

A. Introduction

1. **Titre :** Cybersécurité – Mécanismes de gestion de la sécurité
2. **Numéro :** CIP-003-5
3. **Objet :** Définir des mécanismes de gestion de la sécurité cohérents et viables qui établissent les responsabilités et l'imputabilité à l'égard de la protection des *systèmes électroniques BES* contre les compromissions qui pourraient entraîner un fonctionnement incorrect ou des instabilités dans le BES.
4. **Applicabilité :**
 - 4.1. **Entités fonctionnelles :** Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.
 - 4.1.1 **Responsable de l'équilibrage**
 - 4.1.2 **Distributeur** qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du BES :
 - 4.1.2.1 Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :
 - 4.1.2.1.1 fait partie d'un programme de délestage de *charge* qui est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale, et
 - 4.1.2.1.2 effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant humain.
 - 4.1.2.2 Chaque *automatisme de réseau* ou *plan de défense* dans le cas où l'*automatisme de réseau* ou le *plan de défense* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.
 - 4.1.2.3 Chaque *système de protection* applicable au *transport* (excluant les systèmes DSF et DST) dans le cas où le *système de protection* est visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou régionale.
 - 4.1.2.4 Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.
 - 4.1.3 **Exploitant d'installation de production**
 - 4.1.4 **Propriétaire d'installation de production**

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

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

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

4.2.1.1 Chaque système de DSF ou de DST qui :

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

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

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

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

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

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

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

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

- 4.2.3.2** Les actifs électroniques associés aux réseaux de communication et aux liaisons d'échange de données entre périmètres de sécurité électroniques distincts ;
- 4.2.3.3** Les systèmes, structures et composantes régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme à la norme CFR 10, section 73.54 ;
- 4.2.3.4** Dans le cas des *distributeurs*, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus.

5. Dates d'entrée en vigueur :

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

6. Contexte :

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

Le SDT a intégré à la présente norme une reconnaissance à l'effet que certaines exigences ne devraient pas mettre l'accent sur les cas individuels de défaillance comme seul motif d'infraction à la norme. En particulier, le SDT a intégré une approche visant à 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 fait du sens et est communément compris. Par exemple, les processus documentés qui décrivent une réponse sont généralement appelés « plans » (plan d'action en cas d'incident, plan de rétablissement, etc.). De plus, un plan de sécurité peut décrire une approche comportant plusieurs procédures couvrant un thème étendu.

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

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

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

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

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

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

B. Exigences et mesures

- E1.** Chaque entité responsable, pour ses *systèmes électroniques BES* à impact élevé ou moyen, doit revoir et faire approuver par un *cadre supérieur CIP*, au moins une fois tous les 15 mois civils, une ou plusieurs politiques de cybersécurité documentées qui, collectivement, couvrent les thèmes suivants : [*Facteur de risque de la non-conformité : moyen*] [*Horizon : planification de l'exploitation*]
- 1.1** personnel et formation (CIP-004) ;
 - 1.2** *périmètres de sécurité électronique* (CIP-005), y compris l'*accès distant interactif* ;
 - 1.3** sécurité physique des *systèmes électroniques BES* (CIP-006) ;
 - 1.4** gestion de la sécurité des systèmes (CIP-007) ;
 - 1.5** déclaration des incidents et planification des mesures d'intervention (CIP-008) ;
 - 1.6** plans de rétablissement des *systèmes électroniques BES* (CIP-009) ;
 - 1.7** gestion des changements de configuration et analyses de vulnérabilité (CIP-010) ;
 - 1.8** protection de l'information (CIP-011) ; et
 - 1.9** déclaration et réponse aux *circonstances CIP exceptionnelles*.
- M1.** Des exemples de pièces justificatives peuvent comprendre, mais ne sont pas limités à, des documents de politique ; un historique de révisions, des dossiers d'examen ou des preuves de flux de travail provenant d'un système de gestion documentaire qui indiquent l'examen de chaque politique de cybersécurité au moins une fois tous les 15 mois civils ; et l'approbation documentée de chaque politique de cybersécurité par le *cadre supérieur CIP*.
- E2.** Chaque entité responsable doit, pour ses actifs identifiés à la norme CIP-002-5, exigence E1, alinéa E1.3, mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, une ou plusieurs politiques de cybersécurité documentées qui, collectivement, couvrent les thèmes suivants, et doit revoir et faire approuver ces politiques par un *cadre supérieur CIP* au moins une fois tous les 15 mois civils : [*Facteur de risque de la non-conformité : faible*] [*Horizon : planification de l'exploitation*]
- 2.1** sensibilisation à la cybersécurité ;
 - 2.2** contrôles de sécurité physique ;
 - 2.3** contrôle des accès électroniques pour les connexions externes à protocole routable et la *connectivité par lien commuté* ; et
 - 2.4** intervention en cas d'incident de cybersécurité.

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

- M2.** Des exemples de pièces justificatives peuvent comprendre, mais ne sont pas limités à, une ou plusieurs politiques de cybersécurité documentées et des preuves de processus, de procédures ou de plans qui démontrent la mise en oeuvre des thèmes exigés ; historique de révisions, dossiers d'examen ou preuves de flux de travail provenant d'un système de gestion documentaire qui indique l'examen de chaque politique de cybersécurité au moins une fois tous les 15 mois civils ; et approbation documentée de chaque politique de cybersécurité par un *cadre supérieur CIP*.
- E3.** Chaque entité responsable doit désigner un *cadre supérieur CIP* par nom et documenter tout changement dans un délai de 30 jours civils suivant le changement. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]*
- M3.** Un exemple de pièce justificative peut comprendre, mais n'est pas limité à, un document daté et approuvé par un haut dirigeant indiquant le nom de la personne désignée comme *cadre supérieur CIP*.
- E4.** L'entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, un processus documenté de délégation de pouvoirs, sauf en l'absence de toute délégation. Dans les cas permis par les normes CIP, le *cadre supérieur CIP* peut déléguer ses pouvoirs relatifs à certains actes à un ou plusieurs délégués. Ces délégations doivent être documentées, et comprendre notamment le nom ou le titre du délégué, les actes délégués et la date de la délégation ; approuvées par le *cadre supérieur CIP* ; et mises à jour dans un délai de 30 jours suivant tout changement à la délégation. Il n'est pas nécessaire de réaffirmer les changements de délégation en cas de changement de délégant. *[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation]*
- M4.** Un exemple de pièce justificative peut comprendre, mais n'est pas limité à, un document daté et approuvé par le *cadre supérieur CIP* indiquant la ou les personnes (nom ou titre) auxquelles est délégué le pouvoir d'approuver ou d'autoriser des actions décrites explicitement.

C. Conformité

1. Processus de surveillance de la conformité

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

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

1.2. Conservation des pièces justificatives

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

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

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

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

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

1.4. Autres informations sur la conformité

- Aucune

2. Tableau des éléments de conformité

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

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

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

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

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

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

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

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Aucun.

Principes directeurs et fondements techniques

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

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

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

La section « 4.2 Installations » définit la portée des *installations*, systèmes et équipements détenus par l'entité responsable qualifiée à la section 4.1, qui est visée par les exigences de la norme. Outre l'ensemble des *installations* du BES, des *centres de contrôle* et des autres systèmes et équipements, la liste comprend l'ensemble des systèmes et équipements détenus par les distributeurs. Bien que le terme « *installations* » du glossaire de la NERC comprenne déjà la caractéristique BES, l'utilisation additionnelle du terme « BES » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité. Cela établit quels sont les *installations*, systèmes et équipements visés par les normes.

Exigence E1

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

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

1.1 Personnel et formation (CIP-004)

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

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

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

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

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

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

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

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

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

- Obligations de signaler les *incidents de cybersécurité*

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

- Disponibilité des composants de rechange
- Disponibilité des sauvegardes système

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

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

1.8 Protection de l'information (CIP-011)

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

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

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

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

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

Exigence E2

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

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

Exigence E3

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

Exigence E4

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

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

Raisonnement

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

Raisonnement pour E1 :

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

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

Raisonnement pour E2 :

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

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

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

Raisonnement pour E3 :

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

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

Raisonnement pour E4 :

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

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

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	16 janvier 2006	E3.2 — Remplacement de « Control Center » par « control center ».	24 mars 2006
2	30 septembre 2009	Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes. Suppression de la mention sur la prise en compte des considérations d'affaires. Remplacement de l'organisation régionale de fiabilité par l'entité régionale comme entité responsable. Reformulation de la date d'entrée en vigueur. Remplacement de « Responsable de la surveillance de la conformité » par « Responsable de la surveillance de l'application des normes ».	
3	16 décembre 2009	Changement du numéro de version de -2 à -3. Approbation par le Conseil d'administration de la NERC.	
3	31 mars 2010	Approbation par la FERC.	
4	24 janvier 2011	Approbation par le Conseil d'administration de la NERC.	Mise à jour en fonction des changements apportés à la norme CIP-002-4 (projet 2008-06)
5	26 novembre 2012	Adoption par le Conseil d'administration de la NERC.	Modifiée en coordination avec les autres normes CIP et révision du format selon le gabarit RBS.
5	22 novembre 2013	Émission d'une ordonnance de la FERC approuvant CIP-003-5. (L'ordonnance entre en vigueur le 3 février 2014.)	

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

A. Introduction

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

2. **Numéro :** CIP-003-5

3. **Objet :** Aucune disposition particulière

4. **Applicabilité :**

Entités fonctionnelles

Aucune disposition particulière

Installations

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

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