

A. Introduction

1. **Titre :** Cybersécurité – Protection des ~~l'~~informations
2. **Numéro :** CIP-011-~~23~~
3. **Objet :** Empêcher tout accès non autorisé ~~à aux l'~~informations de système électronique BES (BCSI) en définissant des exigences de protection des ~~l'~~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 ~~des exigences~~ de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « ~~les~~ entités responsables ». ~~Dans le cas des Si certaines~~ exigences ~~de cette norme qui~~ plus spécifiquement 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, systèmes~~ et équipements suivants pour la protection ou la remise en charge du BES :
 - 4.1.2.1 ~~Chaque s~~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 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 des~~ délestages ~~s automatique~~ de charge automatiques de 300 MW ~~ou plus par un système de sous la~~ commande d'un système commun détenu par l'entité responsable, sans intervention humaine ~~déclenchement par un exploitant humain~~.
 - 4.1.2.2 ~~Chaque a~~Automatisme de réseau (RAS) ~~ou plan de défense~~ visé par une ou plusieurs exigences d'une *norme de fiabilité* de la NERC ou de l'entité régionale.
 - 4.1.2.3 ~~Chaque s~~Système de protection ~~applicable au 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 ~~Chaque c~~Chemin de démarrage et groupe d'éléments respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes de production suivants à démarrer.
 - 4.1.3 **Exploitant d'installation de production**
 - 4.1.4 **Propriétaire d'installation de production**
 - 4.1.5 ~~Coordonnateur des échanges ou responsable des échanges~~
 - 4.1.6 **Coordonnateur de la fiabilité**
 - 4.1.7 **Exploitant de réseau de transport**
 - 4.1.8 **Propriétaire d'installation de transport**

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

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

4.2.1.1 ~~Chaque s~~ 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 s ~~automatique~~ de charge automatiques de 300 MW ~~ou plus au moyen d'un système de sous la~~ commande d'un système commun détenu par l'entité responsable, sans intervention humaine ~~déclenchement par un exploitant~~.

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

4.2.1.3 ~~Chaque s~~ Système de protection applicable au de réseau de transport (à l'exclusion des systèmes de DSF et de 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 c~~ 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-011-23 :

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 ~~D~~ 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~~ n'avoir aucun ~~systèmes électroniques BES classés~~ dans les catégories « impact élevé » ou « impact moyen » selon le processus d'inventaire de désignation et de catégorisation de la norme CIP-002-5.1a.

5. **Dates ~~d'entrée de mise~~ en vigueur** : Voir le plan de mise en œuvre de la norme CIP-011-23.
6. **Contexte** : La norme CIP-011 fait partie d'une série de normes CIP sur la cybersécurité qui exigent ~~l'inventaire la détermination~~ et la catégorisation initiales des *systèmes électroniques BES*, ~~ainsi qu'.~~ ~~Ces normes 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 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 ~~de~~ ~~fiabilité~~ 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 les ~~s~~ processus ~~de désignation~~ 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 les ~~s~~ processus ~~de désignation~~ 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 ~~s~~ Informations ~~s~~ 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-011-23) – Protection des ~~s~~ Informations ~~s~~.

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

- M1.** Les pièces justificatives du programme de protection des ~~s~~ Informations ~~s~~ doivent couvrir toutes les parties applicables du tableau E1 (CIP-011-23) – Programme de protection des ~~s~~ Informations ~~s~~ ; d'autres pièces justificatives doivent attester la mise en œuvre, selon la colonne Mesures du tableau.

Tableau E1 (CIP-011-23) – <u>Programme de p</u> rotection des s Informations s			
Alinéa	Systèmes visés	Exigences	Mesures
1.1	<p>Systèmes électroniques BES à impact élevé et :</p> <ol style="list-style-type: none"> 1. les EACMS associés; et 2. les PACS associés. <p>Systèmes électroniques BES à impact moyen et :</p> <ol style="list-style-type: none"> 1. les EACMS associés; et 2. les PACS associés. 	<p>M Méthodes permettant de désigner <u>les BCSI</u> l'information qui répond à la définition d'information de système électronique BES.</p>	<p>Exemples non limitatifs de pièces justificatives acceptables :</p> <ul style="list-style-type: none"> • méthode documentée permettant de désigner <u>les BCSI</u> l'information de système électronique BES à partir du programme de protection des s Informations s de l'entité ; • indications sur <u>les</u> s Informations s (étiquetage, classification, etc.) qui permettent de désigner <u>les BCSI</u> l'information de système électronique BES telles que désignées dans le programme de protection des s Informations s de l'entité; • <u>matériel</u> de formation qui donne au personnel des connaissances suffisantes pour reconnaître <u>les BCSI</u> l'information de système électronique BES; ou

Tableau E1 (CIP-011-23) – ~~Programme de p~~Protection des ~~s~~ Informations

Alinéa	Systèmes visés	Exigences	Mesures
			<ul style="list-style-type: none">• emplacements désignés pour le stockage des BCSI dans le cadre du programme de protection des informations de l'entité.• archive ou emplacement électronique et physique affecté au stockage de l'information de système électronique BES dans le cadre du programme de protection de l'information de l'entité.

Tableau E1 (CIP-011-23) – Programme de pProtection des s Informations

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

E2. Chaque entité responsable doit mettre en œuvre un ou plusieurs processus documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-011-23) – 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-011-23) – 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-011-23) – 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. 	<p>Avant d'autoriser la réutilisation d'un <i>actif électronique</i> visé qui contient des <u>BCSI</u> l'information de système électronique BES (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 <u>de</u> BCSI d'information de système électronique BES stockées sur le support de stockage de l'<i>actif électronique</i> en question.</p>	<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 <u>de</u> BCSI d'information de système électronique BES, 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 <u>de</u> BCSI d'information de système électronique BES.

Tableau E2 (CIP-011-23) – Réutilisation et élimination des *actifs électroniques BES*

Alinéa	Systèmes visés	Exigences	Mesures
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. 	<p>Avant l'élimination d'un <i>actif électronique</i> visé qui contient de s BCSI l'information de système électronique BES, l'entité responsable doit faire en sorte d'empêcher toute récupération non autorisée de BCS l'information de système électronique BES stockées s sur l'<i>actif électronique</i> en question, ou encore de détruire son support d'information.</p>	<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 BCS l'information de système électronique BES 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

~~Selon la définition des règles de procédure de la NERC, le terme « responsable des mesures pour assurer la conformité » (CEA) désigne la NERC ou l'entité régionale dans leurs rôles respectifs de surveillance de la conformité aux normes de fiabilité de la NERC.~~

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~~~~responsable~~ 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 :

- ~~Chaque~~ L'entité ~~visée~~~~responsable~~ doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité ~~visée~~~~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. ~~Programme~~~~Processus~~ de surveillance de la conformité ~~et de mise en~~ d'application des normes

~~Audits de conformité~~

~~Déclarations sur la conformité~~

~~Contrôles ponctuels~~

~~Enquêtes de conformité~~

~~Déclarations de non-conformité~~

~~Plaintes~~

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.

1.4. ~~Autres informations sur la conformité~~

~~Aucune.~~

2. ~~Tableau des éléments de conformité~~ Niveaux de gravité de la non-conformité (VSL)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité <u>(VSL)</u> (CIP-011-23)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
E1	Planification de l'exploitation	Moyen	Sans objet	Sans objet	<p>Sans objet</p> <p><u>L'entité responsable a documenté mais n'a pas mis en œuvre un ou des programmes de protection des BCSI. (E1)</u></p> <p><u>OU</u></p> <p><u>L'entité responsable a documenté mais n'a pas mis en œuvre au moins une méthode permettant de désigner les BCSI. (1.1)</u></p> <p><u>OU</u></p> <p><u>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)</u></p>	L'entité responsable n'a pas <u>ni</u> documenté ou ni mis en œuvre une <u>de</u> programme de protection des <u>BCSI</u> <u>l'information de système électronique BES</u> . (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 <u>de BCSI d'information de système électronique BES</u> à	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 <u>de BCSI d'information de</u>	L'entité responsable n'a documenté ou mis en œuvre aucun processus pour les alinéas applicables du tableau E23 (CIP-011-23) – Réutilisation et élimination des <u>actifs électroniques BES</u> . (E2)

Ex.	Horizon	VRF	Niveaux de gravité de la non-conformité (VSL) (CIP-011-23)			
			VSL faible	VSL modéré	VSL élevé	VSL critique
				partir de l'actif électronique BES. (2.1)	système électronique BES à partir de l'actif électronique BES. (2.2)	

D. Différences régionales

Aucune.

E. Interprétations

Aucune.

F. Documents connexes~~Principes directeurs et fondements techniques (ci-joints)~~**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.

Version	Date	Intervention	Suivi des modifications
2	21 janvier 2016	Lettre d'ordonnance RM15-14-000 de la FERC approuvant la norme de fiabilité CIP-011-2.	
<u>3</u>	<u>12 août 2021</u>	<u>Adoption par le conseil d'administration de la NERC.</u>	<u>Révision visant à améliorer la fiabilité en rapport avec la gestion par les entités de leurs BCSL.</u>
<u>3</u>	<u>7 décembre 2021</u>	<u>Lettre d'ordonnance RD21-6-000 de la FERC approuvant la norme de fiabilité CIP-011-3.</u>	
<u>3</u>	<u>10 décembre 2021</u>	<u>Date d'entrée en vigueur.</u>	<u>1^{er} janvier 2024</u>

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) présente 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, les normes CIP sur la cybersécurité de la NERC s'y appliquent. Il est à noter qu'en ce qui concerne les *distributeurs*, la section 4.1 limite l'applicabilité 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 qui, selon la section 4.1, est visée par les exigences de la norme. Comme il est indiqué à la section d'exemption 4.2.3.5, la présente norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou moyen selon la catégorisation de la norme CIP-002-5.1. 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* » dans le glossaire de la NERC indique déjà qu'il s'agit d'*éléments* du *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 aide à clarifier quels sont les *installations*, systèmes et équipements visés par les normes.

Exigence E1

Les entités responsables sont libres d'utiliser les systèmes existants de gestion des changements et des actifs. Cependant, l'information que contiennent ces systèmes doit être évaluée, car les exigences de protection de l'information s'appliquent toujours.

La justification de cette exigence est déjà présente dans les versions précédentes des normes CIP, ainsi que dans l'ordonnance 706 de la FERC et la proposition réglementaire (*Notice of Proposed Rulemaking*) connexe.

Cette exigence stipule qu'il faut désigner l'*information de système électronique BES*. L'entité responsable dispose d'une certaine latitude quant à la mise en œuvre de cette exigence. L'entité responsable devrait expliquer par quels moyens l'*information de système électronique BES* est désignée dans son programme de protection de l'information. Par exemple, l'entité peut décider de marquer ou d'étiqueter les documents. Il n'est pas exigé d'établir des classes distinctes d'*information de système électronique BES*. Cependant, l'entité responsable est libre de le faire si elle le souhaite. Pour autant que le programme de protection de l'information englobe tous les éléments pertinents, l'entité peut aller plus loin et créer des niveaux de classification (public, confidentiel, usage interne, etc.). Si l'entité responsable choisit d'utiliser un système de classification, elle doit documenter les classes de ce système et tout étiquetage connexe dans son programme d'*information de système électronique BES*.

L'entité responsable peut stocker toute l'information concernant les *systèmes électroniques BES* dans une archive ou un emplacement séparé (physique ou électronique) protégé par un contrôle d'accès. Par exemple, le programme de l'entité responsable pourrait spécifier que toute l'information stockée dans une archive particulière est une *information de système électronique BES*, ou que toute l'information stockée dans telle section d'une archive particulière est une *information de système électronique BES*, ou encore que toutes les copies papier de cette information sont stockées dans une partie sécurisée du bâtiment. D'autres méthodes pour la mise en œuvre de cette exigence sont suggérées à la section

Mesures. Cependant, ces méthodes ne forment pas une liste exhaustive, et l'entité responsable peut recourir à d'autres moyens pour désigner l'information de système électronique BES.

La SDT souhaite préciser que cette exigence ne s'applique pas à l'information accessible au public, comme les manuels de fournisseurs consultables sur des sites Web publics, non plus qu'à toute information considérée comme divulgable au grand public.

La protection de l'information englobe les versions électroniques et papiers. L'exigence E1.2 prescrit une ou plusieurs procédures pour la protection et la manipulation sécuritaire de l'information de système électronique BES, notamment le stockage, le transport et l'utilisation. Ces procédures s'appliquent aussi à l'information qui peut se trouver sur des actifs électroniques transitoires ou des supports amovibles.

Le programme écrit de protection de l'information de l'entité doit expliquer comment celle-ci gère divers aspects de la protection de l'information de système électronique BES, notamment pendant le transport, afin de prévenir tout accès non autorisé, toute mauvaise utilisation ou toute corruption, et aussi pour protéger la confidentialité de l'information transmise. Par exemple, le recours à un fournisseur de service de télécommunications tiers plutôt qu'à une infrastructure détenue par l'organisation peut justifier le cryptage de l'information. L'entité peut choisir d'établir un trajet de communication de confiance pour le transport de l'information de système électronique BES; ce trajet de confiance utiliserait un mécanisme d'authentification ou d'autres mesures pour assurer la sécurité pendant le transport. L'entité peut adopter d'autres mesures de protection physique, comme le transport par messenger ou l'utilisation d'un contenant de transport verrouillé. La présente norme ne cherche pas à imposer un moyen particulier de sécuriser l'information pendant son transport.

Un bon programme de protection de l'information spécifie par écrit les circonstances dans lesquelles l'information de système électronique BES peut être partagée avec des tiers ou être utilisée par ceux-ci. L'entité ne doit diffuser ou partager l'information que selon le principe de l'accès sélectif. Par exemple, l'entité peut spécifier qu'un accord de confidentialité, une entente de non-divulcation, un contrat ou toute autre convention écrite concernant l'utilisation de l'information doit être en place entre l'entité et le tiers. Le programme de protection de l'information de l'entité doit spécifier les modalités de partage de l'information de système électronique BES avec des tiers ou de son utilisation par ceux-ci, par exemple une entente de non-divulcation. L'entité doit ensuite respecter son programme documenté. Ces exigences n'imposent pas un type particulier d'arrangement.

Exigence E2

Cette exigence permet le retrait du service des systèmes électroniques BES et leur analyse avec leur support intact, car cela ne constitue pas une autorisation de réutilisation. Cependant, si après analyse le support doit être réutilisé à l'extérieur d'un système électronique BES ou doit être éliminé, l'entité doit prendre des mesures pour empêcher la récupération non autorisée de l'information de système électronique BES présente sur le support.

La justification de cette exigence est déjà présente dans les versions précédentes des normes CIP, ainsi que dans l'ordonnance 706 de la FERC et la proposition réglementaire (*Notice of Proposed Rulemaking*) connexe.

Si un actif électronique visé est retiré du périmètre de sécurité physique avant que des mesures aient été prises pour empêcher la récupération non autorisée de l'information de système électronique BES ou avant que le support d'information ait été détruit, l'entité responsable doit tenir un dossier indiquant le détenteur du support d'information pendant que ce dernier se trouve hors du périmètre de sécurité physique avant l'application par l'entité des mesures prescrites à l'exigence E2.

On appelle « expurgation » le procédé qui consiste à éliminer l'information d'un support de données de manière à assurer raisonnablement que l'information ne pourra pas être récupérée ou reconstituée. Les moyens d'expurgation sont généralement divisés en quatre catégories : la mise au rebut, l'écrasement, la purge et la destruction. Aux fins de la présente exigence, la mise au rebut en elle-même — sauf dans certaines circonstances spéciales, comme le recours à un cryptage fort pour un disque utilisé dans un réseau de stockage (SAN) ou un autre support — ne doit jamais être jugée acceptable. Les techniques d'écrasement peuvent constituer un moyen d'expurgation adéquat pour les supports destinés à être réutilisés, tandis que les techniques de purge peuvent mieux convenir pour les supports destinés à l'élimination.

L'information suivante, tirée de la publication spéciale 800-88 du NIST, donne des précisions supplémentaires sur les types de mesures que l'entité pourrait prendre pour empêcher la récupération non autorisée de l'information de système électronique BES à partir de ses supports d'information :

Écrasement : Cette méthode d'expurgation consiste à écrire des données non sensibles à la place des données existantes du support, au moyen d'un logiciel ou d'un appareil spécial. Ce procédé peut écraser ainsi non seulement l'emplacement logique du ou des fichiers en cause (par exemple, la table d'allocation de fichiers), mais aussi tous les emplacements mémoire adressables. Cette opération a pour objet de remplacer les données existantes par des données quelconques. L'écrasement n'est pas possible dans le cas d'un support endommagé ou non réinscriptible. Le type et la taille du support peuvent aussi déterminer si l'écrasement est une méthode d'expurgation convenable [800-36].

Purge : La démagnétisation et l'exécution de la commande d'effacement sécurisé du microprogramme (pour les disques ATA seulement) sont des méthodes de purge acceptables. La démagnétisation consiste à exposer le support magnétique à un fort champ magnétique afin de perturber les domaines magnétiques d'enregistrement; ce champ magnétique est produit par un démagnétiseur. Il existe différents types de démagnétiseur (à faible puissance, à grande puissance, etc.) selon le type de support magnétique qu'ils peuvent traiter. Les démagnétiseurs comportent un aimant permanent puissant ou une bobine électromagnétique. La démagnétisation convient particulièrement pour purger un support endommagé, inopérant ou de très grande capacité, ou pour effacer rapidement des disquettes. [800-36] La commande d'effacement sécurisé (disques ATA) et la démagnétisation sont des exemples de méthodes de purge acceptables. La démagnétisation d'un disque dur détruit habituellement celui-ci, car elle efface aussi le microprogramme qui commande le disque.

Destruction : Il existe de nombreux moyens pour détruire un support d'information. La désintégration, la pulvérisation, la fusion et l'incinération sont des procédés d'expurgation conçus pour détruire complètement le support. On les confie généralement à une entreprise agréée de destruction de produits métalliques ou d'incinération disposant des moyens techniques appropriés pour effectuer cette opération de manière efficace, sécurisée et sécuritaire. Les supports optiques, notamment les cédéroms (réinscriptibles ou non), les disques optiques (DVD) et les disques magnéto-optiques, doivent être détruits par pulvérisation, par déchiquetage transversal ou par combustion.

Dans certains cas, notamment pour de l'équipement réseau, il peut être nécessaire de consulter le fabricant pour connaître la méthode d'expurgation appropriée.

~~Il est de la plus grande importance que l'organisation tienne un dossier de ses activités d'expurgation afin d'empêcher la récupération non autorisée d'information de système électronique BES. Les entités sont fortement invitées à consulter la publication spéciale 800-88 du NIST pour de plus amples renseignements sur l'élaboration de procédés d'expurgation des supports.~~

Justification

~~Pendant l'élaboration de cette norme, des zones de texte ont été incorporées à celle-ci pour exposer la justification de ses diverses parties. Après l'approbation par le Conseil d'administration, le contenu de ces zones de texte a été transféré ci-après.~~

Justification de l'exigence E1:

~~L'exigence d'un programme de protection de l'information vise à empêcher tout accès non autorisé à l'information de système électronique BES.~~

Justification de l'exigence E2:

~~Le processus de réutilisation et d'élimination des actifs électroniques BES vise à empêcher toute diffusion non autorisée d'information de système électronique BES en cas de réutilisation ou d'élimination de ces actifs.~~