

**TABLEAU DE CONCORDANCE DES NORMES CIP
VERSION 5 ET CIP VERSION 6**

Tableau de concordance de la version 5 des normes CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, et CIP-011-2

CIP-003-6 – Cybersécurité – Mécanismes de gestion de la sécurité		
CIP-003-5	CIP-003-6	Description et justification de la modification
E1	E1	Modification de l'exigence principale 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.
NOUVEAU	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	E1.1.2	Aucun changement.
E1.3	E1.1.3	Aucun changement.
E1.4	E1.1.4	Aucun changement.
E1.5	E1.1.5	Aucun changement.
E1.6	E1.1.6	Aucun changement.
E1.7	E1.1.7	Aucun changement.
E1.8	E1.1.18	Aucun changement.
E1.9	E1.1.9	Aucun changement.

CIP-003-6 – Cybersécurité – Mécanismes de gestion de la sécurité		
CIP-003-5	CIP-003-6	Description et justification de la modification
NOUVEAU	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 de retirer 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.
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'une nouvelle définition pour le terme « connectivité externe routable à impact faible » est proposée.
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.
NOUVEAU	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.

CIP-003-6 – Cybersécurité – Mécanismes de gestion de la sécurité		
CIP-003-5	CIP-003-6	Description et justification de la modification
E4	E4	En réponse à l'ordonnance 791 de la FERC demandant de retirer 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-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.
E2	E2	En réponse à l'ordonnance 791 de la FERC demandant de retirer de l'exigence les formulations ambiguës, l'expression « d'une manière permettant de détecter, d'évaluer et de corriger les lacunes » a été supprimée. La SDT a également revu l'exigence afin d'accorder aux entités responsables la flexibilité d'avoir un ou plusieurs programmes de formation sur la cybersécurité, la norme CIP-004-5 actuelle précisant à l'exigence E2 « a cyber security training program(s) » (en français, « un ou des programmes de formation sur la cybersécurité »). Cette modification vise à clarifier l'exigence et à uniformiser l'ensemble des normes.
E2.1	E2.1	Aucun changement.
E2.1.1 à E2.1.8	E2.1.1 à E2.1.8	Aucun changement.
E2.1.2	E2.1.2	Aucun changement.
E2.1.3	E2.1.3	Aucun changement.
E2.1.4	E2.1.4	Aucun changement.

CIP-004-6 – Cybersécurité –Personnel et formation		
CIP-004-5.1	CIP-004-6	Description et justification de la modification
E2.1.5	E2.1.5	Aucun changement.
E2.1.6	E2.1.6	Aucun changement.
E2.1.7	E2.1.7	Aucun changement.
E2.1.8	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 électronique transitoire, la SDT a ajouté les actifs électroniques transitoires et les supports de stockage 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 transitoires et les supports de stockage 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 de retirer 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	E3.1	Aucun changement.
E3.2	E3.2	Aucun changement.
E3.3	E3.3	Aucun changement.
E3.4	E3.4	Aucun changement.
E3.5	E3.5	Aucun changement.

CIP-004-6 – Cybersécurité –Personnel et formation		
CIP-004-5.1	CIP-004-6	Description et justification de la modification
E4	E4	En réponse à l'ordonnance 791 de la FERC demandant de retirer 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	E4.1	Aucun changement.
E4.1.1	E4.1.1	Aucun changement.
E4.1.2	E4.1.2	Aucun changement.
E4.1.3	E4.1.3	Aucun changement.
E4.2	E4.2	Aucun changement.
E4.3	E4.3	Aucun changement.
E4.4	E4.4	Aucun changement.
E5	E5	En réponse à l'ordonnance 791 de la FERC demandant de retirer 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	E5.1	Aucun changement.
E5.2	E5.2	Aucun changement.
E5.3	E5.3	Aucun changement.
E5.4	E5.4	Aucun changement.
E5.5	E5.5	Aucun changement.

CIP-006-6 – Cybersécurité – Sécurité physique des systèmes électroniques BES		
CIP-006-5	CIP-006-6	Description et justification de la modification
E1	E1	En réponse à l'ordonnance 791 de la FERC demandant de retirer 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	Aucun changement.
E1.3	E1.3	Aucun changement.
E1.4	E1.4	Aucun changement.
E1.5	E1.5	Aucun changement.
E1.6	E1.6	Aucun changement.
E1.7	E1.7	Aucun changement.
E1.8	E1.8	Aucun changement.
E1.9	E1.9	Aucun changement.
NOUVEAU	E1.10	En réponse aux directives dans l'ordonnance 791 de la FERC de 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.

CIP-006-6 – Cybersécurité – Sécurité physique des systèmes électroniques BES		
CIP-006-5	CIP-006-6	Description et justification de la modification
E2	E2	En réponse à l'ordonnance 791 de la FERC demandant de retirer 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	E2.1	Aucun changement.
E2.2	E2.2	Aucun changement.
E2.3	E2.3	Aucun changement.
E3	E3	Aucun changement.
E3.1	E3.1	Aucun changement

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 de retirer 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 de stockage amovibles visant ces ajouts répond à la directive sur les réseaux de communication dans l'ordonnance 791 de la FERC. Le terme supports de stockage amovibles a été mis en italique, car il figure maintenant au Glossaire.

CIP-007-6 – Cybersécurité – Gestion de la sécurité des systèmes		
CIP-007-5	CIP-007-6	Description et justification de la modification
E2	E2	En réponse à l'ordonnance 791 de la FERC demandant de retirer 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	E2.1	Aucun changement.
E2.2	E2.2	Aucun changement.
E2.3	E2.3	Aucun changement.
E2.4	E2.4	Aucun changement.
E3	E3	En réponse à l'ordonnance 791 de la FERC demandant de retirer 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	E3.1	Aucun changement.
E3.2	E3.2	Aucun changement.
E3.3	E3.3	Aucun changement.
E4	E4	En réponse à l'ordonnance 791 de la FERC demandant de retirer 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	E4.1	Aucun changement.
E4.1.1	E4.1.1	Aucun changement.
E4.1.2	E4.1.2	Aucun changement.

CIP-007-6 – Cybersécurité – Gestion de la sécurité des systèmes		
CIP-007-5	CIP-007-6	Description et justification de la modification
E4.1.3	E4.1.3	Aucun changement.
E4.2	E4.2	Aucun changement.
E4.2.1	E4.2.1	Aucun changement.
E4.2.2	E4.2.2	Aucun changement.
E4.3	E4.3	Aucun changement.
E4.4	E4.4	Aucun changement.
E5	E5	En réponse à l'ordonnance 791 de la FERC demandant de retirer 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	E5.1	Aucun changement.
E5.2	E5.2	Aucun changement.
E5.3	E5.3	Aucun changement.
E5.4	E5.4	Aucun changement.
E5.5	E5.5	Aucun changement.
E5.5.1	E5.5.1	Aucun changement.
E5.5.2	E.5.5.2	Aucun changement.

CIP-007-6 – Cybersécurité – Gestion de la sécurité des systèmes		
CIP-007-5	CIP-007-6	Description et justification de la modification
E6	E6	Aucun changement.
E7	E7	Aucun changement.

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	E1.1	Aucun changement.
E1.2	E1.2	Aucun changement.
E1.3	E1.3	Aucun changement.
E1.4	E1.4	Aucun changement.
E.1.5	E.1.5	Aucun changement.
E2	E2	En réponse à l'ordonnance 791 de la FERC demandant de retirer 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	E2.1	Aucun changement.
E2.2	E2.2	Aucun changement.
E2.3	E2.3	Aucun changement.

CIP-009-6 – Cybersécurité –Plans de rétablissement des systèmes électroniques BES		
CIP-009-5	CIP-009-6	Description et justification de la modification
E3	E3	Aucun changement.
E3.1	E3.1	Aucun changement.
E3.1.1	E3.1.1	Aucun changement.
E3.1.2	E3.1.2	Aucun changement.
E3.1.3	E3.1.3	Aucun changement.
E3.2	E3.2	Aucun changement.
E3.2.1	E3.2.1	Aucun changement.
E3.2.2	E3.2.2	Aucun changement.

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 de retirer 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	Aucun changement.
E1.3	E1.3	Aucun changement.

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
E1.4	E1.4	Aucun changement.
E1.4.1	E1.4.1	Aucun changement.
E1.4.2	E1.4.2	Aucun changement.
E1.4.3	E1.4.3	Aucun changement.
E1.5	E1.5	Aucun changement.
E1.5.1	E1.5.1	Aucun changement.
E1.5.2	E1.5.2	Aucun changement.
E2	E2	En réponse à l'ordonnance 791 de la FERC demandant de retirer 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	E2.1	Aucun changement.
E3	E3	Aucun changement.
E3.1	E3.1	Aucun changement.
E3.2	E3.2	Aucun changement.
E3.2.1	E3.2.1	Aucun changement.
E3.2.2	E3.2.2	Aucun changement.

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
E3.3	E3.3	Aucun changement.
E3.4	E3.4	Aucun changement.
NOUVEAU	E4	En réponse à la directive dans l'ordonnance 791 de la FERC concernant les actifs transitoires, 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 transitoires et les supports de stockage amovibles ; ces plans doivent être conformes aux sections de l'annexe 1. »
NOUVEAU	Annexe 1	L'annexe 1 de la CIP-010-2 dresse la liste des éléments que doivent couvrir les plans concernant les actifs électroniques transitoire et les supports de stockage amovibles. L'annexe répond à l'ordonnance 791 de la FERC concernant les risques liés aux actifs transitoires.

CIP-011-2 – Cybersécurité – Protection de l'information		
CIP-011-2	CIP-011-2	Description et justification de la modification
E1	E1	En réponse à l'ordonnance 791 de la FERC demandant de retirer 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	Aucun changement.
E2	E2	Aucun changement.
E2.1	E2.1	Aucun changement.

CIP-011-2 – Cybersécurité – Protection de l'information		
CIP-011-2	CIP-011-2	Description et justification de la modification
E2.2	E2.2	Aucun changement.

1. [Project 2014-02 – CIP Version 5 Revisions, Mapping Document](#), NERC