
Projet QC-2017-01
Normes CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6
CIP-010-2 et CIP-011-2
Protection des infrastructures critiques

1. ÉVALUATION DE LA PERTINENCE

Les outils d'exploitation des réseaux électriques interconnectés ont considérablement évolué avec les années. La fiabilité du réseau électrique dépend de composantes informatiques, d'appareils intelligents sophistiqués et de réseaux de communication de nouvelle génération permettant de minimiser les défaillances potentielles.

Ces technologies amènent également un risque accru d'attaques cybernétiques menaçant l'intégrité du réseau de transport électrique nord-américain. Quotidiennement, les médias rapportent des incidents majeurs touchant les installations et équipements de fournisseurs d'électricité, et ce à travers le monde.

Les infrastructures critiques sont donc menacées par des cyber-attaques de plus en plus fréquentes et d'un niveau de sophistication élevé. L'interconnexion des réseaux de transport électriques peut permettre à des cyber pirates de faire tomber en cascade les infrastructures et mettre en péril la sécurité de la population. Les coûts financiers reliés à ces attaques peuvent être considérables.

L'adoption en continu et l'évolution des normes en matière de cybersécurité sont donc nécessaires pour protéger les réseaux électriques interconnectés contre les menaces potentielles. Le projet 2014-02-CIP-version 5 révisé de la NERC découle de la nécessité de clarifier et faire évoluer ces normes en fonction de l'environnement cybernétique. Il représente un élargissement de certaines exigences de la version 5.

L'adoption par la FERC dans les ordonnances 791 et 791a des normes développées dans ce projet de révision fait évoluer les normes CIP en matière de cybersécurité, ce qui est nécessaire pour protéger les réseaux électriques interconnectés contre les menaces potentielles. Ces normes, la version 6 des normes CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, CIP-011-2, sont une amélioration par rapport à la version 5 des normes CIP adoptées par la Régie de l'énergie (D-2016-119) le 29 juillet 2016.

Le cadre d'application des nouvelles normes CIP dans son ensemble demeure semblable, et les CIP version 6 apportent plusieurs améliorations :

- Clarification de certains termes vagues sujets à interprétation ;
- Modification de la formulation de l'exigence 1 afin d'incorporer une ou des politiques de cybersécurité pour la norme CIP-003-6 ;

- Ajout des actifs électroniques transitoires comme élément de contenu à inclure dans les programmes de formation sur la cybersécurité pour la norme CIP-004-6 ;
- Restriction de l'accès physique au câblage et autres composantes de communication non programmable pour la norme CIP-006-6 ;
- Protection des ports physiques pour les actifs électroniques protégés et les composantes de communication non programmables pour la norme CIP-007-6 ;
- Modification de l'exigence 4 concernant les actifs électroniques et les supports amovibles pour la norme CIP-010-2.
- Optimisation de traduction de la version française

Il n'y a eu aucun changement à noter concernant la catégorisation du risque (Faible, Moyen, Élevé) et le cycle de vie de la mitigation du risque (mise en œuvre, évaluation, surveillance et mise à jour) concernant la version 6 des normes CIP.

Les principaux changements prescrits par la FERC sont résumés dans le tableau ci-dessous. Les tableaux de 11.1 à 11.7 décrivent la concordance de la version 5 et de la version 6 des normes CIP-003-6, CIP-004-6, CIP-006-6, CIP-009-6, CIP-010-2, CIP-011-2.

Exigence	Description et justification du changement	Changement
17 exigences des normes CIPV5	Élimination de la formulation « détecter, évaluer et corriger » car la formulation est vague et sujette à des multiples interprétations.	Retrait du texte
CIP-003-6, E1	Modification de la formulation de l'exigence principale afin d'incorporer une ou des politiques de cybersécurité touchant les systèmes électroniques BES à impact faible. Les expressions « pour ses systèmes électroniques BES à impact élevé ou moyen » et « Pour ses actifs qui comportent des systèmes électroniques BES à impact faible selon les critères de la norme CIP-002, le cas échéant : » ont été ajoutées pour qualifier les sous-alinéas. L'annexe 1 de la CIP-003-6 dresse la liste des éléments que doivent couvrir les plans de cybersécurité pour ses systèmes électroniques BES à impact faible.	Exigence élargie

Exigence	Descriptions et justifications du changement	Changement
CIP-004-6, E2, l'alinéa 2.1.9	Ajout des actifs électroniques transitoires (tel que les ordinateurs portables) et les supports de stockage amovibles (tel que les clés USB, CD etc.) comme éléments de contenu à inclure dans les programmes de formation sur la cybersécurité de l'entité responsable. La formation doit porter sur les risques pour la cybersécurité associés à l'interconnectabilité et à l'interopérabilité des systèmes électroniques BES avec les actifs électroniques transitoires et les supports de stockage amovibles.	Exigence élargie
CIP-006-6, E1.10	Restriction de l'accès physique au câblage et autres composantes de communication non programmables qui servent à interrelier des actifs électroniques visés situés dans un même périmètre de sécurité électronique, mais localisé à l'extérieur d'un périmètre de sécurité physique.	Nouvelle exigence
CIP-007-6, E1, l'alinéa 1.2	Protection des ports physiques pour les actifs électroniques protégés (PCA) et les composantes de communication non programmables situés à la fois dans un périmètre de sécurité physique et dans un périmètre de sécurité électronique.	Exigence élargie
CIP-010-2, E4	L'équipe de rédaction recourt à l'annexe 1 de la norme plutôt qu'à des tableaux en regard des actifs transitoires. Elle a donc changé l'exigence E4 pour y inclure le texte suivant : « mettre en œuvre (sauf dans des circonstances CIP exceptionnelles) un ou plusieurs plans documentés concernant les actifs électroniques transitoires et les supports de stockage amovibles; ces plans doivent être conformes aux sections de l'annexe 1. ». L'annexe 1 de la CIP-010-2 dresse la liste des éléments que doivent couvrir les plans concernant les actifs électroniques transitoires et les supports de stockage amovibles.	Nouvelle exigence

2. PRÉREQUIS À L'ADOPTION

Adoption des définitions proposées à la section suivante.

3. MODIFICATIONS À D'AUTRES NORMES OU AUX DÉFINITIONS DU GLOSSAIRE

Les ajouts, modifications ou retraits suivants entreront en vigueur en même temps que les normes proposées.

3.1. Normes ou exigences à retirer lors de l'entrée en vigueur :

Les normes CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, CIP-011-1.

3.2. Nouvelles définitions à ajouter au glossaire :

Terme	Acronyme	Définition
Actif électronique transitoire	TCA	<p><i>Actif électronique</i> qui i) est capable de transmettre ou de transférer du code exécutable, ii) ne fait pas partie d'un <i>système électronique BES</i>, iii) n'est pas un <i>actif électronique protégé (PCA)</i> et iv) est relié directement (par exemple au moyen d'une connexion Ethernet, série ou USB, ou encore d'une liaison sans fil, y compris une communication en champ proche ou Bluetooth) pendant au maximum 30 jours civils consécutifs à un <i>actif électronique BES</i>, à un réseau situé dans un <i>périmètre de sécurité électronique</i> ou à un <i>actif électronique protégé</i>. Exemples non limitatifs : <i>actifs électroniques</i> utilisés pour le transfert de données, l'analyse de vulnérabilité, la maintenance ou le dépannage.</p> <p>(Transient Cyber Asset)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>
Connectivité externe routable à impact faible	LERC	<p>Accès commandé par une personne utilisant un client d'accès distant ou une autre technologie d'accès distant avec un protocole routable. L'accès distant provient d'un <i>actif électronique</i> qui n'est pas un <i>système intermédiaire</i> et qui n'est situé ni à l'intérieur d'un des <i>périmètres de sécurité électronique</i> de l'entité responsable, ni à un <i>point d'accès électronique (LEAP)</i> défini. L'accès distant peut être commandé à partir d'<i>actifs électroniques</i> utilisés ou détenus : 1) par l'entité responsable, 2) par des employés ou 3) par des fournisseurs, des entrepreneurs ou des consultants. L'<i>accès distant interactif</i> ne comprend pas les communications de processus de système à système.</p> <p>(Low Impact External Routable Connectivity)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>

Terme	Acronyme	Définition
Point d'accès électronique de système électronique BES à impact faible	LEAP	<p>Interface d'<i>actif électronique</i> qui contrôle une <i>connectivité externe routable à impact faible</i>. L'<i>actif électronique</i> qui comporte le LEAP peut être situé à l'extérieur du ou des actifs qui comportent des <i>systèmes électroniques BES</i> à impact faible.</p> <p>(Low Impact BES Cyber System Electronic Access Point)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>
Support d'information de stockage	RM	<p>Support de stockage qui i) n'est pas un actif électronique, ii) est capable de transférer du code exécutable, iii) peut servir à stocker, à copier, à déplacer ou à rendre accessibles des données, et iv) est relié directement pendant au maximum 30 jours civils consécutif à un <i>actif électronique BES</i>, à un réseau situé dans un <i>périmètre de sécurité électronique</i> ou à un <i>actif électronique protégé</i>. Exemples non limitatifs : disquettes, cédéroms, clés USB, disques durs externes et lecteurs ou cartes à mémoire flash non volatile.</p> <p>(Removable Media)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>

3.3. Définitions du glossaire à modifier :

Terme	Acronyme	Définition
Actifs électroniques BES	BCA	<p><u>Nouvelle définition :</u></p> <p><i>Actif électronique</i> qui, s'il était endommagé, mal utilisé ou rendu indisponible, entraînerait, dans les 15 minutes suivant son fonctionnement requis, son fonctionnement incorrect, ou son non-fonctionnement, un impact négatif sur un ou plusieurs réseaux, <i>installations</i> ou équipements, lesquels, s'ils se trouvaient détruits, endommagés ou autrement rendus indisponibles en cas de besoin, affecteraient l'exploitation fiable du <i>système de production-transport d'électricité</i>. La redondance des réseaux, installations ou équipements en question ne doit pas être prise en compte dans l'évaluation de l'impact négatif. Chaque <i>actif électronique BES</i> est compris dans un ou plusieurs <i>systèmes électroniques BES</i>.</p> <p><u>Ancienne définition :</u></p> <p><i>Actif électronique</i> qui, s'il était endommagé, mal utilisé ou rendu indisponible, entraînerait, dans les 15 minutes suivant son fonctionnement requis, son fonctionnement incorrect, ou son non-fonctionnement, un impact négatif sur un ou plusieurs réseaux, <i>installations</i> ou équipements, lesquels, s'ils se trouvaient détruits, endommagés ou autrement rendus indisponibles en cas</p>

Terme	Acronyme	Définition
		<p>de besoin, affecteraient l'exploitation fiable du <i>système de production-transport d'électricité</i>. La redondance des réseaux, <i>installations</i> ou équipements en question ne doit pas être prise en compte dans l'évaluation de l'impact négatif. Chaque actif électronique BES est compris dans un ou plusieurs systèmes électroniques BES. (Un <i>actif électronique</i> n'est pas un <i>actif électronique BES</i> si, pendant 30 jours civils consécutifs ou moins, il est relié directement à un réseau situé dans un <i>périmètre de sécurité électronique</i> (ESP), à un <i>actif électronique</i> situé à l'intérieur d'un ESP ou à un <i>actif électronique BES</i> et qu'il est utilisé à des fins de transfert de données, d'analyse de vulnérabilité, de maintenance ou de diagnostic.)</p> <p>(BES Cyber Asset)</p> <p>Source Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>
Actifs électroniques protégés	PCA	<p><u>Nouvelle définition :</u></p> <p>Un ou plusieurs <i>actifs électroniques</i> reliés au moyen d'un protocole routable, à l'intérieur ou autour d'un <i>périmètre de sécurité électronique</i> et qui ne font pas partie du <i>système électronique BES</i> dont le degré d'impact est le plus élevé à l'intérieur d'un même <i>périmètre de sécurité électronique</i>. Le degré d'impact des <i>actifs électroniques protégés</i> est égal à celui du <i>système électronique BES</i> dont le degré d'impact est le plus élevé dans le même ESP.</p> <p><u>Ancienne définition :</u></p> <p>Un ou plusieurs <i>actifs électroniques</i> reliés au moyen d'un protocole routable, à l'intérieur ou autour d'un <i>périmètre de sécurité électronique</i> et qui ne font pas partie du <i>système électronique BES</i> dont le degré d'impact est le plus élevé à l'intérieur d'un même <i>périmètre de sécurité électronique</i>. Le degré d'impact des <i>actifs électroniques protégés</i> est égal à celui du <i>système électronique BES</i> dont le degré d'impact est le plus élevé dans le même ESP. Un <i>actif électronique</i> n'est pas un <i>actif électronique</i> protégé si, pendant 30 jours civils consécutifs ou moins, il est relié à un <i>actif électronique</i> situé à l'intérieur de l'ESP ou au réseau situé à l'intérieur de l'ESP, et qu'il est utilisé pour le transfert de données, l'analyse de vulnérabilité, la maintenance ou le diagnostic</p> <p>(Protected Cyber Asset)</p> <p>Source : Glossaire des termes en usage dans les normes de fiabilité (NERC)</p>

3.4. Définitions à retirer du glossaire :

Aucun changement

4. MODIFICATIONS AU REGISTRE DES ENTITÉS VISÉES

Les normes proposées ne nécessitent aucun changement au Registre des entités visées.

5. NOTE CONCERNANT L'UTILISATION DU TERME « POSTE » DANS LA VERSION FRANÇAISE

La version anglaise des normes utilise les termes « stations » et « substations » pour désigner un ensemble d'équipements de transport situés dans un même emplacement. Le terme « substation » est souvent utilisé dans l'industrie pour désigner un poste qui contient au moins un autotransformateur, tandis que le terme « station » est utilisé pour désigner les postes qui sont exploités à un seul niveau de tension. Cette distinction n'existe pas en français, et le terme « poste » est utilisé pour désigner ces deux types d'installations. La version française des normes utilise donc uniquement le terme « poste » pour traduire les termes « station » et « substation ».

6. APPLICABILITÉ

L'ensemble des normes CIP version 6 visent le même ensemble de fonctions et d'installations.

Fonctions visées :

- Responsable de l'équilibrage
- Exploitant d'installation de production
- Propriétaire d'installation de production
- Responsable des échanges
- Coordonnateur de la fiabilité
- Exploitant de réseau de transport
- Propriétaire d'installation de transport

Installations visées :

- Toutes les installations du système de production-transport d'électricité (BES)
- Installations spécifiques pour les *distributeurs*¹

Exemptions :

Se référer à la section « Applicabilité » de chaque norme pour les exemptions spécifiques à celles-ci.

7. DISPOSITIONS PARTICULIÈRES POUR LE QUÉBEC (ANNEXES QC)

Les normes CIP visent uniquement les installations du *réseau de transport principal* (RTP) ainsi que les installations spécifiées dans les normes pour les *distributeurs*.

Par ailleurs, le Coordonnateur reconduit la disposition particulière de la version 5, accepté par la Régie de l'énergie dans sa décision D-2015-119 qui exempte certaines centrales et leur poste élévateur, comme suit :

Exemptions additionnelles

Sont exemptés de l'application de la présente norme :

- Installations de production ayant une puissance nominale de 300 MVA ou moins, à moins que l'installation comprenne un ou plusieurs groupes pouvant être îlotés sur un réseau voisin.
- Postes élévateurs des installations de production identifiées au point précédent.

¹ Voir la section « Applicabilité » des normes CIP pour les détails concernant l'application pour les distributeurs

8. DATES D'ENTRÉE EN VIGUEUR PROPOSÉES

Le délai accordé aux entités américaines lors de l'approbation de ces normes aux États-Unis varie selon la norme et les exigences qui s'y rattachent. Les dates d'entrée en vigueur proposées pour le Québec tiennent compte du fait qu'une entité possède déjà ou non des actifs critiques en vertu de la version 1 des normes CIP adoptées par la Régie :

Norme	Entité	Dates d'entrée en vigueur aux États-Unis	Date d'entrée en vigueur proposée au Québec		Justification
			Impacts moyen et élevé	Impact faible	
<ul style="list-style-type: none"> CIP-003-6 CIP-003-6, E1, l'alinéa 1.1 CIP-004-6 CIP-006-6 	Entités visées par la version 1 des normes CIP adoptées par la Régie.	2016-07-01	2017-07-01	2017-07-01	Uniformisation des pratiques avec les autres juridictions.
<ul style="list-style-type: none"> CIP-006-6, E1, l'alinéa 1.10 (systèmes électroniques BES à impact élevé et à impact moyen existant des centres de contrôles) CIP-007-6 CIP-009-6 CIP-010-2 CIP-011-2 	Entités exemptées de l'application de la version 1 des normes CIP en vertu des dispositions particulières associées à ces normes.		2018-10-01	2019-10-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.
	Entités qui possèdent des installations de production à vocation industrielle		2019-04-01	2020-04-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.
<ul style="list-style-type: none"> CIP-003-6, E1 l'alinéa 1.2 CIP-003-6, E2 CIP-003-6, 	Entités visées par la version 1 des normes CIP adoptées par la Régie.	2017-04-01	2017-07-01	2017-07-01	Uniformisation des pratiques avec les autres juridictions.

Norme	Entité	Dates d'entrée en vigueur aux États-Unis	Date d'entrée en vigueur proposée au Québec		Justification
			Impacts moyen et élevé	Impact faible	
Annexe 1, Sect.1 <ul style="list-style-type: none"> CIP-003-6, Annexe 1, Sect.4 CIP-006-6, E1, l'alinéa 1.10 (systèmes électroniques BES à impact élevé et à impact moyen des centres de contrôles) 	Entités exemptées de l'application de la version 1 des normes CIP en vertu des dispositions particulières associées à ces normes.		2018-10-01	2019-10-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.
<ul style="list-style-type: none"> CIP-007-6, E1, l'alinéa 1.2 (pour les PCA et les composantes de communication non programmables situés à la fois dans un périmètre de sécurité physique et dans un périmètre de sécurité électronique pour les systèmes électronique BES à impact moyen ou élevé) CIP-010-2, E4 	Entités qui possèdent des installations de production à vocation industrielle		2019-04-01	2020-04-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.
<ul style="list-style-type: none"> CIP-003-6, Annexe 1, Sect.2 CIP-003-6, Annexe 1, Sect.3 CIP-003-6, 	Entités visées par la version 1 des normes CIP adoptées par la Régie.	2018-09-01	2018-09-01	2018-09-01	Uniformisation des pratiques avec les autres juridictions.

Norme	Entité	Dates d'entrée en vigueur aux États-Unis	Date d'entrée en vigueur proposée au Québec		Justification
			Impacts moyen et élevé	Impact faible	
Annexe 1, Sect.2 • CIP-003-6, Annexe 1, Sect.3	Entités exemptées de l'application de la version 1 des normes CIP en vertu des dispositions particulières associées à ces normes.		2018-10-01	2019-10-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.
	Entités qui possèdent des installations de production à vocation industrielle		2019-04-01	2020-04-01	Donner le temps nécessaire à la mise en œuvre de la version 6 des normes CIP aux entités qui étaient exemptées de l'application de la version 1.

Le Coordonnateur compte demander la suspension de l'entrée en vigueur prévue au 1^{er} octobre 2017 des exigences CIPv5 visant les systèmes électroniques BES à impact « faible » actuellement visés, tel qu'ordonné par la Régie dans ses décisions D-2016-119 et D-2016-138.

9. ÉVALUATION PRÉLIMINAIRE DE L'IMPACT

Cette section présente l'évaluation préliminaire de l'impact monétaire des normes effectuée par le Coordonnateur. À noter que le cadre d'application des normes CIP implique, en premier lieu, l'identification et la catégorisation des systèmes électroniques selon la norme CIP-002. Une entité n'ayant identifié aucun système en vertu de cette norme n'aura pas à se conformer aux normes, CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, CIP-011-2. L'impact pour ces entités serait donc nul pour ces normes

Sommaire des impacts *

Norme	Implantation			Maintien et suivi de la conformité		
	Faible	Modéré	Élevé	Faible	Modéré	Élevé
CIP-003-6		X			X	
CIP-004-6		X			X	
CIP-006-6		X			X	
CIP-007-6		X			X	
CIP-009-6		X			X	
CIP-010-2		X			X	
CIP-011-2		X			X	

Légende :

Faible :	Pratique normale de l'industrie ou norme n'entraînant que des ajustements mineurs aux processus ou aux pratiques en place.
Modéré :	Changement qui nécessite d'allouer certaines ressources matérielles, humaines ou financières pour implanter, maintenir ou assurer le suivi de la conformité à la norme proposée.
Élevé :	Changement qui nécessite de prévoir et d'allouer des ressources matérielles, humaines ou financières importantes pour planifier et réaliser l'implantation, le maintien ou le suivi de la conformité à la norme proposée.

* L'évaluation du Coordonnateur est par rapport à l'écart entre la version 5 et la version 6 des normes CIP.

10. ÉVALUATION FINALE DE L'IMPACT

Section à compléter à la réception des formulaires d'évaluation de l'impact et à la conclusion du processus de consultation préalable au dépôt des normes à la Régie de l'énergie.

11. Tableau de concordance CIP V5 vs CIP V6

11.1.CIP-003-6 – Cybersécurité- Mécanismes de gestion de la sécurité

CIP-003-5	CIP-003-6	Description et justification de la modification
E1	E1	La formulation de l'exigence principale a été modifiée afin d'incorporer une ou des politiques touchant les systèmes électroniques BES à impact faible. L'expression « pour ses systèmes électroniques BES à impact élevé ou moyen » a été supprimée lors de la création des nouveaux alinéas. Voir les alinéas 1.1 et 1.2 ci-dessous pour la justification du changement.
	E1.1	L'expression « pour ses systèmes électroniques BES à impact élevé ou moyen » a été ajoutée pour qualifier les sous-alinéas ci-dessous.
E1.1	E1.1.1	Les alinéas 1.1 à 1.9 sont devenus 1.1.1 à 1.1.9, et l'expression ci-dessus a été ajoutée à l'alinéa 1.1 de la CIP-003-6.
E1.2 à E1.9	E1.1.2 à E1.1.9	Aucun changement.
	E1.2	L'expression « Pour ses actifs qui comportent des systèmes électroniques BES à impact faible selon les critères de la norme CIP-002, le cas échéant : » a été ajoutée pour qualifier les sous-alinéas ci-dessous.
E2	E2	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée. De plus, l'équipe de rédaction (SDT) ayant changé d'approche pour recourir à l'annexe 1 plutôt qu'à des tableaux, l'exigence E2 a été modifiée ainsi : « mettre en œuvre pour ses systèmes électroniques BES à impact faible un ou plusieurs plans de cybersécurité documentés conformes à toutes les sections de l'annexe 1. »
E2.1	E1.2.1	L'alinéa concernant la sensibilisation à la cybersécurité qui doit être couverte par une ou plusieurs politiques de cybersécurité documentées a été déplacé à l'alinéa 1.2.1 de l'exigence E1 de la CIP-003-6.
E2.2	E1.2.2	L'alinéa concernant les mesures de sécurité physique qui doivent être couvertes par une ou plusieurs politiques de cybersécurité documentées a été déplacé à l'alinéa 1.2.2 de l'exigence E1 de la CIP-003-6.

CIP-003-5	CIP-003-6	Description et justification de la modification
E2.3	E1.2.3	L'alinéa concernant le contrôle des accès électroniques qui doit être couvert par une ou plusieurs politiques de cybersécurité documentées a été déplacé à l'alinéa 1.2.3 de l'exigence E1 de la CIP-003-6. De plus, la SDT a modifié l'expression « connexions externes à protocole routable » parce qu'elle a proposé « connectivité externe routable à impact faible » comme nouveau terme défini.
E2.4	E1.2.4	L'alinéa 2.4 concernant l'intervention en cas d'incident de cybersécurité qui doit être couverte par une ou plusieurs politiques de cybersécurité documentées a été déplacé à l'alinéa 1.2.4 de l'exigence E1 de la CIP-003-6.
	Annexe 1	L'annexe 1 de la CIP-003-6 dresse la liste des éléments que doivent couvrir les plans de cybersécurité pour ses systèmes électroniques BES à impact faible. L'annexe répond à l'ordonnance 791 de la FERC concernant le manque de critères objectifs pour la protection des actifs à impact faible.
E3	E3	Aucun changement.
E4	E4	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée.

11.2.CIP-004-6 – Cybersécurité – Personnel et formation

CIP-004-5.1	CIP-004-6	Description et justification de la modification
E1	E1	Aucun changement.
E1.1	E1.1	Aucun changement.

CIP-004-5.1	CIP-004-6	Description et justification de la modification
E2.1	E2.1	Aucun changement.
E2.1.1 à E2.1.8	E2.1.1 à E2.1.8	Aucun changement.
E2.1.9	E2.1.9	En réponse aux directives dans l'ordonnance 791 de la FERC concernant les actifs électroniques temporaires, la SDT a ajouté les actifs électroniques temporaires et les supports d'information amovibles comme éléments de contenu à inclure dans les programmes de formation sur la cybersécurité de l'entité responsable. La formation doit porter sur les risques pour la cybersécurité associés à l'interconnectabilité et à l'interopérabilité des systèmes électroniques BES avec les actifs électroniques temporaires et les supports d'information amovibles.
E2.2	E2.2	Aucun changement.
E2.3	E2.3	Aucun changement.
E3	E3	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée.
E3.1 à E3.5	E3.1 à E3.5	Aucun changement.
E4	E4	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée.
E4.1 à E4.4	E4.1 à E4.4	Aucun changement.
E5	E5	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée.
E5.1 à E5.5	E5.1 à E5.5	Aucun changement.

11.3.CIP-006-6 – Cybersécurité – Sécurité physique des systèmes électroniques BES

<i>Cip-006-5</i>	<i>CIP-006-6</i>	Description et justification de la modification
E1	E1	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée.
E1.1 à E1.9	E1.1 à E1.9	Aucun changement.
	E1.10	En réponse aux directives dans l'ordonnance 791 de la FERC selon laquelle il fallait protéger les composants non programmables des réseaux de communication, la SDT a ajouté à l'exigence E1 l'alinéa 1.10 qui demande de restreindre l'accès physique aux câbles et autres composants de communication non programmables qui permettent à des actifs électroniques visés situés dans un même périmètre de sécurité électronique de communiquer entre eux. L'entité a trois autres mécanismes pour protéger adéquatement ces réseaux, y compris : le cryptage des données qui transitent par ces câbles et composants ; la surveillance de l'état de la liaison de communication, avec déclenchement d'une alarme sur détection d'une défaillance de communication ; une protection logique d'une efficacité équivalente.
E2	E2	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée.
E2.1 à E2.3	E2.1 à E2.3	Aucun changement.
E3	E3	Aucun changement.
E3.1	E3.1	Aucun changement.

11.4.CIP-007-6 – Cybersécurité – Gestion de la sécurité des systèmes

CIP-007-5	CIP-007-6	Description et justification de la modification
E1	E1	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée.
E1.1	E1.1	Aucun changement.
E1.2	E1.2	La colonne des systèmes visés a été modifiée pour inclure les actifs électroniques protégés et les composants de communication non programmables situés à la fois dans un périmètre de sécurité physique et dans un périmètre de sécurité électronique. La protection contre l'utilisation de ports d'entrée-sortie physiques non nécessaires pour la connectivité de réseau, les commandes pupitre ou les supports d'information amovibles visant ces ajouts répond à la directive sur les réseaux de communication dans l'ordonnance 791 de la FERC. Le terme supports d'information amovible a été mis en italique, car il figure maintenant au Glossaire.
E2	E2	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée.
E2.1 à E2.4		Aucun changement.
E3	E3	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée.
E3.1 à E3.3	E3.1 à E3.3	Aucun changement.
E4	E4	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée.
E4.1 à E4.4	E4.1 à E4.4	Aucun changement.
E5	E5	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée.
E5.1 à E5.5	E5.1 à E5.5	Aucun changement.

CIP-007-5	CIP-007-6	Description et justification de la modification
E6	E6	Aucun changement.
E7	E7	Aucun changement.

11.5.CIP-009-6 – Cybersécurité – Plans de rétablissement des systèmes électroniques BES

CIP-009-5	CIP-009-6	Description et justification de la modification
E1	E1	Aucun changement.
E1.1 à E1.5	E1.1 à E1.5	Aucun changement.
E2	E2	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée.
E2.1 à E2.3	E2.1 à E2.3	Aucun changement.
E3	E3	Aucun changement.
E3.1 à 3.2	E3.1 à E3.2	Aucun changement.

11.6.CIP-010-2 – Cybersécurité – Gestion des changements de configuration et analyses de vulnérabilité

CIP-010-1	CIP-010-2	Description et justification de la modification
E1	E1	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée.

CIP-010-1	CIP-010-2	Description et justification de la modification
	E4	En réponse à la directive dans l'ordonnance 791 de la FERC concernant les actifs temporaires, la SDT a changé d'approche pour recourir à l'annexe 1 plutôt qu'à des tableaux. Elle a donc changé l'exigence E4 pour y inclure le texte suivant : « mettre en œuvre (sauf dans des circonstances CIP exceptionnelles) un ou plusieurs plans documentés concernant les actifs électroniques temporaires et les supports d'information amovibles ; ces plans doivent être conformes aux sections de l'annexe 1. »
	Annexe 1	L'annexe 1 de la CIP-010-2 dresse la liste des éléments que doivent couvrir les plans concernant les actifs électroniques temporaires et les supports d'information amovibles. L'annexe répond à l'ordonnance 791 de la FERC concernant les risques liés aux actifs temporaires.

11.7.CIP-011-2 – Cybersécurité – Protection de l'information

CIP-011-1	Cip-011-2	Description et justification de la modification
E1	E1	En réponse à l'ordonnance 791 de la FERC demandant que l'on retire de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée.
E1.1 à E1.2	E1.1 à E1.2	Aucun changement.
E2	E2	Aucun changement.
E2.1 à E2.2	E2.1 à E2.2	Aucun changement.