

A. Introduction

1. **Titre :** Cybersécurité – Protection des informations
2. **Numéro :** CIP-011-3
3. **Objet :** Empêcher tout accès non autorisé aux *informations de système électronique BES* (BCSI) en définissant des exigences de protection des informations visant à prévenir toute compromission pouvant entraîner un fonctionnement incorrect ou une instabilité dans le *système de production-transport d'électricité (BES)*.
4. **Applicabilité :**
 - 4.1. **Entités fonctionnelles :** Dans le contexte de la présente norme, les entités fonctionnelles indiquées ci-après seront 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* ; et
 - 4.1.2.1.2 effectue des délestages de *charge* automatiques de 300 MW 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 groupes de production suivants à démarrer.
 - 4.1.3 **Exploitant d'installation de production**
 - 4.1.4 **Propriétaire d'installation de production**
 - 4.1.5 **Coordonnateur 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 : 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 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 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 CIP-011-3 :

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 composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme au règlement CFR 10, section 73.54.

4.2.3.4 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 n'avoir 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-002-5.1a.

5. Dates d'entrée en vigueur : Voir le plan de mise en œuvre de la norme CIP-011-3.

6. Contexte : La norme CIP-011 fait partie d'une série de normes CIP sur la cybersécurité qui exigent l'inventaire et la catégorisation initiales des *systèmes électroniques BES*, ainsi qu'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 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 la compréhension relève du bon sens. 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 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 *BES*. 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. La SDT (équipe de rédaction)

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 le processus d'inventaire et de catégorisation de la norme CIP-002-5.1a.
- **Systèmes électroniques BES à impact moyen** – Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon le processus d'inventaire et de catégorisation de la norme CIP-002-5.1a.
- **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'événements et d'alerte.
- **Systèmes de contrôle des accès physiques (PACS)** – Désigne tout *système de contrôle des accès physiques* associés à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.
- **Actifs électroniques protégés (PCA)** – Désigne tout *actif électronique protégé* associé à un *système électronique BES* à impact élevé ou moyen visé.

B. Exigences et mesures

- E1.** Chaque entité responsable doit mettre en œuvre un ou plusieurs programmes documentés de protection des *informations de système électronique BES* (BCSI) relatives aux systèmes désignés à la colonne Systèmes visés du tableau E1 (CIP-011-3) – Programme de protection des informations, qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-011-3) – Protection des informations.

[Facteur de risque de la non-conformité : moyen] [Horizon : planification de l'exploitation]

- M1.** Les pièces justificatives du programme de protection des informations doivent couvrir toutes les parties applicables du tableau E1 (CIP-011-3) – Programme de protection des informations ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-011-3) – Programme de protection des informations			
Alinéa	Systèmes visés	Exigences	Mesures
1.1	<p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; et 2. les <i>PACS</i> associés. <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés ; et 2. les <i>PACS</i> associés. 	Méthodes permettant de désigner les BCSI.	<p>Exemples non limitatifs de pièces justificatives acceptables :</p> <ul style="list-style-type: none"> • méthode documentée permettant de désigner les BCSI à partir du programme de protection des informations de l'entité ; • indications sur les informations (étiquetage, classification, etc.) qui permettent de désigner les BCSI telles que désignées dans le programme de protection des informations de l'entité ; • matériel de formation qui donne au personnel des connaissances suffisantes pour reconnaître les BCSI ; ou • emplacements désignés pour le stockage des BCSI dans le cadre du programme de protection des informations de l'entité.

Tableau E1 (CIP-011-3) – Programme de protection des informations			
Alinéa	Systèmes visés	Exigences	Mesures
1.2	<p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés; et 2. les <i>PACS</i> associés. <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés; et 2. les <i>PACS</i> associés. 	Méthodes de protection et de manipulation sécuritaire des BCSI visant à réduire les risques de brèche de confidentialité.	<p>Exemples non limitatifs de pièces justificatives pour les BCSI présentes sur place :</p> <ul style="list-style-type: none"> • procédures pour la protection et la manipulation sécuritaire des BCSI, portant sur des aspects comme le stockage, la sécurité pendant le transport et l'utilisation ; ou • enregistrements indiquant que les BCSI sont manipulées conformément aux procédures documentées de l'entité. <p>Exemples non limitatifs de pièces justificatives pour les BCSI hors site :</p> <ul style="list-style-type: none"> • mise en œuvre de techniques électroniques pour protéger les BCSI électroniques (masquage de données, chiffrement, hachage, tokenisation, système de clés électroniques, etc.) ; ou • mise en œuvre de moyens physiques pour protéger les BCSI physiques (verrouillage physique et gestion des clés, système de cartes d'identification, biométrie, système d'alarme, etc.) ; ou • mise en œuvre de méthodes administratives pour protéger les BCSI (évaluation des risques des fournisseurs de services, ententes commerciales, etc.).

E2. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-011-3) – Réutilisation et élimination des *actifs électroniques BES*.

[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation]

M2. Les pièces justificatives doivent comprendre chacun des processus documentés applicables qui, collectivement, couvrent toutes les parties applicables du tableau E2 (CIP-011-3) – Réutilisation et élimination des *actifs électroniques BES* ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E2 (CIP-011-3) – Réutilisation et élimination des <i>actifs électroniques BES</i>			
Alinéa	Systèmes visés	Exigences	Mesures
2.1	<p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés; 2. les <i>PACS</i> associés; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés; 2. les <i>PACS</i> associés; et 3. les <i>PCA</i> associés. 	Avant d'autoriser la réutilisation d'un <i>actif électronique</i> visé qui contient des BCSI (sauf si cet actif est réutilisé dans d'autres systèmes indiqués à la colonne Systèmes visés), l'entité responsable doit faire en sorte d'empêcher toute récupération non autorisée de BCSI stockées sur le support de stockage de l' <i>actif électronique</i> en question.	<p>Exemples non limitatifs de pièces justificatives acceptables :</p> <ul style="list-style-type: none"> • enregistrements de suivi des mesures d'expurgation visant à empêcher toute récupération non autorisée de BCSI, notamment par écrasement, purge ou destruction ; ou • enregistrements de suivi de mesures comme le cryptage, la rétention dans le <i>périmètre de sécurité physique</i> ou d'autres moyens d'empêcher la récupération non autorisée de BCSI.
2.2	<p><i>Systèmes électroniques BES</i> à impact élevé et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés; 2. les <i>PACS</i> associés; et 3. les <i>PCA</i> associés. <p><i>Systèmes électroniques BES</i> à impact moyen et :</p> <ol style="list-style-type: none"> 1. les <i>EACMS</i> associés; 2. les <i>PACS</i> associés; et 3. les <i>PCA</i> associés. 	Avant l'élimination d'un <i>actif électronique</i> visé qui contient des BCSI, l'entité responsable doit faire en sorte d'empêcher toute récupération non autorisée de BCSI stockées sur l' <i>actif électronique</i> en question, ou encore de détruire son support d'information.	<p>Exemples non limitatifs de pièces justificatives acceptables :</p> <ul style="list-style-type: none"> • enregistrements attestant que le support d'information a été détruit avant l'élimination d'un <i>actif électronique</i> visé ; ou • enregistrements attestant les mesures prises pour empêcher la récupération non autorisée de BCSI d'un <i>actif électronique</i> visé avant son élimination.

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 visée doit conserver les données ou 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 visée doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité visée 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. 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.	Horizon	VRF	Niveaux de gravité de la non-conformité (VSL) (CIP-011-3)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1	Planification de l'exploitation	Moyen	Sans objet	Sans objet	<p>L'entité responsable a documenté mais n'a pas mis en œuvre un ou des programmes de protection des BCSI. (E1)</p> <p>OU</p> <p>L'entité responsable a documenté mais n'a pas mis en œuvre au moins une méthode permettant de désigner les BCSI. (1.1)</p> <p>OU</p> <p>L'entité responsable a documenté mais n'a pas mis en œuvre au moins une méthode de protection et de manipulation sécuritaire des BCSI. (1.2)</p>	L'entité responsable n'a ni documenté ni mis en œuvre de programme de protection des BCSI. (E1)
E2	Planification de l'exploitation	Faible	Sans objet	L'entité responsable a mis en œuvre un ou plusieurs processus documentés, mais n'a pas inclus de processus de réutilisation visant à empêcher la récupération non autorisée de BCSI à partir de l' <i>actif électronique BES</i> . (2.1)	L'entité responsable a mis en œuvre un ou plusieurs processus documentés, mais n'a pas inclus de processus d'élimination ou de destruction de support afin d'empêcher la récupération non autorisée de BCSI à partir de l' <i>actif électronique BES</i> . (2.2)	L'entité responsable n'a documenté ou mis en œuvre aucun processus pour les alinéas applicables du tableau E3 (CIP-011-3) – Réutilisation et élimination des <i>actifs électroniques BES</i> . (E2)

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	26 novembre 2012	Adoption par le conseil d'administration de la NERC	Cette norme définit les exigences de protection de l'information en coordination avec d'autres normes CIP et met en œuvre certaines dispositions de l'ordonnance 706 de la FERC.
1	22 novembre 2013	Ordonnance de la FERC approuvant CIP-011-1 (L'ordonnance entre en vigueur le 3 février 2014)	
2	13 novembre 2014	Adoption par le conseil d'administration de la NERC	Mise en œuvre de deux prescriptions de l'ordonnance 791 de la FERC concernant l'obligation de « détecter, évaluer et corriger » ainsi que les réseaux de communication.
2	12 février 2015	Adoption par le conseil d'administration de la NERC	Remplace la version adoptée par le conseil d'administration le 13 novembre 2014. La version à jour met en œuvre des prescriptions en instance de l'ordonnance 791 relativement aux actifs temporaires et aux <i>systèmes électroniques BES</i> à impact faible.
2	21 janvier 2016	Lettre d'ordonnance RM15-14-000 de la FERC approuvant la norme de fiabilité CIP-011-2.	

Version	Date	Intervention	Suivi des modifications
3	12 août 2021	Adoption par le conseil d'administration de la NERC.	Révision visant à améliorer la fiabilité en rapport avec la gestion par les entités de leurs BCSI.
3	7 décembre 2021	Lettre d'ordonnance RD21-6-000 de la FERC approuvant la norme de fiabilité CIP-011-3.	
3	10 décembre 2021	Date d'entrée en vigueur.	1 ^{er} janvier 2024