

## A. Introduction

1. **Titre :** Cybersécurité – Surveillance de sécurité de réseau interne
2. **Numéro :** CIP-015-1
3. **Objet :** Améliorer la probabilité de détection d'activités réseau anormales ou non autorisées afin de renforcer la capacité d'intervention et de rétablissement en cas d'attaque.
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, celles-ci sont précisées explicitement.
    - 4.1.1. **Responsable de l'équilibrage**
    - 4.1.2. **Distributeur** qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du *BES* :
      - 4.1.2.1. 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* ; et
        - 4.1.2.1.2. 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.
      - 4.1.2.2. *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 *installations*, systèmes et équipements suivants détenus par une entité responsable indiquée à la section 4.1 sont visés par ces exigences. Si certaines exigences visent plus spécifiquement un type ou un sous-ensemble d'*installations*, de systèmes ou d'équipements, ceux-ci sont précisés explicitement

**4.2.1. Distributeur :** Les *installations*, systèmes 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 automatiques de *charge* de 300 MW ou plus sous la commande d'un système commun détenu par l'entité responsable, sans intervention humaine.

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

**4.2.1.3.** *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 de fiabilité* CIP-015-1 :

- 4.2.3.1.** les *systèmes électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire ;
- 4.2.3.2.** les *systèmes électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électronique (ESP)* distincts ;
- 4.2.3.3.** les *systèmes électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des systèmes électroniques assurant la confidentialité et l'intégrité des données dans un *ESP* qui s'étend à différents emplacements géographiques ;
- 4.2.3.4.** les systèmes, structures et composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme au règlement CFR 10, section 73.54 ;
- 4.2.3.5.** dans le cas des *distributeurs*, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus ;

- 4.2.3.6.** les entités responsables qui déterminent n'avoir aucun *système électronique BES* classé dans les catégories « impact élevé » ou « impact moyen à *connectivité externe routable (ERC)* » selon les processus d'inventaire et de catégorisation prescrits dans la *norme de fiabilité* CIP-002 ou toute version postérieure.

**5. Date d'entrée en vigueur :** Voir le plan de mise en œuvre de la norme CIP-015-1.

## **B. Exigences et mesures**

- E1.** Chaque entité responsable doit mettre en œuvre un ou des processus documentés, pour la surveillance de sécurité de réseau interne des réseaux protégés par les *périmètres de sécurité électronique* de ses *systèmes électroniques BES* à impact élevé et de ses *systèmes électroniques BES* à impact moyen à *connectivité externe routable*, permettant d'établir des méthodes pour la détection de toute activité réseau anormale et son évaluation. Ce ou ces processus documentés doivent répondre aux prescriptions de chacun des alinéas suivants : *[Facteur de risque de non-conformité : moyen] [Horizon : exploitation le même jour et évaluation des activités d'exploitation]*
- 1.1.** mettre en œuvre, à partir d'une démarche axée sur les risques, d'un ou de plusieurs flux de données réseau afin de surveiller l'activité réseau, en spécifiant les connexions, les dispositifs et les communications réseau ;
- 1.2.** mettre en œuvre une ou des méthodes pour détecter toute activité réseau anormale, à partir des flux de données réseau spécifiés à l'alinéa 1.1 ;
- 1.3.** mettre en œuvre une ou des méthodes permettant d'évaluer toute activité réseau anormale détectée selon l'alinéa 1.2 afin de déterminer les mesures à prendre.
- M1.** Les pièces justificatives doivent couvrir tous les processus documentés qui, collectivement, correspondent aux différents alinéas de l'exigence E1, et attester la mise en œuvre de ces processus. Exemples non limitatifs de pièces justificatives :

### Alinéa 1.1

- Documentation décrivant le ou les flux de données réseau, y compris une justification axée sur les risques expliquant comment ces flux ont été choisis aux fins de la collecte de données.

### Alinéa 1.2

- Documentation de cas de détection d'activité réseau anormale ;
- documentation des paramètres de configuration de systèmes de surveillance de sécurité de réseau interne ;
- documentation de la référence de communication réseau par rapport à laquelle se fait la détection d'activité réseau anormale ; ou
- documentation d'autres moyens de détection d'activité réseau anormale.

### Alinéa 1.3

- Documentation de méthodes d'évaluation d'une activité anormale ;
- documentation de mesures prises à la suite d'une détection d'activité anormale ; ou

- documentation de processus d'escalade pouvant inclure des plans d'intervention en cas d'*incident de cybersécurité* prévus dans la norme CIP-008.

**E2.** Chaque entité responsable doit mettre en œuvre, sauf en cas de *circonstance CIP exceptionnelle*, un ou des processus documentés en vue de conserver les données de surveillance de sécurité de réseau interne associées à une activité réseau jugée anormale par l'entité responsable, au moins jusqu'à ce que les mesures pertinentes prévues à l'alinéa 1.3 de l'exigence E1 aient été prises.  
[Facteur de risque de non-conformité : faible] [Horizon : exploitation le même jour et évaluation des activités d'exploitation]

Remarque : L'entité responsable n'est pas tenue de conserver des données de surveillance de sécurité de réseau interne qui ne sont pas pertinentes à une activité réseau anormale détectée selon l'alinéa 1.2 de l'exigence E1.

**M2.** Exemples non limitatifs de pièces justificatives : documentation du ou des processus de conservation des données de la surveillance de sécurité de réseau interne, configurations de systèmes ou rapports générés automatiquement attestant la conservation des données sur des périodes suffisantes pour la conformité à l'alinéa 1.3 de l'exigence E1.

**E3.** Chaque entité responsable doit mettre en œuvre, sauf en cas de *circonstance CIP exceptionnelle*, un ou des processus documentés visant à protéger les données de surveillance de sécurité de réseau interne collectées aux fins de l'exigence E1, ainsi que les données conservées aux fins de l'exigence E2, contre les risques de modification ou de suppression non autorisée.  
[Facteur de risque de non-conformité : faible] [Horizon : exploitation le même jour et évaluation des activités d'exploitation]

**M3.** Exemples non limitatifs de pièces justificatives : documentation indiquant comment les données de surveillance de sécurité de réseau interne sont protégées contre les risques de modification ou de suppression non autorisée.

## C. Conformité

### 1. Processus de surveillance de la conformité

**1.1. Responsable des mesures pour assurer la conformité :** Le terme « *responsable des mesures pour assurer la conformité* » (CEA) désigne la NERC ou l'*entité régionale*, ou toute entité désignée par un organisme gouvernemental pertinent, dans leurs rôles respectifs visant à surveiller et à assurer la conformité avec les *normes de fiabilité* obligatoires et exécutoires dans leurs territoires respectifs.

**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 attestant sa conformité pendant la période complète écoulée depuis le dernier audit.

L'entité responsable doit conserver les données ou les pièces justificatives attestant sa conformité selon les modalités indiquées ci-après, à moins que son CEA lui demande de conserver certaines pièces justificatives plus longtemps dans le cadre d'une enquête :

- L'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 dossiers du dernier audit ainsi que tous les dossiers d'audit demandés et soumis par la suite.

**1.3. Programme de surveillance de la conformité et d'application des normes :** Selon la définition des règles de procédure de la NERC, l'expression « programme de surveillance de la conformité et d'application des normes » désigne la liste des processus qui serviront à évaluer les données ou l'information afin de déterminer les résultats de conformité avec la *norme de fiabilité*.

**Niveaux de gravité de la non-conformité (VSL)**

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
<b>E1</b>	S. O.	S. O.	<p>L'entité responsable n'a pas mis en œuvre, à partir d'une démarche axée sur les risques, une collecte d'un ou de plusieurs flux de données réseau afin de surveiller l'activité réseau, en spécifiant les connexions, les dispositifs et les communications réseau. (1.1)</p> <p>OU</p> <p>L'entité responsable n'a pas mis en œuvre une ou des méthodes pour détecter toute activité réseau anormale, à partir des flux de données réseau spécifiés à l'alinéa 1.1. (1.2)</p> <p>OU</p> <p>L'entité responsable n'a pas mis en œuvre une ou des méthodes permettant d'évaluer toute activité réseau anormale détectée selon l'alinéa 1.2 afin de déterminer les mesures à prendre. (1.3)</p>	L'entité responsable n'a mis en œuvre aucun des alinéas pertinents en vue de détecter et d'évaluer les activités réseau anormales.

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
<b>E2</b>	S. O.	S. O.	S. O.	L'entité responsable n'a pas mis en œuvre, sauf en cas de <i>circonstance CIP exceptionnelle</i> , un ou des processus documentés en vue de conserver les données de surveillance de sécurité de réseau interne associées à une activité réseau jugée anormale par l'entité responsable, au moins jusqu'à ce que les mesures pertinentes prévues à l'alinéa 1.3 de l'exigence E1 aient été prises.
<b>E3</b>	S. O.	S. O.	S. O.	L'entité responsable n'a pas mis en œuvre, sauf en cas de <i>circonstance CIP exceptionnelle</i> , un ou des processus documentés visant à protéger les données de surveillance de sécurité de réseau interne collectées aux fins de l'exigence E1, ainsi que les données conservées aux fins de l'exigence E2, contre les risques de modification ou de suppression non autorisée.

## D. Différences régionales

Aucune

## E. Documents connexes

Lien vers le plan de mise en œuvre et d'autres documents connexes importants.

## Historique des versions

Version	Date	Intervention	Suivi des modifications
1	9 mai 2024	Approbation par le Conseil d'administration de la NERC.	
1	26 juin 2025	Ordonnance de la FERC approuvant la norme CIP-015-1. Dossier RD24-7-000).	