A. Introduction

1. Titre : Cybersécurité — Plans de rétablissement des systèmes électroniques BES

2. Numéro : CIP-009-5

3. Objet : Rétablir les fonctions de fiabilité exercées par les *systèmes électroniques BES* en définissant les exigences relatives aux plans de rétablissement en vue du maintien de la stabilité, de l'exploitabilité et de la fiabilité du 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 systèmes, *installations* 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 de l'entité régionale, et

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

4.1.2.2 Chaque *automatisme de réseau* 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 de l'entité 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 de l'entité régionale.

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

4.1.3 Exploitant d'installation de production

4.1.4 Propriétaire d'installation de production

4.1.5 Coordonnateur des échanges ou Responsable des échanges

4.1.6 Coordonnateur de la fiabilité

4.1.7 Exploitant de réseau de transport

4.1.8 Propriétaire d'installation de transport

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

4.2.1 Distributeur : Un ou plusieurs des systèmes, *installations* 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 de l'entité 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.

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 de l'entité 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 de l'entité régionale.

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

4.2.2 Entités responsables indiquées en 4.1, sauf les distributeurs :

Toutes les *installations* du BES.

4.2.3 Exemptions : Sont exemptés de la norme CIP-009-5 :

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

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

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

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

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

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

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

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

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

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

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

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

Colonnes « Systèmes visés » des tableaux

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. Le SDT 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.
- **Systèmes électroniques BES à impact moyen situés aux centres de contrôle –** Désigne uniquement les *systèmes électroniques BES* situés aux *centres de contrôle* et classés dans la catégori*e* impact moyen , conformément aux processus d'inventaire et de catégorisation de la norme CIP-002-5.
- **Systèmes de contrôle ou de surveillance des accès électroniques (EACMS)** – Désigne tout *système de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d'authentification, et systèmes de surveillance de registre d'événement et d'alerte.
- **Systèmes de contrôle des accès physiques (PACS)** – Désigne tout *système de contrôle des accès physique*s associé à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.

B. Exigences et mesures

E1. Chaque entité responsable doit disposer d'un ou de plusieurs plans de rétablissement documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-009-5) – Caractéristiques d'un plan de rétablissement. *[Facteur de risque de la non-conformité : moyen] [Horizon : planification à long terme]*

M1. Les pièces justificatives doivent inclure le ou les plans de rétablissement documentés qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E1 (CIP-009-5) – Caractéristiques d'un plan de rétablissement.

Tableau E1 (CIP-009-5) – Caractéristiques d'un plan de rétablissement			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; et 2. PACS associés.	Conditions de déclenchement du ou des plans de rétablissement.	Exemples non limitatifs de pièces justificatives : un ou plusieurs plans de rétablissement où sont énoncées les conditions de déclenchement du ou des plans.
1.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; et 2. PACS associés.	Rôles et responsabilités des intervenants.	Exemples non limitatifs de pièces justificatives : un ou plusieurs plans de rétablissement où sont énoncés les rôles et responsabilités des intervenants.

Tableau E1 (CIP-009-5) – Caractéristiques d'un plan de rétablissement			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
1.3	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; et 2. PACS associés.	Un ou plusieurs processus pour la sauvegarde et le stockage de l'information nécessaire au rétablissement des *systèmes électroniques BES*.	Exemples non limitatifs de pièces justificatives : processus documentés pour la sauvegarde et le stockage de l'information nécessaire au rétablissement des *systèmes électroniques BES*.
1.4	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et leurs : 1. EACMS associés ; et 2. PACS associés.	Un ou plusieurs processus de vérification du bon déroulement des processus de sauvegarde énoncés à la partie 1.3 et de prise en compte des échecs de sauvegarde.	Exemples non limitatifs de pièces justificatives : journaux, preuves d'activité ou autres documents attestant le bon déroulement du processus de sauvegarde et la prise en compte des échecs de sauvegarde, le cas échéant.
1.5	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen et leurs : 1. EACMS associés ; et 2. PACS associés.	Un ou plusieurs processus de conservation des données, selon les capacités des *actifs électroniques*, permettant de déterminer la cause d'un *incident de cybersécurité* qui déclenche le ou les plans de rétablissement. La conservation des données ne doit pas nuire au rétablissement ni le limiter.	Exemples non limitatifs de pièces justificatives : procédures de conservation des données, comme la conservation d'un périphérique de stockage victime de corruption de données, ou la copie miroir des données du système avant d'entreprendre le rétablissement.

E2. Chaque entité responsable doit mettre en œuvre, d'une manière permettant d'identifier, d'évaluer et de corriger les lacunes, son ou ses plans de rétablissement documentés, qui, collectivement, comprennent toutes les parties d'exigence applicables du tableau E2 (CIP-009-5) – Mise en œuvre et essais du plan de rétablissement. *[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-009-5) – Mise en œuvre et essais du plan de rétablissement.

Tableau E2 (CIP-009-5) – Mise en œuvre et essais du plan de rétablissement			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et leurs : 1. EACMS associés ; et 2. PACS associés.	Tester chacun des plans de rétablissement visés par l'exigence E1 au moins une fois tous les 15 mois civils : • En se rétablissant après un incident réel ; • Avec un exercice sur papier ou sur table ; ou • Avec un exercice opérationnel.	Exemples non limitatifs de pièces justificatives : preuve datée de l'existence d'un essai du plan de rétablissement (rétablissement des systèmes après un incident réel, exercice sur papier ou sur table, ou exercice opérationnel) au moins une fois tous les 15 mois civils. Dans le cas de l'exercice sur papier ou de l'exercice opérationnel complet, des avis de réunion, des procès-verbaux ou autres documents consignant les résultats des exercices peuvent constituer des pièces justificatives.

Tableau E2 (CIP-009-5) – Mise en œuvre et essais du plan de rétablissement			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
2.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et leurs : 1. EACMS associés ; et 2. PACS associés.	Tester un échantillon représentatif de l'information nécessaire pour rétablir la fonctionnalité du *système électronique BES* au moins une fois tous les 15 mois civils afin de s'assurer que l'information est utilisable et compatible avec les configurations courantes. Ce test peut être remplacé par un rétablissement suivant un incident réel utilisant l'information nécessaire pour rétablir la fonctionnalité du *système électronique BES*.	Exemples non limitatifs de pièces justificatives : journaux d'exploitation ou résultats de l'essai ainsi que les critères de vérification que l'information est utilisable (p. ex., échantillonner les données sur une bande, parcourir le contenu d'une bande) et de sa compatibilité avec les configurations courantes des systèmes (p. ex., points de comparaison manuels ou automatisés entre le contenu des supports de sauvegarde et la configuration courante).
2.3	*Systèmes électroniques BES* à impact élevé	Tester chacun des plans de rétablissement visés par l'exigence E1 au moins une fois tous les 36 mois civils, en effectuant un exercice opérationnel des plans de rétablissement dans un environnement représentatif de l'environnement de production. Les mesures de rétablissement prises après un incident réel peuvent remplacer l'exercice opérationnel.	Exemples non limitatifs de pièces justificatives : • preuve documentée et datée d'un exercice opérationnel effectué au moins une fois tous les 36 mois civils, qui démontre le rétablissement dans un environnement représentatif ; ou • preuve documentée et datée de mesures de rétablissement prises, dans la fenêtre de 36 mois civils, après un incident réel ayant déclenché les plans de rétablissement.

E3. Chaque entité responsable doit tenir à jour chacun de ses plans de rétablissement conformément à chacune des parties d'exigence applicables du tableau E3 (CIP-009-5) – Examen, mise à jour et communication d'un plan de rétablissement. *[Facteur de risque de la non-conformité : faible] [Horizon : évaluation de l'exploitation]*

M3. Les pièces justificatives acceptables comprennent, sans toutefois s'y limiter, chacune des parties d'exigence applicables du tableau E3 (CIP-009-5) – Examen, mise à jour et communication d'un plan de rétablissement.

Tableau E3 (CIP-009-5) – Examen, mise à jour et communication d'un plan de rétablissement			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.1	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et leurs : 1. EACMS associés ; et 2. PACS associés.	Au plus tard 90 jours civils après la réalisation d'un test de plan de rétablissement ou un rétablissement réel : 3.1.1. documenter toutes les leçons apprises se rapportant au test de plan de rétablissement ou au rétablissement réel, ou documenter l'absence de leçons apprises ; 3.1.2. mettre à jour le plan de rétablissement en tenant compte des leçons apprises documentées associées au plan ; et 3.1.3. aviser chaque personne ou groupe qui joue un rôle défini dans le plan de rétablissement des mises à jour qui ont été apportées au plan de rétablissement en tenant compte des leçons apprises documentées.	Exemples non limitatifs de pièces justificatives : 1. documents datés consignant les lacunes relevées ou les leçons apprises pour chaque test du plan de rétablissement ou chaque rétablissement suivant un incident réel, ou documents datés attestant l'absence de leçons apprises ; 2. plan de rétablissement daté et révisé indiquant toutes les modifications apportées en tenant compte des leçons apprises ; et 3. preuve de distribution du plan révisé, par exemple : • courriels ; • « US Postal Service » ou autre service postal ; • système de distribution électronique ; ou • feuilles de présence aux formations.

Tableau E3 (CIP-009-5) – Examen, mise à jour et communication d'un plan de rétablissement			
Partie	**Systèmes visés**	**Exigences**	**Mesures**
3.2	*Systèmes électroniques BES* à impact élevé et leurs : 1. EACMS associés ; et 2. PACS associés. *Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et leurs : 1. EACMS associés ; et 2. PACS associés.	Au plus tard 60 jours civils après un changement aux rôles ou responsabilités, aux intervenants ou à une technologie que l'entité responsable juge qu'il pourrait avoir un impact sur la capacité d'exécuter le plan de rétablissement : 3.2.1. mettre à jour le plan de rétablissement ; et 3.2.2. aviser des mises à jour chaque personne ou groupe jouant un rôle défini dans le plan de rétablissement.	Exemples non limitatifs de pièces justificatives : 1. plan de rétablissement, révisé et daté, comprenant les changements apportés aux rôles ou responsabilités, aux intervenants ou à une technologie ; et 2. preuve de distribution du plan révisé, par exemple : • 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 des mesures pour assurer la conformité :

L'entité régionale joue le rôle de responsable des mesures pour assurer la conformité (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 de non-conformité
- 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-009-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E1	**Planification à long terme**	**Moyen**	Sans objet	L'entité responsable a élaboré un ou des plans de rétablissement, mais n'a pas traité de l'une des exigences comprises aux parties 1.2 à 1.5.	L'entité responsable a élaboré un ou des plans de rétablissement, mais n'a pas traité de deux des exigences comprises aux parties 1.2 à 1.5.	L'entité responsable n'a pas créé un ou des plans de rétablissement pour les *systèmes électroniques BES*. OU L'entité responsable a créé un ou des plans de rétablissement pour les *systèmes électroniques BES*, mais le ou les plans ne traitent pas des conditions de déclenchement de la partie 1.1. OU L'entité responsable a créé un ou des plans de rétablissement pour les *systèmes électroniques BES*, mais le ou les plans ne

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						traitent pas de trois des exigences des parties 1.2 à 1.5 ou plus.
E2	**Planification de l'exploitation** **Exploitation en temps réel**	**Faible**	L'entité responsable n'a pas testé le ou les plans de rétablissement conformément à la partie 2.1 (E2) à l'intérieur de 15 mois civils, sans dépasser 16 mois civils entre les tests du plan, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.1) OU L'entité responsable n'a pas testé un échantillon représentatif de l'information utilisée pour le rétablissement de la fonctionnalité du	L'entité responsable n'a pas testé le ou les plans de rétablissement conformément à la partie 2.1 (E2) à l'intérieur de 16 mois civils, sans dépasser 17 mois civils entre les tests du plan, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.1) OU L'entité responsable n'a pas testé un échantillon représentatif de l'information utilisée pour le rétablissement de la fonctionnalité du	L'entité responsable n'a pas testé le ou les plans de rétablissement conformément à la partie 2.1 (E2) à l'intérieur de 17 mois civils, sans dépasser 18 mois civils entre les tests du plan, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.1) OU L'entité responsable n'a pas testé un échantillon représentatif de l'information utilisée pour le rétablissement de la fonctionnalité du	L'entité responsable n'a pas testé le ou les plans de rétablissement conformément à la partie 2.1 (E2) à l'intérieur de 18 mois civils entre les tests du plan. (2.1) OU L'entité responsable a testé le ou les plans de rétablissement conformément à la partie 2.1 (E2) et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes. (2.1) OU L'entité responsable a

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
			système électronique BES conformément à la partie 2.2 (E2) à l'intérieur de 15 mois civils, sans dépasser 16 mois civils entre les tests, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.2) OU L'entité responsable n'a pas testé le plan de rétablissement conformément à la partie 2.3 (E2) à l'intérieur de 36 mois civils, sans dépasser 37 mois civils entre les tests, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.3)	*système électronique BES* conformément à la partie 2.2 (E2) à l'intérieur de 16 mois civils, sans dépasser 17 mois civils entre les tests, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.2) OU L'entité responsable n'a pas testé le plan de rétablissement conformément à la partie 2.3 (E2) à l'intérieur de 37 mois civils, sans dépasser 38 mois civils entre les tests, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.3)	*système électronique BES* conformément à la partie 2.2 (E2) à l'intérieur de 17 mois civils, sans dépasser 18 mois civils entre les tests, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.2) OU L'entité responsable n'a pas testé le plan de rétablissement conformément à la partie 2.3 (E2) à l'intérieur de 38 mois civils, sans dépasser 39 mois civils entre les tests, et lorsque testé, toutes les lacunes ont été identifiées, évaluées et corrigées. (2.3)	testé le ou les plans de rétablissement conformément à la partie 2.1 (E2), mais elle n'a pas identifié, évalué ou corrigé les lacunes. (2.1) OU L'entité responsable n'a pas testé un échantillon représentatif de l'information utilisée pour le rétablissement de la fonctionnalité du *système électronique BES* conformément à la partie 2.2 (E2) à l'intérieur de 18 mois civils entre les tests. (2.2) OU L'entité responsable a testé un échantillon représentatif de l'information utilisée

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						pour le rétablissement de la fonctionnalité du *système électronique BES* conformément à la partie 2.2 (E2) et a identifié les lacunes, mais elle n'a pas évalué ou corrigé les lacunes. (2.2) OU L'entité responsable a testé un échantillon représentatif de l'information utilisée pour le rétablissement de la fonctionnalité du *système électronique BES* conformément à la partie 2.2 (E2), mais elle n'a pas identifié, évalué ou corrigé les lacunes. (2.2) OU L'entité responsable n'a pas testé le ou les plans de

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
						rétablissement conformément à la partie 2.3 (E2) à l'intérieur de 39 mois civils entre les tests du plan. (2.3) OU L'entité responsable a testé le ou les plans de rétablissement conformément à la partie 2.3 (E2) et a identifié les lacunes, mais n'a pas évalué ou corrigé les lacunes. (2.3) OU L'entité responsable a testé le ou les plans de rétablissement conformément à la partie 2.3 (E2), mais elle n'a pas identifié, évalué ou corrigé les lacunes. (2.3)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
E3	**Évaluation de l'exploitation**	**Faible**	L'entité responsable n'a pas avisé chaque personne ou groupe jouant un rôle défini dans le ou les plans de rétablissement des mises à jour à l'intérieur de 90 et en moins de 120 jours civils suivant la réalisation complète de la mise à jour. (3.1.3)	L'entité responsable n'a pas mis à jour le ou les plans de rétablissement en tenant compte de toutes leçons apprises documentées à l'intérieur de 90 et en moins de 120 jours civils suivant chaque test de plan de rétablissement ou rétablissement réel. (3.1.2) OU L'entité responsable n'a pas avisé chaque personne ou groupe jouant un rôle défini dans le ou les plans de rétablissement des mises à jour à l'intérieur 120 jours civils suivant la réalisation complète de la mise à jour. (3.1.3)	L'entité responsable n'a ni leçons apprises documentées, ni n'a documenté l'absence de leçons apprises à l'intérieur de 90 et en moins de 120 jours civils suivant chaque test de plan de rétablissement ou rétablissement réel. (3.1.1) OU L'entité responsable n'a pas mis à jour le ou les plans de rétablissement en tenant compte de toutes leçons apprises documentées à l'intérieur de 120 jours civils suivant chaque test de plan de rétablissement ou rétablissement réel. (3.1.2)	L'entité responsable n'a ni leçons apprises documentées, ni n'a documenté l'absence de leçons apprises à l'intérieur de 120 jours civils suivant chaque test de plan de rétablissement ou rétablissement réel. (3.1.1)

E#	Horizon	VRF	Niveaux de gravité de la non-conformité (CIP-009-5)			
			VSL Faible	VSL Modéré	VSL Élevé	VSL Critique
				OU L'entité responsable n'a pas mis à jour le ou les plans de rétablissement ou avisé chaque personne ou groupe jouant 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 qu'il pourrait avoir un impact sur la capacité d'exécuter le plan : (3.2) • Rôles et responsabilités, ou • Intervenants, ou • Changements technologiques.	OU L'entité responsable n'a pas mis à jour le ou les plans de rétablissement ou avisé chaque personne ou groupe jouant un rôle défini à l'intérieur de 90 jours civils suivant un des changements suivants que l'entité responsable juge qu'il pourrait avoir un impact sur la capacité d'exécuter le plan : (3.2) • Rôles et responsabilités, ou • Intervenants, 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 de rétablissement :

- North American Electric Reliability Corporation (NERC). Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions. September 2011. En ligne au http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology (NIST). Contingency Planning Guide for Federal Information Systems. Special Publication 800-34 revision 1, May 2010. En ligne au http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Le terme plan de rétablissement est utilisé dans la présente norme pour désigner un ensemble documenté d'instructions et de ressources nécessaires au rétablissement des fonctions de fiabilité exercées par les *systèmes électroniques BES*. Le plan de rétablissement peut s'inscrire dans un plan global de continuité des activités ou de reprise après sinistre, mais ce terme n'implique pas d'autres obligations associées aux disciplines non visées par les exigences.

Un plan de rétablissement documenté peut ne pas être nécessaire pour chaque *système électronique BES* visé. Par exemple, le plan de rétablissement à court terme d'un *système électronique BES* situé dans un poste électrique donné peut être géré quotidiennement à l'aide d'applications avancées pour les réseaux électriques, telles que l'estimation d'état, les contingences et les mesures correctives ainsi que la gestion prévisionnelle des retraits. Un seul plan de rétablissement de *systèmes électroniques BES* devrait être suffisant pour plusieurs installations similaires, comme celles qu'on retrouve dans les postes électriques ou les centrales.

À la partie 1.1, les conditions de déclenchement du plan de rétablissement doivent tenir compte de menaces viables pour le *système électronique BES*, comme une catastrophe naturelle, une panne de matériel ou d'environnement informatique ou un *incident de cybersécurité*. Une analyse des incidences opérationnelles pour le *système électronique BES* peut s'avérer utile en vue de déterminer ces conditions.

À la partie 1.2, les entités doivent identifier les personnes chargées des mesures de rétablissement du *système électronique BES* visé.

À la partie 1.3, les entités doivent tenir compte des types d'information suivants lors du rétablissement des *systèmes électroniques BES* :

1. fichiers et supports d'installation ;
2. bandes de sauvegarde courantes et autres paramètres de configuration documentés ;
3. procédures documentées d'assemblage ou de restauration ; et
4. stockage de duplication entre les sites.

À la partie 1.4, les processus de vérification du bon déroulement des processus de sauvegarde doivent comprendre notamment : (1) la vérification de l'intégrité des supports de sauvegarde, (2) la vérification des journaux ou une inspection attestant que l'information du système de production courant peut être lue, et (3) la vérification des journaux ou une inspection attestant que l'information a été écrite sur le support de sauvegarde. Cette partie de l'exigence n'impose pas la réalisation d'essais de restauration. Les scénarios de sauvegarde suivants donnent des exemples de processus efficaces pour vérifier le bon déroulement des sauvegardes et déceler les échecs de sauvegarde :

- Processus de sauvegarde périodique (p. ex., quotidienne ou hebdomadaire) – Examen des journaux générés ou des rapports d'état des travaux et mise en place d'avis d'échec de sauvegarde.
- Processus de sauvegarde non périodique – Essai initial et essais périodiques (tous les 15 mois) seulement si une sauvegarde unique est fournie durant la mise en service du système. Essais supplémentaires effectués au besoin, par exemple dans le cadre du programme de gestion des changements de configuration.

- Écriture de données miroir – Configuration d'alertes en cas d'échec de transfert de données pendant un délai précisé par l'entité (p. ex., 15 minutes), après lequel l'information miroir n'est peut-être plus utile aux fins de rétablissement.
- Données de configuration manuelle – Inspection initiale et périodique (tous les 15 mois) des données utilisées pour le rétablissement avant leur stockage. Inspections supplémentaires effectuées au besoin, par exemple dans le cadre du programme de gestion des changements de configuration.

Le plan doit aussi inclure des processus de prise en compte des échecs de sauvegarde, qui précisent les mesures à prendre en cas d'avis d'échec ou de toute autre indication d'un échec.

À la partie 1.5, le plan de rétablissement doit inclure des modalités de conservation des données permettant de déterminer la cause d'un *incident de cybersécurité*. Puisqu'il n'est pas toujours possible de savoir initialement si un *incident de cybersécurité* est ce qui a entraîné le déclenchement du plan de rétablissement, les procédures de conservation des données doivent être suivies tant et aussi longtemps que la possibilité d'un *incident de cybersécurité* n'est pas écartée. La norme CIP-008 traite de la conservation des données associées à ce type d'incident.

Exigence E2 :

Une entité responsable doit tester chaque plan de rétablissement des *systèmes électroniques BES* tous les 15 mois. Toutefois, cela ne veut pas nécessairement dire que l'entité doit mettre à l'essai chaque plan individuel. Les *systèmes électroniques BES* qui sont répartis et en grand nombre, comme ceux qu'on retrouve dans les postes électriques, peuvent ne pas nécessiter un plan de rétablissement individuel et les installations redondantes connexes si les mesures à prendre en cas d'événement grave consistent généralement à reconfigurer et à reconstruire ces systèmes. Inversement, chaque zone de production-transport d'électricité comporte habituellement un centre de contrôle nécessitant une installation redondante ou de repli. Étant donné ces différences, les plans de rétablissement associés aux centres de contrôle diffèrent grandement de ceux qui sont associés aux centrales et aux postes électriques.

Le test d'un plan de rétablissement ne porte pas nécessairement sur tous les aspects du plan ou des scénarios de panne, mais il doit suffire pour s'assurer que le plan est à jour et il doit porter sur au moins un processus de restauration des systèmes électroniques visés.

Les entités peuvent remplacer un test du plan aux 15 mois par un rétablissement suivant un incident réel. Autrement, elles doivent mettre à l'essai le plan au moyen d'un exercice sur papier, d'un exercice sur table ou d'un exercice opérationnel. 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). »

À la partie 2.2, les entités doivent se reporter aux exigences de sauvegarde et de stockage de l'information nécessaire au rétablissement des *systèmes électroniques BES* précisées à la partie 1.3. Cela permet d'offrir une assurance supplémentaire que cette information permettra effectivement de rétablir le *système électronique BES*, le cas échéant. Dans le cas d'équipement informatique complexe, un essai complet de l'information est irréaliste. Les entités doivent alors déterminer l'échantillon représentatif de l'information qui offre une assurance dans les processus mentionnés à la partie 1.3. Cet essai doit comprendre les étapes nécessaires pour s'assurer que l'information est à la fois accessible et courante. Dans le cas des supports de sauvegarde, il peut s'agir d'en mettre à l'essai un échantillon représentatif pour s'assurer que l'information peut être chargée et d'en vérifier le contenu pour s'assurer que l'information reflète la configuration courante des *actifs électroniques* visés.

Exigence E3 :

Cette exigence prescrit la tenue à jour par les entités de leurs plans de rétablissement. Deux parties d'exigence déclenchent la mise à jour d'un plan : (1) les leçons apprises, et (2) les changements organisationnels ou technologiques.

La documentation des leçons apprises concerne chaque déclenchement de plan de rétablissement, et comprend les activités illustrées à la figure 1 ci-dessous. Elle débute à la fin des activités de rétablissement, en reconnaissance du fait que les activités de rétablissement complexes peuvent prendre des jours sinon des semaines à réaliser. Durant le processus d'intégration des leçons apprises, l'équipe de rétablissement peut être amenée à discuter de l'incident en vue de déterminer les lacunes ou les points à améliorer dans le plan. Il est possible qu'aucune leçon apprise documentée ne soit associée à un déclenchement de plan de rétablissement. Dans un tel cas, l'entité doit conserver les documents attestant l'absence de leçons apprises associées à ce déclenchement.

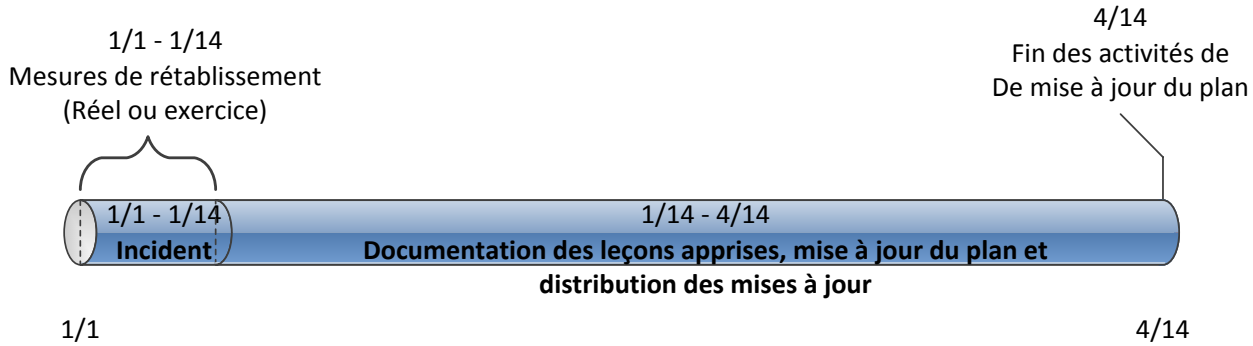

Figure 1 : Calendrier pour E3 CIP-009-5

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 le plan de rétablissement et de documenter les leçons apprises aussitôt que possible après qu'il a été déclenché. 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 de rétablissement.

L'exigence 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 définis dans le plan et 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.

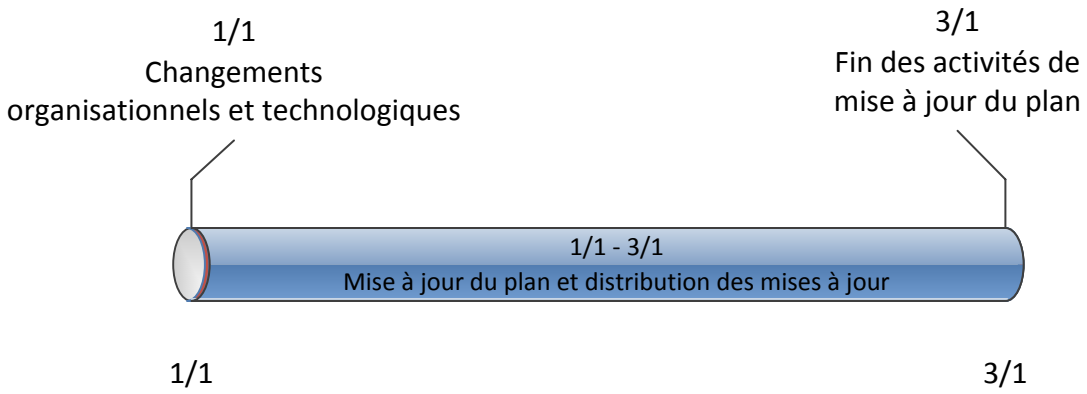

Figure 2 : Calendrier pour les changements au plan de 3.2.

Au moment d'aviser les personnes de changements apportés au plan d'intervention, les entités doivent garder à l'esprit que les plans de rétablissement peuvent être considérés comme de l'information de *système électronique BES*. Elles doivent donc prendre les mesures qui s'imposent pour empêcher la divulgation non autorisée de l'information contenue dans ces plans. Par exemple, le plan de rétablissement lui-même et toute autre information sensible concernant le plan doivent être retranchés des courriels et autres communications non chiffrées.

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 :

Les activités de prévention peuvent limiter le nombre d'incidents, sans toutefois les prévenir tous. Il est donc nécessaire de se doter de moyens pour assurer un rétablissement rapide après les incidents, limiter les pertes et la destruction, combler les lacunes exploitées et rétablir les services informatiques afin que la restauration des fonctionnalités des *systèmes électroniques BES* se fasse de manière cohérente et organisée.

Sommaire des modifications : Ajout de modalités visant la protection des données pouvant être utiles dans le cadre d'une enquête sur un événement qui nécessite le déclenchement d'un plan de rétablissement de systèmes électroniques.

Référence à une version précédente : (Partie 1.1) CIP-009, E1.1

Description et justification des modifications : (Partie 1.1)

Reformulations mineures ; libellé pratiquement inchangé.

Référence à une version précédente : (Partie 1.2) CIP-009, E1.2

Description et justification des modifications : (Partie 1.2)

Reformulations mineures ; libellé pratiquement inchangé.

Référence à une version précédente : (Partie 1.3) CIP-009, E4

Description et justification des modifications : (Partie 1.3)

Prise en compte de l'ordonnance de la FERC, paragraphes 739 et 748. Le texte modifié résume le paragraphe 744.

Référence à une version précédente : (Partie 1.4) Nouvelle exigence

Description et justification des modifications : (Partie 1.4)

Prise en compte de l'ordonnance de la FERC, paragraphes 739 et 748.

Référence à une version précédente : (Partie 1.5) Nouvelle exigence

Description et justification des modifications : (Partie 1.5)

Ajout de l'exigence pour tenir compte de l'ordonnance 706 de la FERC, paragraphe 706.

Raisonnement pour E2 :

La mise en œuvre d'un plan de rétablissement efficace réduit les risques posés fonctionnement fiable du BES en réduisant le délai de rétablissement après différents types d'incidents nuisibles

pour les *systèmes électroniques BES*. Cette exigence encadre la mise en œuvre continue des plans d'intervention.

La partie d'exigence 2.2 offre une assurance supplémentaire quant à l'information (p. ex., bandes de sauvegarde, centres miroir, etc.) nécessaire au rétablissement des *systèmes électroniques BES*. Dans la plupart des cas, une mise à l'épreuve complète du plan est irréaliste en raison de la grande quantité d'information nécessaire au rétablissement. L'entité responsable doit donc déterminer un échantillonnage qui offre l'assurance que l'information est utilisable.

Sommaire des modifications : Ajout d'essais opérationnels du plan de rétablissement des *systèmes électroniques BES*.

Référence à une version précédente : (Partie 2.1) CIP-009, E2

Description et justification des modifications : (Partie 2.1)

Reformulations mineures ; libellé pratiquement inchangé.

Référence à une version précédente : (Partie 2.2) CIP-009, E5

Description et justification des modifications : (Partie 2.2)

Précisions sur ce qui doit être mis à l'essai et clarification du fait qu'un échantillonnage représentatif suffit. Ces modifications, ainsi que l'exigence de la partie 1.4, tiennent compte de l'ordonnance 706 de la FERC, paragraphes 739 et 748, qui porte sur la mise à l'essai des sauvegardes, en offrant un haut degré de confiance que l'information permettra effectivement de rétablir le système au besoin.

Référence à une version précédente : (Partie 2.3) CIP-009, E2

Description et justification des modifications : (Partie 2.3)

Prise en compte de l'ordonnance 706 de la FERC, paragraphe 725, stipulant que le plan de rétablissement doit faire l'objet d'un essai opérationnel complet tous les trois ans.

Raisonnement pour E3 :

Améliorer l'efficacité du ou des plans de rétablissement des systèmes électroniques BES après un essai et assurer la tenue à jour et la distribution de ces plans. Pour ce faire, les entités responsables doivent (i) passer en revue les leçons apprises, à la partie 3.1, et (ii) réviser le plan, selon la partie 3.2, à la suite de changements organisationnels ou technologiques spécifiques qui pourraient avoir un impact sur l'exécution du plan. Dans les deux cas, l'entité responsable doit mettre à jour et distribuer le plan si ce dernier nécessite des modifications.

Sommaire des modifications :

Clarification du moment où les leçons apprises du plan doivent être passées en revue et précision du délai de mise à jour du plan de rétablissement.

Référence à une version précédente : (Partie 3.1) CIP-009, E1 et E3

Description et justification des modifications : (Partie 3.1)

Ajout des délais de documentation des leçons apprises et de mise à jour du plan. Cette exigence regroupe les trois activités en un seul endroit. Tandis que les versions antérieures précisaient un délai de 30 jours civils pour documenter les leçons apprises, suivi d'un autre délai pour mettre à jour les plans de rétablissement et transmettre l'avis, cette exigence regroupe ces activités en une seule période.

Référence à une version précédente : (Partie 3.2) Nouvelle exigence

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. Remplacement de l'organisation régionale de fiabilité par l'entité régionale comme entité responsable. Reformulation de la date d'entrée en vigueur. Remplacement de « Responsabilité de la surveillance de la conformité » par « Responsable des mesures pour assurer la conformité ».	

Version	Date	Modification apportée	Suivi des modifications
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 sur l'identification des *actifs critiques*.	Mise à jour
4	24 janvier 2011	Approbation par le Conseil d'administration de la NERC.	
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-009-5.	
5	9 juillet 2014	Émission d'une lettre d'ordonnance de la FERC approuvant les révisions aux VRF et VSL de certaines normes CIP	Révision des délais contenus dans les VSL de 90-210 jours à 90-120 jours.

Annexe QC-CIP-009-5
Dispositions particulières de la norme CIP-009-5 applicables au Québec

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

A. Introduction

1. Titre : Cybersécurité — Plans de rétablissement des systèmes électroniques BES

2. Numéro : CIP-009-5

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.

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

- Toute installation de production qui répond aux deux conditions suivantes : (1) la puissance nominale de l'installation est de 300 MVA ou moins et (2) aucun groupe de l'installation ne peut être synchronisé avec un réseau voisin.
- Postes élévateurs des installations de production identifiées au point précédent.

5. Date d'entrée en vigueur au Québec :

5.1. Adoption de la norme par la Régie de l'énergie : 29 juillet 2016

5.2. Adoption de l'annexe par la Régie de l'énergie : 29 juillet 2016

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

Pour les entités qui possèdent des actifs classés critiques aux fins des normes CIP (version 1) :

- 1er janvier 2017 pour les systèmes électroniques BES dont l'impact est « moyen » ou « élevé » ;
- 1er octobre 2017 pour les systèmes électroniques BES dont l'impact est « faible ».

Pour les entités qui ne possèdent ni des actifs critiques aux fins de normes CIP (version 1), ni des installations de production à vocation industrielle:

- 1er octobre 2018 pour les systèmes électroniques BES dont l'impact est « moyen » ou « élevé » ;
- 1er octobre 2019 pour les systèmes électroniques BES dont l'impact est « faible ».

Pour les entités qui possèdent des installations de production à vocation industrielle :

- 1er avril 2019 pour les systèmes électroniques BES dont l'impact est « moyen » ou « élevé » ;
- 1er avril 2020 pour les systèmes électroniques BES dont l'impact est « faible ».

6. Contexte : Aucune disposition particulière

B. Exigences et mesures

Aucune disposition particulière

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

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

1.2. Conservation des pièces justificatives

Aucune disposition particulière

1.3. Processus de surveillance et 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	29 juillet 2016	Nouvelle annexe. Décision D-2016-119 émise par la Régie de l'énergie : • Adoption de la norme et son annexe Québec • Suspension de l'application de la norme et de son annexe Québec pour les entités qui possèdent des installations de production à vocation industrielle	Nouvelle
1	16 septembre 2016	Décision D-2016-138 émise par la Régie de l'énergie reportant la date d'entrée en vigueur en ce qui a trait aux systèmes électroniques BES dont l'impact est « moyen » ou « élevé ».	Révision
2	21 mars 2017	Décision D-2017-031 émise par la Régie de l'énergie : • Levée de suspension d'application de la norme et de son annexe Québec pour les entités qui possèdent des installations de production à vocation industrielle • Fixe la date d'entrée en vigueur pour les entités qui possèdent des installations de production à vocation industrielle.	Révision