

A. Introduction

1. **Titre :** Cybersécurité — Déclaration des incidents et planification des mesures d'intervention
2. **Numéro :** CIP-008-5
3. **Objet :** Réduire les risques posés au fonctionnement fiable du BES par un *incident de cybersécurité* en définissant des exigences d'intervention en cas d'incident.
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-008-5 :

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 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 ;
- 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-008-5 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-008-5 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-008-5 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.

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 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 CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards

and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- **Systèmes électroniques BES à impact élevé** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », conformément 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.

B. Exigences et mesures

- E1.** Chaque entité responsable doit mettre en œuvre un ou plusieurs plans d'intervention en cas d'*incident de cybersécurité* documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-008-5) – Caractéristiques du plan d'intervention en cas d'*incident de cybersécurité*. [Facteur de risque de la non-conformité : faible]
[Horizon : planification à long terme]
- M1.** Les pièces justificatives doivent comprendre chacun des plans documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-008-5) – Caractéristiques du plan d'intervention en cas d'*incident de cybersécurité*.

Tableau E1 (CIP-008-5) – Caractéristiques du plan d'intervention en cas d'incident de cybersécurité			
Partie	Systèmes visés	Exigences	Mesures
1.1	<i>Systèmes électroniques BES à impact élevé.</i> <i>Systèmes électroniques BES à impact moyen.</i>	Un ou plusieurs processus visant à identifier les <i>incidents de cybersécurité</i> , à les classer et à y répondre.	Exemple non limitatif de pièce justificative : plan ou plans d'intervention en cas d' <i>incident de cybersécurité</i> documentés et datés qui prévoient un processus pour détecter les <i>incidents de cybersécurité</i> , les classer et y répondre.

Tableau E1 (CIP-008-5) – Caractéristiques du plan d'intervention en cas d'incident de cybersécurité			
Partie	Systèmes visés	Exigences	Mesures
1.2	<p><i>Systèmes électroniques BES à impact élevé.</i></p> <p><i>Systèmes électroniques BES à impact moyen.</i></p>	<p>Un ou plusieurs processus visant à déterminer si un <i>incident de cybersécurité</i> identifié est un <i>incident de cybersécurité à déclarer</i> et à aviser l'Electricity Sector Information Sharing and Analysis Center (ES-ISAC), à moins que la loi ne l'interdise.</p> <p>L'ES-ISAC doit recevoir le premier avis (qui peut n'être que préliminaire) concernant un <i>incident de cybersécurité à déclarer</i> dans un délai d'au plus une heure.</p>	<p>Exemples non limitatifs de pièces justificatives : plan ou plans d'intervention en cas d'<i>incident de cybersécurité</i> documentés et datés qui fournissent des indications ou des seuils pour déterminer quels <i>incidents de cybersécurité</i> sont à déclarer ; preuve que des avis préliminaires ont été transmis à l'ES-ISAC.</p>
1.3	<p><i>Systèmes électroniques BES à impact élevé.</i></p> <p><i>Systèmes électroniques BES à impact moyen.</i></p>	<p>Rôles et responsabilités des groupes ou des personnes chargés de l'intervention en cas d'<i>incident de cybersécurité</i>.</p>	<p>Exemple non limitatif de pièce justificative : processus ou procédures d'intervention en cas d'<i>incident de cybersécurité</i> datés qui définissent les rôles et les responsabilités (p. ex., surveillance, déclaration, déclenchement, documentation, etc.) des groupes ou des personnes chargés de l'intervention en cas d'<i>incident de cybersécurité</i>.</p>

Tableau E1 (CIP-008-5) – Caractéristiques du plan d'intervention en cas d'incident de cybersécurité			
Partie	Systèmes visés	Exigences	Mesures
1.4	<i>Systèmes électroniques BES à impact élevé.</i> <i>Systèmes électroniques BES à impact moyen.</i>	Procédures de gestion des <i>incidents de cybersécurité</i> .	Exemples non limitatifs de pièces justificatives : processus ou procédures d'intervention en cas d' <i>incident de cybersécurité</i> datés qui traitent de la gestion des incidents (p. ex., confinement, élimination, reprise après incident ou résolution de l'incident).

- E2.** Chaque entité responsable doit mettre en œuvre chacun de ses plans d'intervention en cas d'*incident de cybersécurité* documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-008-5) – Mise en œuvre et vérification du plan d'intervention en cas d'*incident de cybersécurité*. [*Facteur de risque de la non-conformité : faible*] [*Horizon : planification de l'exploitation et exploitation en temps réel*].
- M2.** Les pièces justificatives doivent comprendre, sans toutefois s'y limiter, des documents qui, collectivement, démontrent la mise en œuvre de toutes les parties d'exigence applicables du tableau E2 (CIP-008-5) – Mise en œuvre et vérification du plan d'intervention en cas d'*incident de cybersécurité*.

Tableau E2 (CIP-008-5) – Mise en œuvre et vérification du plan d'intervention en cas d'incident de cybersécurité

Partie	Systèmes visés	Exigences	Mesures
2.1	<p><i>Systèmes électroniques BES à impact élevé.</i></p> <p><i>Systèmes électroniques BES à impact moyen.</i></p>	<p>Tester chaque plan d'intervention en cas d'<i>incident de cybersécurité</i> au moins une fois tous les 15 mois civils :</p> <ul style="list-style-type: none"> • en répondant à un <i>incident de cybersécurité à déclarer</i> réel ; • en effectuant un exercice sur papier ou sur table de réponse à un <i>incident de cybersécurité à déclarer</i> ; ou • en effectuant un exercice opérationnel de réponse à un <i>incident de cybersécurité à déclarer</i>. 	<p>Exemple non limitatif de pièce justificative : preuve datée de l'existence d'un rapport sur les leçons apprises qui contient un résumé de l'épreuve ou une compilation des notes, des journaux et des communications qui résultent du test. Les types d'exercices peuvent inclure des exercices axés sur les discussions ou sur les opérations.</p>
2.2	<p><i>Systèmes électroniques BES à impact élevé.</i></p> <p><i>Systèmes électroniques BES à impact moyen.</i></p>	<p>Utiliser le ou les plans d'intervention en cas d'<i>incident de cybersécurité</i> cités à l'exigence E1 au moment de répondre à un <i>incident de cybersécurité à déclarer</i> ou d'effectuer un exercice de réponse à un <i>incident de cybersécurité à déclarer</i>. Documenter les écarts entre le ou les plans et les mesures prises pendant l'intervention en cas d'incident ou l'exercice.</p>	<p>Exemples non limitatifs de pièces justificatives : rapports d'incident, journaux et notes prises durant l'intervention en cas d'incident, et documents de suivi décrivant les écarts entre le ou les plans et les mesures prises durant l'intervention en cas d'incident ou l'exercice.</p>

Tableau E2 (CIP-008-5) – Mise en œuvre et vérification du plan d'intervention en cas d'incident de cybersécurité			
Partie	Systèmes visés	Exigences	Mesures
2.3	<p><i>Systèmes électroniques BES à impact élevé.</i></p> <p><i>Systèmes électroniques BES à impact moyen.</i></p>	Conserver les dossiers relatifs aux <i>incidents de cybersécurité à déclarer.</i>	Exemples non limitatifs de pièces justificatives : documents datés, tels que journaux de sécurité, rapports de police, courriels, formulaires d'intervention ou listes de contrôle, résultats d'analyses judiciaires, dossiers de remise en charge et notes d'analyse après incident relativement à des <i>incidents de cybersécurité à déclarer.</i>

- E3.** Chaque entité responsable doit tenir à jour chacun de ses plans d'intervention en cas d'*incident de cybersécurité* conformément à chacune des parties d'exigence applicables du tableau E3 (CIP-008-5) – Examen, mise à jour et communication du plan d'intervention en cas d'*incident de cybersécurité*. *[Facteur de risque de la non-conformité : faible]*
[Horizon : évaluation de l'exploitation]
- M3.** Les pièces justificatives doivent comprendre, sans toutefois s'y limiter, des documents qui, collectivement, démontrent que tous les plans d'intervention en cas d'*incident de cybersécurité* sont tenus à jour conformément aux parties d'exigence applicables du tableau E3 (CIP-008-5) – Examen, mise à jour et communication du plan d'intervention en cas d'*incident de cybersécurité*.

Tableau E3 (CIP-008-5) – Examen, mise à jour et communication du plan d'intervention en cas d'incident de cybersécurité

Partie	Systèmes visés	Exigences	Mesures
3.1	<p><i>Systèmes électroniques BES à impact élevé.</i></p> <p><i>Systèmes électroniques BES à impact moyen.</i></p>	<p>Au plus tard 90 jours civils après la réalisation d'un test des plans d'intervention en cas d'<i>incident de cybersécurité</i> ou après une intervention en cas d'<i>incident de cybersécurité à déclarer</i> réel :</p> <p>3.1.1. documenter les leçons apprises, ou encore l'absence de leçons apprises ;</p> <p>3.1.2. mettre à jour le plan d'intervention en cas d'<i>incident de cybersécurité</i> en tenant compte des leçons apprises documentées qui se rapportent à ce plan ; et</p> <p>3.1.3. aviser chaque personne ou groupe qui joue un rôle défini dans le plan d'intervention en cas d'<i>incident de cybersécurité</i> des mises à jour à ce plan qui tiennent compte des leçons apprises documentées.</p>	<p>Exemples non limitatifs de pièces justificatives :</p> <ol style="list-style-type: none"> documents datés, tels que notes de réunion après incident ou rapports de suivi indiquant les leçons apprises associées à la mise à l'épreuve du ou des plans d'intervention en cas d'<i>incident de cybersécurité</i> ou à une intervention en cas d'<i>incident de cybersécurité à déclarer</i> réelle, ou encore documents datés confirmant l'absence de leçons apprises ; plan d'intervention en cas d'<i>incident de cybersécurité</i> daté et révisé indiquant toutes les modifications apportées en tenant compte des leçons apprises ; et preuve de distribution du plan révisé, par exemple : <ul style="list-style-type: none"> courriels ; « US Postal Service » ou autre service postal ; système de distribution électronique ; ou feuilles de présence aux formations.

Tableau E3 (CIP-008-5) – Examen, mise à jour et communication du plan d'intervention en cas d'incident de cybersécurité

Partie	Systèmes visés	Exigences	Mesures
3.2	<p><i>Systèmes électroniques BES à impact élevé.</i></p> <p><i>Systèmes électroniques BES à impact moyen.</i></p>	<p>Au plus tard 60 jours civils après qu'un changement jugé par l'entité responsable comme ayant un impact sur la capacité d'exécuter le plan a été apporté aux rôles ou responsabilités, aux groupes ou personnes chargés de l'intervention en cas d'<i>incident de cybersécurité</i> ou à une technologie :</p> <p>3.2.1. mettre à jour le ou les plans d'intervention en cas d'<i>incident de cybersécurité</i> ; et</p> <p>3.2.2. aviser des mises à jour chaque personne ou groupe jouant un rôle défini dans le plan d'intervention en cas d'<i>incident de cybersécurité</i>.</p>	<p>Exemples non limitatifs de pièces justificatives :</p> <ol style="list-style-type: none"> 1. plan d'intervention en cas d'<i>incident de cybersécurité</i> révisé et daté incluant les changements apportés aux rôles ou responsabilités, aux intervenants ou à une technologie ; et 2. preuve de distribution du plan révisé, par exemple : <ul style="list-style-type: none"> • courriels ; • « US Postal Service » ou autre service postal ; • système de distribution électronique ; ou • feuilles de présence aux formations.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable 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-008-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	Planification à long terme	Faible	Sans objet	Sans objet	<p>L'entité responsable a élaboré les plans d'intervention en cas d'<i>incident de cybersécurité</i>, mais le plan ne comprend pas les rôles et responsabilités des groupes ou des personnes chargés de l'intervention en cas d'<i>incident de cybersécurité</i>. (1.3)</p> <p>OU</p> <p>L'entité responsable a élaboré les plans d'intervention en cas d'<i>incident de cybersécurité</i>, mais le plan ne comprend pas les procédures de gestion des incidents pour les <i>incidents de cybersécurité</i>. (1.4)</p>	<p>L'entité responsable n'a pas élaboré un plan d'intervention en cas d'<i>incident de cybersécurité</i> comprenant un ou plusieurs processus pour identifier, classifier et répondre aux <i>incidents de cybersécurité</i>. (1.1)</p> <p>OU</p> <p>L'entité responsable a élaboré un plan d'intervention en cas d'<i>incident de cybersécurité</i>, mais le plan ne comprend pas un ou plusieurs processus pour identifier les <i>incidents de cybersécurité à déclarer</i>. (1.2)</p> <p>OU</p> <p>L'entité responsable a</p>

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-008-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						élaboré un plan d'intervention en cas d' <i>incident de cybersécurité</i> , mais n'a pas fourni au moins un avis préliminaire au ES-ISAC dans l'heure suivant l'identification d'un <i>incident de cybersécurité à déclarer</i> . (1.2)
E2	Planification de l'exploitation Exploitation en temps réel	Faible	L'entité responsable n'a pas testé le ou les plans d'intervention en cas d' <i>incident de cybersécurité</i> à l'intérieur de 15 mois civils, sans excéder 16 mois civils entre les tests du plan. (2.1)	L'entité responsable n'a pas testé le ou les plans d'intervention en cas d' <i>incident de cybersécurité</i> à l'intérieur de 16 mois civils, sans excéder 17 mois civils entre les tests du plan. (2.1)	L'entité responsable n'a pas testé le ou les plans d'intervention en cas d' <i>incident de cybersécurité</i> à l'intérieur de 17 mois civils, sans excéder 18 mois civils entre les tests du plan. (2.1) OU L'entité responsable n'a pas documenté les écarts, s'il y en a, par rapport au plan pendant un test ou	L'entité responsable n'a pas testé le ou les plans d'intervention en cas d' <i>incident de cybersécurité</i> à l'intérieur de 18 mois civils entre les tests du plan. (2.1) OU L'entité responsable n'a pas conservé les dossiers pertinents relatifs aux <i>incidents de cybersécurité à déclarer</i> . (2.3)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-008-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
					lorsqu'un <i>incident de cybersécurité</i> à déclarer se produit. (2.2)	
E3	Évaluation de l'exploitation	Faible	L'entité responsable n'a pas avisé chaque personne ou groupe qui joue un rôle défini dans le plan d'intervention en cas d' <i>incident de cybersécurité</i> des mises à jour au plan d'intervention en cas d' <i>incident de cybersécurité</i> à l'intérieur de plus de 90, mais en moins de 120 jours civils suivant un test ou une intervention réelle à un <i>incident de cybersécurité</i> à déclarer. (3.1.3)	L'entité responsable n'a pas mis à jour le plan d'intervention en cas d' <i>incident de cybersécurité</i> en tenant compte des leçons apprises documentées à l'intérieur de 90 à moins de 120 jours civils suivant un test ou une intervention réelle à un <i>incident de cybersécurité</i> à déclarer. (3.1.2) OU L'entité responsable n'a pas avisé chaque personne ou groupe qui joue un rôle défini dans le plan d'intervention en cas	L'entité responsable n'a ni documenté les leçons apprises ni documenté l'absence de leçons apprises à l'intérieur de 90, et en moins de 120 jours civils suivant un test ou une intervention réelle à un <i>incident de cybersécurité</i> à déclarer. (3.1.1) OU L'entité responsable n'a pas mis à jour le plan d'intervention en cas d' <i>incident de cybersécurité</i> en tenant compte des leçons apprises documentées à l'intérieur de 120 jours	L'entité responsable n'a ni documenté les leçons apprises ni documenté l'absence de leçons apprises à l'intérieur de 120 jours civils suivant un test ou une intervention réelle à un <i>incident de cybersécurité</i> à déclarer. (3.1.1)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-008-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				<p><i>d'incident de cybersécurité</i> des mises à jour au plan d'intervention en cas d'<i>incident de cybersécurité</i> à l'intérieur de 120 jours civils suivant un test ou une intervention réelle à un <i>incident de cybersécurité</i> à déclarer. (3.1.3)</p> <p>OU</p> <p>L'entité responsable n'a pas mis à jour le ou les plans d'intervention en cas d'<i>incident de cybersécurité</i> ou avisé chaque personne ou groupe qui joue un rôle défini à l'intérieur de 60, et en moins de 90 jours civils suivant un des changements suivants que l'entité responsable juge comme pouvant</p>	<p>civils suivant un test ou une intervention réelle à un <i>incident de cybersécurité</i> à déclarer. (3.1.2)</p> <p>OU</p> <p>L'entité responsable n'a pas mis à jour le ou les plans d'intervention en cas d'<i>incident de cybersécurité</i> ou avisé chaque personne ou groupe qui joue un rôle défini à l'intérieur de 90 jours civils suivant un des changements suivants que l'entité responsable juge comme pouvant affecter la capacité à exécuter le plan: (3.2)</p> <ul style="list-style-type: none"> • Rôles et responsabilités, ou • Personnes ou groupes d'intervention en 	

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-008-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				affecter la capacité à exécuter le plan: (3.2) <ul style="list-style-type: none"> • Rôles et responsabilités, ou • Personnes ou groupes d'intervention en cas d'<i>incident de cybersécurité</i>, ou • Changements technologiques. 	<i>cas d'incident de cybersécurité</i> , ou Changements technologiques.	

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. 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 :

Les directives suivantes servent de guide pour les éléments que doit comporter un plan d'intervention en cas d'*incident de cybersécurité* :

- Department of Homeland Security, Control Systems Security Program, Developing an Industrial Control Systems Cyber Security Incident Response Capability, 2009, en ligne à l'adresse http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, Computer Security Incident Handling Guide, Special Publication 800-61 revision 1, March 2008, en ligne à l'adresse <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>

À la partie 1.2, un *incident de cybersécurité à déclarer* est un *incident de cybersécurité* qui a compromis ou perturbé une ou plusieurs tâches de fiabilité d'une entité fonctionnelle. Il est à noter que les *incidents de cybersécurité à déclarer* sont ceux qui doivent faire l'objet d'une mesure d'intervention, laquelle peut s'inscrire dans l'une de deux catégories : nécessaire ou facultative. Celles-ci se distinguent par la réponse ou non à un événement. Les mesures de précaution qui ne sont pas adoptées en réponse à des dommages ou à des effets persistants peuvent être classées comme facultatives. Toutes les autres mesures d'intervention prises pour

éviter des dommages persistants ou des effets néfastes, y compris l'activation de systèmes redondants, sont désignées comme requises.

Selon les obligations de déclaration des *incidents de cybersécurité à déclarer*, un avis au moins préliminaire doit être transmis à l'ES-ISAC dans l'heure qui suit la détermination qu'un *incident de cybersécurité* doit être déclaré (et non dans l'heure qui suit l'*incident de cybersécurité*, une distinction importante). Cet ajout vient répondre à la directive traitant de cette question à l'ordonnance 706 de la FERC, paragraphes 673 et 676, qui stipule que la déclaration (au moins préliminaire) doit être faite dans un délai d'au plus une heure. La présente norme n'exige pas la transmission d'un rapport complet dans l'heure qui suit la détermination qu'un *incident de cybersécurité* doit être déclaré, mais d'un avis au moins préliminaire (par exemple, un appel téléphonique, un courriel ou un avis envoyé via le Web). La norme ne précise pas de délai particulier pour achever le rapport.

Exigence E2 :

L'exigence E2 prescrit la mise à l'épreuve périodique du plan d'intervention en cas d'*incident de cybersécurité* par les entités. Ceci comprend l'exigence à la partie 2.2, qui stipule que le plan doit être suivi pendant la mise à l'épreuve. Les exigences de mise à l'épreuve concernent expressément les *incidents de cybersécurité à déclarer*.

Les entités peuvent remplacer la mise à l'épreuve annuelle du plan par une intervention à l'occasion d'un *incident de cybersécurité à déclarer* réel. Autrement, elles doivent mettre le plan à l'épreuve au moyen d'un exercice sur papier, d'un exercice sur table ou d'un exercice opérationnel complet. Le programme Homeland Security Exercise and Evaluation Program (HSEEP) de la Federal Emergency Management Agency (FEMA) présente d'autres types d'exercices, dont les quatre types suivants d'exercices axés sur les discussions : séminaires, ateliers, exercices sur table et jeux. Il définit, en particulier, l'exercice sur table, à savoir « un exercice où des membres clés du personnel se réunissent pour discuter de scénarios de simulation dans un contexte informel. On peut avoir recours à des exercices sur table pour évaluer des plans, des politiques ou des procédures. »

Le programme HSEEP énumère les trois types suivants d'exercices axés sur les opérations : exercice d'entraînement, exercice fonctionnel et exercice à grand déploiement. Il définit, en particulier, l'exercice à grand déploiement, à savoir « un exercice multidisciplinaire, intergouvernemental et multi-agences qui donne lieu à des interventions fonctionnelles (p. ex., bureaux locaux conjoints, centres des opérations d'urgence, etc.) et sur le terrain (p. ex., pompiers décontaminant des mannequins). »

Outre les exigences de mise en œuvre du plan d'intervention, la partie 3.2 stipule que les entités doivent conserver les dossiers des *incidents de cybersécurité à déclarer*. La colonne « Mesures » énumère plusieurs exemples de types de preuve. Les entités devraient consulter leurs procédures de gestion pour déterminer les types de preuve à conserver et la façon de les transporter et de les stocker. Pour plus d'information relativement à la conservation des dossiers sur les incidents, consulter le guide SP800-86 du NIST, *Guide to Integrating Forensic Techniques into Incident Response*. Celui-ci comprend une section (3.1.2) sur l'acquisition de données dans le cadre d'une analyse judiciaire.

Exigence E3 :

Cette exigence prescrit la tenue à jour par les entités de leurs plans d'intervention en cas d'*incident de cybersécurité*. Deux parties dans les exigences requièrent la mise à jour d'un plan : (1) les leçons apprises, à la partie 3.1, et (2) les changements organisationnels ou technologiques, à la partie 3.2.

La documentation des leçons apprises, à la partie 3.1, concerne les *incidents de cybersécurité à déclarer* et les activités illustrées à la figure 1 ci-dessous. Elle doit débuter à la fin de l'incident, en reconnaissant que les mesures d'intervention peuvent prendre des jours sinon des semaines à être mises en place dans le cas d'incidents complexes mettant en jeu des systèmes complexes. Durant le processus d'intégration des leçons apprises, l'équipe d'intervention peut être amenée à discuter de l'incident en vue de déterminer les lacunes ou les points à améliorer dans le plan. Tout écart documenté au plan, mentionné à la partie 2.2, peut faire partie des leçons apprises. Il est possible qu'aucune leçon apprise documentée ne soit associée à un *incident de cybersécurité à déclarer*. Dans un tel cas, l'entité doit conserver les documents attestant l'absence de leçons apprises associées à cet incident.

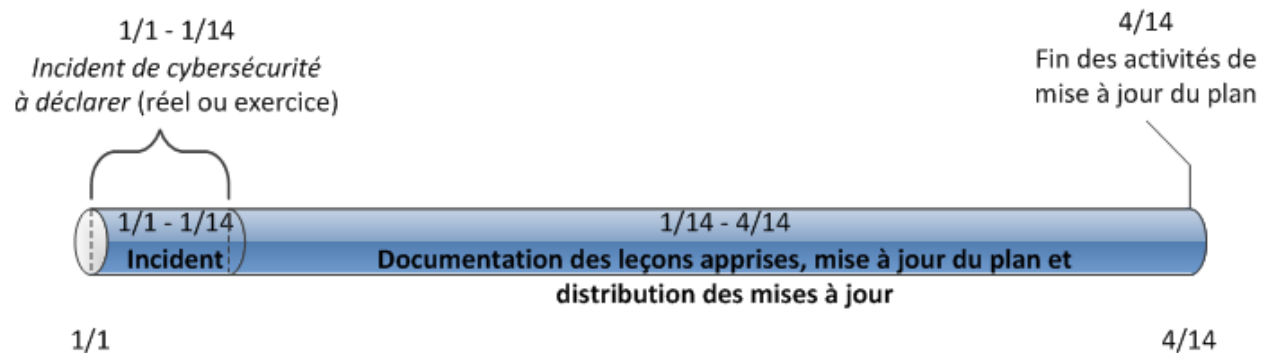


Figure 1 : Calendrier de CIP-008-5 E3 pour les incidents de cybersécurité à déclarer

Les activités nécessaires pour intégrer les leçons apprises au plan comprennent notamment la mise à jour du plan et la distribution de ces mises à jour. Les entités doivent envisager de rencontrer toutes les personnes concernées par l'incident et de documenter les leçons apprises aussitôt que possible après qu'il se produit. On disposera ainsi d'un plus long délai pour mettre à jour le plan, obtenir les approbations requises et distribuer ces mises à jour à l'équipe d'intervention en cas d'incident.

L'exigence de la partie 3.2 portant sur la révision du plan concerne les changements organisationnels et technologiques aux éléments touchés par le plan et vise les activités illustrées à la figure 2 ci-dessous. Parmi les changements organisationnels, on compte les changements apportés aux rôles et responsabilités des personnes définies dans le plan ou aux groupes ou personnes chargés de l'intervention. Il peut s'agir de changements apportés à des noms ou à des coordonnées cités dans le plan. Les changements technologiques qui ont une incidence sur le plan peuvent être des changements apportés à des sources d'information, à des systèmes de communication ou à des systèmes d'établissement de tickets.

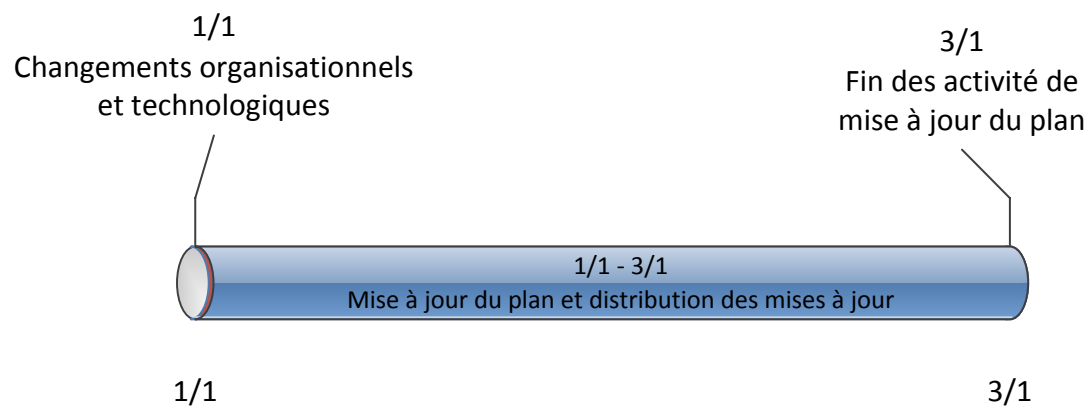


Figure 2 : Calendrier de révision du plan de 3.2.

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 :

La mise en œuvre d'un plan d'intervention efficace en cas d'*incident de cybersécurité* réduit les risques posés au fonctionnement fiable du BES par un *incident de cybersécurité* et procure aux entités responsables une rétroaction qui leur permet d'améliorer les mesures de sécurité relatives aux *systèmes électroniques BES*. Les activités de prévention peuvent limiter le nombre d'incidents, sans toutefois tous les éliminer. Il est donc essentiel de se doter d'une stratégie préétablie d'intervention en cas d'incident en vue de détecter rapidement les incidents, de limiter les pertes et la destruction, de combler les lacunes exploitées et de rétablir les services informatiques. Cette exigence peut être remplie au moyen d'un plan d'entreprise ou d'un seul plan d'intervention pour l'ensemble des *systèmes électroniques BES*. Une organisation peut disposer d'un plan commun pour de multiples entités visées qu'elle détient.

Sommaire des modifications : Des modifications, tenant compte essentiellement des commentaires formulés par l'industrie, ont été apportées au libellé pour décrire plus précisément les mesures à suivre.

Référence à une version précédente : (Partie 1.1) CIP-008, E1.1

Description et justification des modifications : (Partie 1.1)

Remplacement de « caractériser » par « identifier » et de « mesures d'intervention » par « répondre » aux fins de clarification.

Référence à une version précédente : (Partie 1.2) CIP-008, E1.1

Description et justification des modifications : (Partie 1.2)

Prise en compte des exigences de déclaration des versions antérieures de la norme CIP-008. La seule obligation à laquelle doivent se plier les entités, selon la présente partie des exigences, est de disposer d'un processus pour déterminer les *incidents de cybersécurité à déclarer*. Cette partie tient compte aussi de la directive établie dans l'ordonnance 706 de la FERC, aux paragraphes 673 et 676, qui stipule que la déclaration doit être faite dans un délai d'au plus une heure (au moins de façon préliminaire).

Référence à une version précédente : (Partie 1.3) CIP-008, E1.2

Description et justification des modifications : (Partie 1.3)

Remplacement des « équipes d'intervention en cas d'incident » par les « groupes ou personnes » chargés de l'intervention pour éviter l'interprétation selon laquelle les sections portant sur les rôles et responsabilités doivent faire référence à des équipes en particulier.

Référence à une version précédente : (Partie 1.4) CIP-008, E1.2

Description et justification des modifications : (Partie 1.4)

Modification apportée aux fins de conformité pour refléter la redéfinition du terme « *incident de cybersécurité* ».

Raisonnement pour E2 :

La mise en œuvre d'un plan d'intervention efficace en cas d'*incident de cybersécurité* réduit les risques posés à la fiabilité du BES par un tel incident et procure aux entités responsables une rétroaction qui leur permet d'améliorer les mesures de sécurité relatives aux *systèmes électroniques BES*. Cette exigence encadre la mise en œuvre des plans d'intervention. La partie 2.3 de l'exigence prescrit la conservation des documents relatifs à chaque incident aux fins d'analyse ultérieure.

Cette exigence oblige les entités à suivre le plan d'intervention en cas d'*incident de cybersécurité* lorsque se produit un incident ou lors des essais, mais ne les empêche pas de s'écarter du plan en cas de besoin. Elle fait en sorte que le plan représente l'intervention réelle et qu'il n'existe pas aux seules fins de documentation. Si le plan est rédigé de façon assez générale, chaque mesure prise durant l'intervention ne devrait pas être sujette à examen. Le plan devrait tenir compte des différences pertinentes dans les décisions tactiques prises par les personnes ou groupes chargés de l'intervention en cas d'incident. Les écarts par rapport au plan peuvent être documentés durant l'intervention ou après coup, dans le cadre de l'examen.

Sommaire des modifications : Ajout d'exigences de vérification de l'efficacité et de l'application cohérente du plan d'intervention de l'entité responsable en réponse à un ou des *incidents de cybersécurité* ayant un impact sur un *système électronique BES*.

Référence à une version précédente : (Partie 2.1) CIP-008, E1.6

Description et justification des modifications : (Partie 2.1)

Reformulations mineures ; libellé resté pratiquement inchangé.

Référence à une version précédente : (Partie 2.2) CIP-008, E1.6

Description et justification des modifications : (Partie 2.2)

Autorisation des écarts entre le ou les plans et les mesures prises durant des situations réelles ou des épreuves, si ces écarts sont consignés aux fins d'examen.

Référence à une version précédente : (Partie 2.3) CIP-008, E2

Description et justification des modifications : (Partie 2.3)

Suppression des références faites à la période de conservation étant donné que la norme traite de la conservation des données dans la section « Conformité ».

Raisonnement pour E3 :

Effectuer suffisamment d'examen, de mises à jour et de communications pour confirmer l'efficacité et l'application cohérente du plan d'intervention de l'entité responsable en réponse à un ou des *incidents de cybersécurité* ayant un impact sur un *système électronique BES*. Il n'est pas nécessaire de disposer d'un plan distinct pour les parties de l'exigence du tableau s'appliquant aux *systèmes électroniques BES* à impact élevé ou moyen. Si une entité dispose d'un seul plan d'intervention en cas d'*incident de cybersécurité* et détient des *systèmes électroniques BES* à impact élevé et moyen, les exigences supplémentaires s'appliquent à ce plan.

Sommaire des modifications : Les modifications apportées tiennent compte de l'ordonnance 706 de la FERC, paragraphe 686, qui inclut une directive imposant un examen après intervention dans le cadre d'épreuves ou d'incidents réels ainsi qu'une mise à jour du plan tenant compte des leçons apprises. La norme a aussi été modifiée pour préciser ce que sous-entend un examen du plan et les changements qui nécessiteraient une mise à jour du plan.

Référence à une version précédente : (Partie 3.1) CIP-008, E1.5

Description et justification des modifications : (Partie 3.1)

Prise en compte de l'ordonnance 706 de la FERC, paragraphe 686, qui prescrit la documentation des vérifications ou incidents réels et des leçons apprises.

Référence à une version précédente : (Partie 3.2) CIP-008, E1.4

Description et justification des modifications : (Partie 3.2)

Précisions sur les activités nécessaires pour tenir le plan à jour. La version précédente demandait aux entités de mettre le plan à jour après tout changement. Les modifications clarifient les changements qui nécessitent une mise à jour.

Historique des versions

Version	Date	Modification apportée	Suivi des modifications
1	16 janvier 2006	E3.2 — Remplacement de « Control Center » par « control center ».	24 mars 2006
2	30 septembre 2009	Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes. Suppression de la mention sur la prise en compte des considérations d'affaires raisonnables. 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		Changement du numéro de version de -2 à -3. À l'exigence 1.6, suppression de la phrase traitant de la mise hors service d'un composant ou d'un système en vue d'effectuer la vérification conformément à l'ordonnance de la FERC du 30 septembre 2009.	
3	16 décembre 2009	Approbation par le Conseil d'administration de la NERC.	Mise à jour
3	31 mars 2010	Approbation par la FERC.	
4	30 décembre 2010	Ajout de critères précis 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

Version	Date	Modification apportée	Suivi des modifications
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-008-5.	
5	9 juillet 2014	Émission d'une lettre d'ordonnance de la FERC approuvant les révisions aux VRF et VSL de certaines normes CIP.	Exigence E2 de la CIP-008-5, tableau des VSL sous Critique, changé de 19 à 18 mois civils.

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 — Déclaration des incidents et planification des mesures d'intervention
2. **Numéro :** CIP-008-5
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

Annexe QC-CIP-008-5

Dispositions particulières de la norme CIP-008-5 applicables au Québec

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