisation des mots de passe et de leur importance pour restreindre l'accès au système. Le SDT croit que ces modifications renforcent le mécanisme d'authentification en obligeant les entités à se pencher sur la façon d'utiliser les mots de passe qui soit la plus efficace dans leur environnement. En effet, l'imposition d'une politique stricte relative aux mots de passe peut limiter l'efficacité des mécanismes de sécurité et empêcher la mise en place de meilleurs mécanismes à l'avenir.

Référence à une version précédente : (Partie 5.1) CIP-007-4, E5

Justification des modifications : (Partie 5.1)

L'exigence d'imposer l'authentification pour tout accès par un utilisateur est incluse ici. L'exigence d'établir, de mettre en œuvre et de documenter les contrôles est incluse dans cette exigence d'introduction. L'exigence d'avoir des contrôles techniques et procéduraux a été supprimée parce que les contrôles techniques sont suffisants lorsqu'une documentation des procédures est déjà exigée. L'expression « qui minimisent les risques d'un accès non autorisé » a été supprimée et est rendue plus adéquatement dans la justification de l'exigence E5.

Référence à une version précédente : (Partie 5.2) CIP-007-4, E5.2 et E5.2.1

Justification des modifications : (Partie 5.2)

La norme CIP-007-4 oblige les entités à limiter l'étendue et à encadrer l'utilisation admise des droits attachés aux comptes. L'exigence de limiter les droits attachés aux comptes a été supprimée parce que la mise en œuvre d'une telle politique est difficile à mesurer.

Référence à une version précédente : (Partie 5.3) CIP-007-4, E5.2.2

Justification des modifications apportées : (Partie 5.3)

Aucune modification importante. Le mot « autorisés » a été ajouté à « accès » pour préciser clairement que le fait qu'une personne enregistre ou perde un mot de passe ou qu'elle le partage sans autorisation ne constitue pas une non-conformité en vertu de cette exigence.

Référence à une version précédente : (Partie 5.4) CIP-007-4, E5.2.1

Justification des modifications : (Partie 5.4)

L'exigence portant sur « le retrait, la désactivation ou le changement de nom des comptes, lorsque cela est possible » a été supprimée et intégrée à une directive sur l'utilisation acceptable des types de comptes. Cette exigence a été supprimée parce que ces actions ne conviennent pas à tous les types de comptes. Ajout de la possibilité de mots de passe par défaut exclusifs pour les cas où un système a généré un mot de passe par défaut ou les cas où un mot de passe par défaut fixe a été figé dans le code au moment de la fabrication du *système électronique BES*.

Référence à une version précédente : (Partie 5.5) CIP-007-4, E5.3

Justification des modifications : (Partie 5.5)

L'exigence E5.3 de la norme CIP-007-4 prescrit l'utilisation de mots de passe et une politique d'une combinaison d'au moins six caractères alphanumériques et spéciaux. Le niveau de détail dans ces exigences peut par contre limiter le recours à des mesures de sécurité plus efficaces. Les exigences relatives aux mots de passe ont été modifiées afin d'autoriser le maximum alloué par le dispositif dans les cas où les paramètres de mot de passe ne permettent pas d'observer une politique plus stricte. Grâce à cette modification, il est tout de même possible d'atteindre l'objectif de l'exigence – réduire le risque de divulgation non autorisée des justificatifs d'identité des mots de passe – tout en reconnaissant que les paramètres de mot de passe seuls ne sont pas suffisants pour y parvenir. L'équipe de rédaction était convaincue que le fait de laisser à l'entité responsable la possibilité d'appliquer la politique de mot de passe la plus stricte permise par un dispositif surpassait la nécessité de surveiller un contrôle plus ou moins efficace au moyen du recours aux TFE.

Référence à une version précédente : (Partie 5.6) CIP-007-4, E5.3.3

Justification des modifications : (Partie 5.6)

*Initialement l'exigence E5.5.3, elle a été déplacée pour permettre l'ajout de « à connectivité externe routable » après « à impact moyen » en réponse aux commentaires. Cette exigence a une portée limitée parce que le risque d'une attaque sur les mots de passe en provenance du réseau est amoindri par l'absence de connectivité externe routable. Le changement fréquent du mot de passe des actifs sur le terrain peut nécessiter un effort important tout en ne réduisant pas beaucoup le risque.

Référence à une version précédente : (Partie 5.7) Nouvelle exigence

Justification des modifications : (Partie 5.7)

La réduction au minimum du nombre des tentatives d'ouverture de session diminue considérablement le risque lié aux tentatives de craquage en temps réel des mots de passe. Dans de telles situations, ce contrôle est plus efficace que les paramètres de mot de passe.

Historique des versions

| Version | Date | Intervention | Suivi des modifications |
|---------|-------------------|---|-------------------------|
| 1 | 16 janvier 2006 | E3.2 — Remplacement de « Control Center » par « control center ». | 24 mars 2006 |
| 2 | 30 septembre 2009 | Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes. Suppression de la mention sur la prise en compte des considérations d'affaires. Remplacement de l'organisation régionale de fiabilité par l'entité régionale comme entité responsable. Reformulation de la date d'entrée en vigueur. Remplacement de « Responsabilité de la surveillance de la conformité » par « Responsable de la surveillance de | |

| | | | |
|---|------------------|---|---|
| | | l'application des normes». | |
| 3 | 16 décembre 2009 | Changement du numéro de version de - 2 à -3. Approbation par le Conseil d'administration de la NERC. | |
| 3 | 31 mars 2010 | Approbation par la FERC. | |
| 4 | 30 décembre 2010 | Modifications visant à ajouter des critères spécifiques pour l'identification des <i>actifs critiques</i> . | Mise à jour |
| 4 | 24 janvier 2011 | Approbation par le Conseil d'administration de la NERC. | Mise à jour |
| 5 | 26 novembre 2012 | Adoption par le Conseil d'administration de la NERC. | Modifiée en coordination avec les autres normes CIP et révision du format selon le gabarit RBS. |
| 5 | 22 novembre 2013 | Émission d'une ordonnance de la FERC approuvant CIP-007-5 (L'ordonnance entre en vigueur le 3 février 2014) | |

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

A. Introduction

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

2. **Numéro :** CIP-007-5

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

Entités fonctionnelles

Aucune disposition particulière

Installations

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

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

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

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

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

6. **Contexte :** Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

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

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

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

1.2. **Conservation des pièces justificatives**

Aucune disposition particulière

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

Aucune disposition particulière

1.4. Autres informations sur la conformité

Aucune disposition particulière

2. Tableau des éléments de conformité

Aucune disposition particulière

D. Différences régionales

Aucune disposition particulière

E. Interprétations

Aucune disposition particulière

F. Documents connexes

Aucune disposition particulière

Principes directeurs et fondements techniques

Aucune disposition particulière

Raisonnement

Aucune disposition particulière

Historique des révisions

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