

## A. Introduction

1. **Titre :** Cybersécurité — Déclaration des incidents et planification des mesures d'intervention
2. **Numéro :** CIP-008-6
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 de la présente norme, les entités fonctionnelles indiquées ci-après sont appelées collectivement « entités responsables ». Si certaines exigences visent plus spécifiquement une entité fonctionnelle ou un sous-ensemble d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.
    - 4.1.1. **Responsable de l'équilibrage**
    - 4.1.2. **Distributeur** qui possède un ou plusieurs des systèmes, *installations* et équipements suivants pour la protection ou la remise en charge du *BES* :
      - 4.1.2.1. Système de délestage de charge en sous-fréquence (DSF) ou en sous-tension (DST) qui :
        - 4.1.2.1.1. fait partie d'un programme de délestage de *charge* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale* ;
        - 4.1.2.1.2. effectue des délestages automatiques de *charge* de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.
      - 4.1.2.2. *Automatisme de réseau (RAS)* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.
      - 4.1.2.3. *Système de protection* de réseau de *transport* (à l'exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale*.
      - 4.1.2.4. *Chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des prochains groupes de production à démarrer.
    - 4.1.3. **Exploitant d'installation de production**
    - 4.1.4. **Propriétaire d'installation de production**
    - 4.1.5. **Coordonnateur de la fiabilité**
    - 4.1.6. **Exploitant de réseau de transport**
    - 4.1.7. **Propriétaire d'installation de transport**

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

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

**4.2.1.1. Système de DSF ou de DST** qui :

**4.2.1.1.1.** fait partie d'un programme de délestage de *charge* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'*entité régionale* ; et

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

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

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

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

**4.2.2. Entités responsables indiquées en 4.1, sauf les *distributeurs*** : Toutes les *installations* du *BES*.

**4.2.3. Exemptions** : Sont exemptés de la norme CIP-008-6 :

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

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

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

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

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

**5. Dates d'entrée en vigueur :**

Voir le plan de mise en œuvre de la norme CIP-008-6.

**6. Contexte :**

La norme CIP-008 fait partie d'une série de normes CIP sur la cybersécurité. La norme CIP-002 exige l'inventaire et la catégorisation initiale des *systèmes électroniques BES*. Les normes CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010 et CIP-011 exigent aussi un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.

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

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité doit inclure tout ce qu'elle le juge nécessaire dans ses processus documentés, en s'assurant de bien couvrir les exigences pertinentes.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », dans la mesure où cela correspond à la compréhension générale. 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 particulier. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont des exemples qui figurent dans les normes. La mise en œuvre complète des normes CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

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

Les mesures auxquelles renvoie l'énoncé initial de l'exigence correspondent simplement aux processus documentés eux-mêmes. La colonne « Mesures » présente des exemples de pièces justificatives attestant la documentation et la mise en œuvre des éléments pertinents dans les processus documentés ; ces exemples sont présentés à titre indicatif, et leur liste ne doit pas être considérée comme exhaustive.

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

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes de DSF et de DST. Ce seuil particulier de 300 MW pour les systèmes de DSF et de DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il

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

#### **Colonne « Systèmes visés » des tableaux**

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. L'équipe de rédaction (SDT) CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- **Systèmes électroniques BES à impact élevé** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon les processus d'inventaire et de catégorisation de la norme CIP-002.
- **Systèmes électroniques BES à impact moyen** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon les processus d'inventaire et de catégorisation de la norme CIP-002.

## 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, couvrent tous les alinéas applicables du tableau E1 (CIP-008-6) – Caractéristiques du plan d'intervention en cas d'*incident de cybersécurité*.

[Facteur de risque de non-conformité : faible] [Horizon : planification à long terme]

**M1.** Les pièces justificatives doivent comprendre chacun des plans documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-008-6) – Caractéristiques du plan d'intervention en cas d'*incident de cybersécurité*.

| Tableau E1 (CIP-008-6) – Caractéristiques du plan d'intervention en cas d' <i>incident de cybersécurité</i> |  |  |   |
|---|--|--|---|
| Alinéa  | Systèmes visés   | Exigences  | Mesures   |
| 1.1   | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ul style="list-style-type: none"> <li>les EACMS associés.</li> </ul> <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ul style="list-style-type: none"> <li>les EACMS associés</li> </ul> | Un ou plusieurs processus visant à détecter 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 ou des processus pour détecter les <i>incidents de cybersécurité</i> , les classer et y répondre. |

| Tableau E1 (CIP-008-6) – Caractéristiques du plan d'intervention en cas d' <i>incident de cybersécurité</i> |   |  |   |
|---|---|--|---|
| Alinéa  | Systèmes visés  | Exigences  | Mesures   |
| 1.2   | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ul style="list-style-type: none"> <li>les EACMS associés.</li> </ul> <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ul style="list-style-type: none"> <li>les EACMS associés.</li> </ul> | <p>Un ou plusieurs processus :</p> <p>1.2.1 qui comprennent des critères d'évaluation servant à reconnaître les tentatives de compromission ;</p> <p>1.2.2 qui visent à déterminer si un <i>incident de cybersécurité</i> constaté est :</p> <ul style="list-style-type: none"> <li>un <i>incident de cybersécurité à signaler</i> ; ou</li> <li>une tentative de compromettre, selon les critères prescrits à l'alinéa 1.2.1, un ou plusieurs systèmes indiqués à la colonne « Systèmes visés » du présent alinéa ; et</li> </ul> <p>1.2.3 qui spécifient une notification selon l'exigence E4.</p> | <p>Exemples non limitatifs de pièces justificatives : plan ou plans d'intervention pour <i>incident de cybersécurité</i> documentés et datés qui fournissent des indications ou des seuils pour déterminer quels <i>incidents de cybersécurité</i> sont aussi un <i>incident de cybersécurité à signaler</i> ou un <i>incident de cybersécurité</i> dont on détermine qu'il constitue une tentative de compromettre un système indiqué à la colonne « Systèmes visés », y compris la justification des critères d'évaluation, ainsi que des processus documentés de notification.</p> |
| 1.3   | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ul style="list-style-type: none"> <li>les EACMS associés.</li> </ul> <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ul style="list-style-type: none"> <li>les EACMS associés.</li> </ul> | <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-008-6) – Caractéristiques du plan d'intervention en cas d' <i>incident de cybersécurité</i> |   |   |   |
|---|---|---|---|
| Alinéa  | Systèmes visés  | Exigences   | Mesures   |
| 1.4   | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ul style="list-style-type: none"> <li>les EACMS associés.</li> </ul> <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ul style="list-style-type: none"> <li>les EACMS associés.</li> </ul> | 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, couvrent tous les alinéas applicables du tableau E2 (CIP-008-6) – Mise en œuvre et vérification du plan d'intervention en cas d'*incident de cybersécurité*.

[Facteur de risque de 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 tous les alinéas applicables du tableau E2 (CIP-008-6) – Mise en œuvre et vérification du plan d'intervention en cas d'*incident de cybersécurité*.

| Tableau E2 (CIP-008-6) – Mise en œuvre et vérification du plan d'intervention en cas d' <i>incident de cybersécurité</i> |   |  |  |
|--|---|--|--|
| Alinéa   | Systèmes visés  | Exigences  | Mesures  |
| 2.1  | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ul style="list-style-type: none"> <li>les <i>EACMS</i> associés.</li> </ul> <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ul style="list-style-type: none"> <li>les <i>EACMS</i> associés.</li> </ul> | <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"> <li>en répondant à un <i>incident de cybersécurité</i> à déclarer réel ;</li> <li>en effectuant un exercice de réponse à un <i>incident de cybersécurité</i> à déclarer, sur papier ou en salle ; ou</li> <li>en effectuant un exercice opérationnel de réponse à un <i>incident de cybersécurité</i> à déclarer.</li> </ul> | <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> |



| Tableau E2 (CIP-008-6) – Mise en œuvre et vérification du plan d'intervention en cas d' <i>incident de cybersécurité</i> |   |  |   |
|--|---|--|---|
| Alinéa   | Systèmes visés  | Exigences  | Mesures   |
| 2.2  | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ul style="list-style-type: none"> <li>les EACMS associés.</li> </ul> <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ul style="list-style-type: none"> <li>les EACMS associés.</li> </ul> | 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> , de répondre à un <i>incident de cybersécurité</i> consistant en une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa 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 à la suite de l'incident ou lors de l'exercice. | Exemples non limitatifs de pièces justificatives : rapports d'incident, journaux et notes prises durant l'intervention à la suite de l'incident, et documents de suivi décrivant les écarts entre le ou les plans et les mesures prises durant l'intervention à la suite de l'incident ou lors de l'exercice.   |
| 2.3  | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ul style="list-style-type: none"> <li>les EACMS associés.</li> </ul> <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ul style="list-style-type: none"> <li>les EACMS associés.</li> </ul> | Conserver les dossiers relatifs aux <i>incidents de cybersécurité à déclarer</i> et aux <i>incidents de cybersécurité</i> consistant en une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa conformément aux plans d'intervention en cas d' <i>incident de cybersécurité</i> spécifiés à l'exigence E1.   | 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 <i>des incidents de cybersécurité à déclarer</i> et à <i>des incidents de cybersécurité</i> consistant en une tentative de compromettre un système indiqué à la colonne « Systèmes visés ». |

- E3.** Chaque entité responsable doit tenir à jour chacun de ses plans d'intervention en cas d'*incident de cybersécurité* conformément à chacun des alinéas applicables du tableau E3 (CIP-008-6) – Examen, mise à jour et communication du plan d'intervention en cas d'*incident de cybersécurité*.  
*[Facteur de risque de non-conformité : faible] [Horizon : évaluation des activités d'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 alinéas applicables du tableau E3 (CIP-008-6) – Examen, mise à jour et communication du plan d'intervention en cas d'*incident de cybersécurité*.

| Tableau E3 (CIP-008-6) – Examen, mise à jour et communication du plan d'intervention en cas d' <i>incident de cybersécurité</i> |   |   |  |
|---|---|---|--|
| Alinéa  | Systèmes visés  | Exigences   | Mesures  |
| 3.1   | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ul style="list-style-type: none"> <li>les <i>EACMS</i> associés.</li> </ul> <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ul style="list-style-type: none"> <li>les <i>EACMS</i> associés.</li> </ul> | <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 réelle en cas d'<i>incident de cybersécurité</i> à déclarer :</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"> <li>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 réelle en cas d'<i>incident de cybersécurité</i> à déclarer, ou encore documents datés confirmant l'absence de leçons apprises ;</li> <li>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</li> <li>preuve de distribution du plan révisé, par exemple : <ul style="list-style-type: none"> <li>courriels ;</li> <li>service postal (US Postal Service ou autre) ;</li> <li>système de distribution électronique ; ou</li> <li>feuilles de présence aux formations.</li> </ul> </li> </ol> |

| Tableau E3 (CIP-008-6) – Examen, mise à jour et communication du plan d'intervention en cas d' <i>incident de cybersécurité</i> |   |  |  |
|---|---|--|--|
| Alinéa  | Systèmes visés  | Exigences  | Mesures  |
| 3.2   | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ul style="list-style-type: none"> <li>les <i>EACMS</i> associés.</li> </ul> <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ul style="list-style-type: none"> <li>les <i>EACMS</i> associés.</li> </ul> | <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"> <li>plan d'intervention en cas d'<i>incident de cybersécurité</i> révisé et daté comprenant les changements apportés aux rôles ou responsabilités, aux intervenants ou à une technologie ; et</li> <li>preuve de distribution du plan révisé, par exemple : <ul style="list-style-type: none"> <li>courriels ;</li> <li>service postal (US Postal Service ou autre) ;</li> <li>système de distribution électronique ; ou</li> <li>feuilles de présence aux formations.</li> </ul> </li> </ol> |

- E4.** Chaque entité responsable doit aviser l'Electricity Information Sharing and Analysis Center (E-ISAC) et aussi, si elle est soumise à la réglementation des États-Unis, le National Cybersecurity and Communications Integration Center (NCCIC)<sup>1</sup> des États-Unis, ou leurs remplaçants éventuels, de tout *incident de cybersécurité à déclarer* et de tout *incident de cybersécurité* qui constitue une tentative de compromettre, selon les critères prescrits à l'alinéa 1.2.1 de l'exigence E1, un système indiqué à la colonne « Systèmes visés », à moins que la loi ne l'interdise, conformément à chacun des alinéas applicables du tableau E4 (CIP-008-6) – Notification et déclaration des incidents de cybersécurité.

[Facteur de risque de non-conformité : faible] [Horizon : évaluation des activités d'exploitation].

- M4.** Les pièces justificatives doivent comprendre, sans toutefois s'y limiter, des documents qui, collectivement, démontrent la notification de chaque *incident de cybersécurité à déclarer* et *incident de cybersécurité* qui constitue une tentative de compromettre un système indiqué à la colonne « Systèmes visés », conformément aux alinéas applicables du tableau E4 (CIP-008-6) – Notification et déclaration des incidents de cybersécurité.

| Tableau E4 (CIP-008-6) – Notification et déclaration des incidents de cybersécurité |   |   |   |
|---|---|---|---|
| Alinéa  | Systèmes visés  | Exigences   | Mesures   |
| 4.1   | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ul style="list-style-type: none"> <li>les EACMS associés.</li> </ul> <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ul style="list-style-type: none"> <li>les EACMS associés.</li> </ul> | <p>Les notifications initiales et leurs mises à jour doivent au minimum préciser les éléments suivants, dans la mesure où ils sont connus :</p> <p>4.1.1 l'impact fonctionnel ;</p> <p>4.1.2 le vecteur d'attaque utilisé ; et</p> <p>4.1.3 le degré d'intrusion atteint ou visé.</p> | <p>Exemples non limitatifs de pièces justificatives : documents datés de notification initiale et de mise à jour transmis à l'E-ISAC et au NCCIC.</p> |

1. Le National Cybersecurity and Communications Integration Center (NCCIC) est l'organisme qui remplace l'Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). En 2017, le NCCIC a réorganisé ses structures en y intégrant des fonctions antérieurement remplies de façon indépendante par l'ICS-CERT et par la United States Computer Emergency Readiness Team (US-CERT).

| Tableau E4 (CIP-008-6) – Notification et déclaration des <i>incidents de cybersécurité</i> |   |   |   |
|--|---|---|---|
| Alinéa   | Systèmes visés  | Exigences   | Mesures   |
| 4.2  | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ul style="list-style-type: none"> <li>les <i>EACMS</i> associés.</li> </ul> <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ul style="list-style-type: none"> <li>les <i>EACMS</i> associés.</li> </ul> | <p>Après la détermination par l'entité responsable selon le ou les processus documentés prescrits à l'alinéa 1.2 de l'exigence E1, transmettre une notification initiale dans les délais suivants :</p> <ul style="list-style-type: none"> <li>une heure après avoir déterminé qu'il s'est produit un <i>incident de cybersécurité</i> à signaler ;</li> <li>au plus tard à la fin du jour civil suivant la détermination qu'un <i>incident de cybersécurité</i> constitue une tentative de compromettre un système indiqué à la colonne « Systèmes visés » du présent alinéa.</li> </ul> | Exemples non limitatifs de pièces justificatives : documents datés de notification transmis à l'E-ISAC et au NCCIC. |
| 4.3  | <p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ul style="list-style-type: none"> <li>les <i>EACMS</i> associés</li> </ul> <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ul style="list-style-type: none"> <li>les <i>EACMS</i> associés</li> </ul>   | Transmettre toute mise à jour pertinente, dans un délai de 7 jours civils après avoir déterminé des ajouts ou des changements aux éléments d'information exigés à l'alinéa 4.1.   | Exemples non limitatifs de pièces justificatives : documents pertinents datés transmis à l'E-ISAC et au NCCIC.      |

## 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 de la conformité et d'application des normes

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

#### 1.4. Autres informations sur la conformité

- Aucune

## 2. Tableau des éléments de conformité

| Ex. | Horizon                    | VRF    | Niveau de gravité de la non-conformité (VSL) (CIP-008-6) |            |  |  |
|-----|----------------------------|--------|--|------------|--|--|
|     |                            |        | VSL faible   | VSL modéré | VSL élevé  | VSL critique   |
| E1. | Planification à long terme | Faible | Sans objet   | Sans objet | <p>L'entité responsable a élaboré un ou des plans d'intervention en cas <i>d'incident de cybersécurité</i>, mais ces plans ne comprennent pas les rôles et responsabilités des groupes ou des personnes chargés de l'intervention en cas <i>d'incident de cybersécurité</i>. (1.3)</p> <p>OU</p> <p>L'entité responsable a élaboré un ou des plans d'intervention en cas <i>d'incident de cybersécurité</i>, mais ces plans ne comprennent pas les procédures de gestion des <i>incidents de cybersécurité</i>. (1.4)</p> <p>OU</p> <p>L'entité responsable a élaboré un plan d'intervention en cas <i>d'incident de cybersécurité</i>, mais ce plan ne comprend pas de processus qui spécifie</p> | <p>L'entité responsable n'a pas élaboré un plan d'intervention en cas <i>d'incident de cybersécurité</i> comprenant un ou plusieurs processus visant à détecter les <i>incidents de cybersécurité</i>, à les classer et à y répondre. (1.1)</p> <p>OU</p> <p>L'entité responsable a élaboré un plan d'intervention en cas <i>d'incident de cybersécurité</i>, mais ce plan ne comprend pas un ou plusieurs processus permettant de reconnaître les <i>incidents de cybersécurité</i> à déclarer ou tout <i>incident de cybersécurité</i> qui constitue une tentative de compromettre, selon les critères prescrits à l'alinéa 1.2.1, un système indiqué à la colonne « Systèmes visés » de l'alinéa 1.2. (1.2)</p> |



| Ex. | Horizon   | VRF    | Niveau de gravité de la non-conformité (VSL) (CIP-008-6)  |   |  |  |
|-----|---|--------|---|---|--|--|
|     |   |        | VSL faible  | VSL modéré  | VSL élevé  | VSL critique   |
|     |   |        |   |   | <p>une notification selon l'exigence E4. (1.4)</p> <p>OU</p> <p>L'entité responsable a élaboré un plan d'intervention en cas <i>d'incident de cybersécurité</i>, mais ce plan ne comprend pas de processus qui spécifie des critères d'évaluation servant à reconnaître les tentatives de compromission. (1.2)</p>   |  |
| E2. | Planification de l'exploitation<br>Exploitation en temps réel | Faible | L'entité responsable n'a pas testé le ou les plans d'intervention en cas <i>d'incident de cybersécurité</i> dans un intervalle de 15 mois civils, sans excéder 16 mois civils, entre les tests du ou des plans. (2.1) | L'entité responsable n'a pas testé le ou les plans d'intervention en cas <i>d'incident de cybersécurité</i> dans un intervalle de 16 mois civils, sans excéder 17 mois civils, entre les tests du ou des plans. (2.1) | <p>L'entité responsable n'a pas testé le ou les plans d'intervention en cas <i>d'incident de cybersécurité</i> dans un intervalle de 17 mois civils, sans excéder 18 mois civils, entre les tests du ou des plans. (2.1)</p> <p>OU</p> <p>L'entité responsable n'a pas documenté les écarts, s'il y en a, par rapport au plan pendant un exercice ou lorsque se produit un <i>incident de cybersécurité à déclarer</i> ou un <i>incident de cybersécurité</i> qui constitue une tentative de</p> | <p>L'entité responsable n'a pas testé le ou les plans d'intervention en cas <i>d'incident de cybersécurité</i> dans un intervalle de 18 mois civils entre les tests du ou des plans. (2.1)</p> <p>OU</p> <p>L'entité responsable n'a pas conservé les dossiers pertinents relatifs aux <i>incidents de cybersécurité à déclarer</i> ou aux <i>incidents de cybersécurité</i> qui constituent une tentative de compromettre un système indiqué à la colonne</p> |

| Ex. | Horizon                      | VRF    | Niveau de gravité de la non-conformité (VSL) (CIP-008-6)  |   |   |   |
|-----|------------------------------|--------|---|---|---|---|
|     |                              |        | VSL faible  | VSL modéré  | VSL élevé   | VSL critique  |
|     |                              |        |   |   | compromettre un système indiqué à la colonne « Systèmes visés » de l'alinéa 2.2. (2.2)  | « Systèmes visés » de l'alinéa 2.3. (2.3)   |
| 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 à ce plan dans un délai de 90 jours civils suivant un test ou une intervention réelle à un <i>incident de cybersécurité à déclarer</i> , mais l'a fait dans un délai de moins de 120 jours civils. (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 dans un délai de 90 jours civils suivant un test ou une intervention réelle à un <i>incident de cybersécurité à déclarer</i> , mais l'a fait dans un délai de moins de 120 jours civils. (3.1.2)<br>OU<br>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 à ce plan dans un délai de 120 jours civils suivant un test ou une intervention réelle à un <i>incident de cybersécurité à déclarer</i> . (3.1.3)<br>OU | L'entité responsable n'a ni documenté les leçons apprises ni documenté l'absence de leçons apprises dans un délai de 90 jours civils suivant un test ou une intervention réelle à un <i>incident de cybersécurité à déclarer</i> , mais l'a fait dans un délai de moins de 120 jours civils. (3.1.1)<br>OU<br>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 dans un délai de 120 jours civils suivant un test ou une intervention réelle à un <i>incident de cybersécurité à déclarer</i> . (3.1.2)<br>OU<br>L'entité responsable n'a pas mis à jour le ou les plans | L'entité responsable n'a ni documenté les leçons apprises ni documenté l'absence de leçons apprises dans un délai de 120 jours civils suivant un test ou une intervention réelle à un <i>incident de cybersécurité à déclarer</i> . (3.1.1) |

| Ex.        | Horizon  | VRF           | Niveau de gravité de la non-conformité (VSL) (CIP-008-6)  |   |  |  |
|------------|--|---------------|---|---|--|--|
|            |  |               | VSL faible  | VSL modéré  | VSL élevé  | VSL critique   |
|            |  |               |   | <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 dans le plan d'intervention dans un délai de 60 jours civils suivant un des changements ci-après que l'entité responsable juge comme ayant un impact sur la capacité à exécuter le plan, mais l'a fait dans un délai de moins de 90 jours civils : (3.2)</p> <ul style="list-style-type: none"> <li>• changements aux rôles et responsabilités ou</li> <li>• changements aux personnes ou groupes intervenant en cas d'<i>incident de cybersécurité</i> ou</li> <li>• changements technologiques.</li> </ul> | <p>d'intervention en cas d'<i>incident de cybersécurité</i> ou avisé chaque personne ou groupe qui joue un rôle défini dans le plan d'intervention dans un délai de 90 jours civils suivant un des changements ci-après que l'entité responsable juge comme ayant un impact sur la capacité à exécuter le plan : (3.2)</p> <ul style="list-style-type: none"> <li>• changements aux rôles et responsabilités ou</li> <li>• changements aux personnes ou groupes intervenant en cas d'<i>incident de cybersécurité</i> ou</li> <li>• changements technologiques.</li> </ul> |  |
| <b>E4.</b> | <b>Évaluation des activités d'exploitation</b> | <b>Faible</b> | L'entité responsable a avisé l'E-ISAC et le NCCIC, ou leurs remplaçants éventuels, d'un <i>incident de cybersécurité</i> qui constitue une tentative de compromettre un système | L'entité responsable n'a pas avisé l'E-ISAC ou le NCCIC, ou leurs remplaçants éventuels, d'un <i>incident de cybersécurité</i> qui constitue, selon les critères prescrits à l'alinéa 1.2.1 de  | L'entité responsable a avisé l'E-ISAC et le NCCIC, ou leurs remplaçants éventuels, d'un <i>incident de cybersécurité à déclarer</i> , mais ne les a pas avisés dans  | L'entité responsable n'a avisé ni l'E-ISAC, ni le NCCIC, ou leurs remplaçants éventuels, d'un <i>incident de cybersécurité à déclarer</i> . (R4) |

| Ex. | Horizon | VRF | Niveau de gravité de la non-conformité (VSL) (CIP-008-6)  |  |  |              |
|-----|---------|-----|---|--|--|--------------|
|     |         |     | VSL faible  | VSL modéré   | VSL élevé  | VSL critique |
|     |         |     | <p>indiqué à la colonne « Systèmes visés » de l'alinéa 4.2, mais sans respecter les délais prescrits à l'alinéa 4.2. (4.2)</p> <p>OU</p> <p>L'entité responsable a avisé l'E-ISAC et le NCCIC, ou leurs remplaçants éventuels, d'un <i>incident de cybersécurité à déclarer</i> ou d'un <i>incident de cybersécurité</i> qui constitue une tentative de compromettre un système indiqué à la colonne « Systèmes visés » de l'alinéa 4.3, mais n'a pas transmis, dans un délai de 7 jours civils après les avoir déterminés, un ou plusieurs des éléments exigés à l'alinéa 4.1, mais non encore déclarés. (4.3)</p> <p>OU</p> <p>L'entité responsable a avisé l'E-ISAC et le NCCIC, ou leurs remplaçants éventuels, d'un <i>incident de cybersécurité à déclarer</i> ou d'un <i>incident de cybersécurité</i> qui constitue</p> | <p>l'exigence E1, une tentative de compromettre un système indiqué à la colonne « Systèmes visés ». (E4)</p> | <p>les délais prescrits à l'alinéa 4.2. (4.2)</p> <p>OU</p> <p>L'entité responsable n'a pas avisé l'E-ISAC ou le NCCIC, ou leurs remplaçants éventuels, d'un <i>incident de cybersécurité à déclarer</i>. (E4)</p> |              |

| Ex. | Horizon | VRF | Niveau de gravité de la non-conformité (VSL) (CIP-008-6)  |            |           |              |
|-----|---------|-----|---|------------|-----------|--------------|
|     |         |     | VSL faible  | VSL modéré | VSL élevé | VSL critique |
|     |         |     | une tentative de compromettre un système indiqué à la colonne « Systèmes visés » de l'alinéa 4.1, mais n'a pas déclaré un ou plusieurs des éléments exigés à l'alinéa 4.1 après les avoir déterminés. (4.1) |            |           |              |

**D. Différences régionales**

Aucune.

**E. Interprétations**

Aucune.

**F. Documents connexes**

Aucun.

## 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 | <p>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.</p> <p>Suppression de la mention sur la prise en compte des considérations d'affaires raisonnables.</p> <p>Remplacement de l'organisation régionale de fiabilité par l'entité régionale comme entité responsable.</p> <p>Reformulation de la date d'entrée en vigueur.</p> <p>Remplacement de « Responsabilité de la surveillance de la conformité » par « Responsable de la surveillance de l'application des normes ».</p> |                         |
| 3       |                   | <p>Changement du numéro de version de -2 à -3.</p> <p>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.</p>  |                         |
| 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 | Ordonnance de la FERC approuvant la norme CIP-008-5.                                       |  |
| 5       | 9 juillet 2014   | Ordonnance de la FERC approuvant les révisions aux VRF et aux VSL de certaines normes CIP. | Exigence E2 de la norme CIP-008-5, tableau des VSL sous Critique, changé de 19 à 18 mois civils. |
| 6       | 6 février 2019   | Adoption par le Conseil d'administration de la NERC.                                       | Changements en réponse aux prescriptions de l'Ordonnance 848 de la FERC.                         |



**Dispositions particulières applicables au Québec visant la norme  
CIP-008-6 — Cybersécurité — Déclaration des incidents et planification des mesures  
d'intervention**

---

La présente annexe établit les dispositions particulières d'application au Québec de la norme qu'elle vise. Les dispositions de la norme visée et de l'annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme visée et l'annexe, l'annexe a préséance.

## **A. Introduction**

1. **Titre :** Aucune disposition particulière
2. **Numéro :** Aucune disposition particulière
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 : xx mois 20xx

5.2. Adoption de l'annexe par la Régie de l'énergie : xx mois 20xx

5.3. Date d'entrée en vigueur de la norme et de l'annexe au Québec : xx mois 20xx

6. **Contexte :** Aucune disposition particulière

## **B. Exigences et mesures**

Aucune disposition particulière

## **C. Conformité**

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

## Annexe CIP-008-6-QC-1

### Dispositions particulières applicables au Québec visant la norme CIP-008-6 — Cybersécurité — Déclaration des incidents et planification des mesures d'intervention

---

#### 1.1. Responsable des mesures pour assurer la conformité

Au Québec, le terme *responsable des mesures pour assurer la conformité* désigne la Régie de l'énergie dans le rôle visant à surveiller la conformité à la norme de fiabilité visée et à la présente annexe, et à assurer l'application de celles-ci.

#### 1.2. Conservation des pièces justificatives

Aucune disposition particulière

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

La Régie de l'énergie établit les processus de surveillance qui servent à évaluer les données ou l'information afin de déterminer la conformité ou la non-conformité avec la norme de fiabilité visée et avec la présente annexe.

#### 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

### Historique des révisions

| Révision | Date d'adoption | Intervention     | Suivi des modifications |
|----------|-----------------|------------------|-------------------------|
| 1        | xx mois 20xx    | Nouvelle annexe. | Nouvelle                |