

Cybersécurité – Personnel et formation

Justification technique
de la norme de fiabilité CIP-004-7

Mars 2021

FIABILITÉ | RÉSILIENCE | SÉCURITÉ



3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table des matières

Préface.....	1
Introduction	2
Exigence E1	3
Remarques générales sur l'exigence E1.....	3
Justification de l'exigence E1.....	3
Exigence E2	4
Remarques générales sur l'exigence E2.....	4
Justification de l'exigence E2.....	4
Exigence E3.....	5
Remarques générales sur l'exigence E3.....	5
Justification de l'exigence E3.....	5
Exigence E4	6
Remarques générales sur l'exigence E4.....	6
Justification de l'exigence E4.....	6
Exigence E5.....	7
Remarques générales sur l'exigence E5.....	7
Justification de l'exigence E5.....	7
Exigence E6.....	8
Remarques générales sur l'exigence E6.....	8
Justification de l'exigence E6.....	8
Annexe 1 : Justification technique de la norme de fiabilité CIP-004-6.....	11

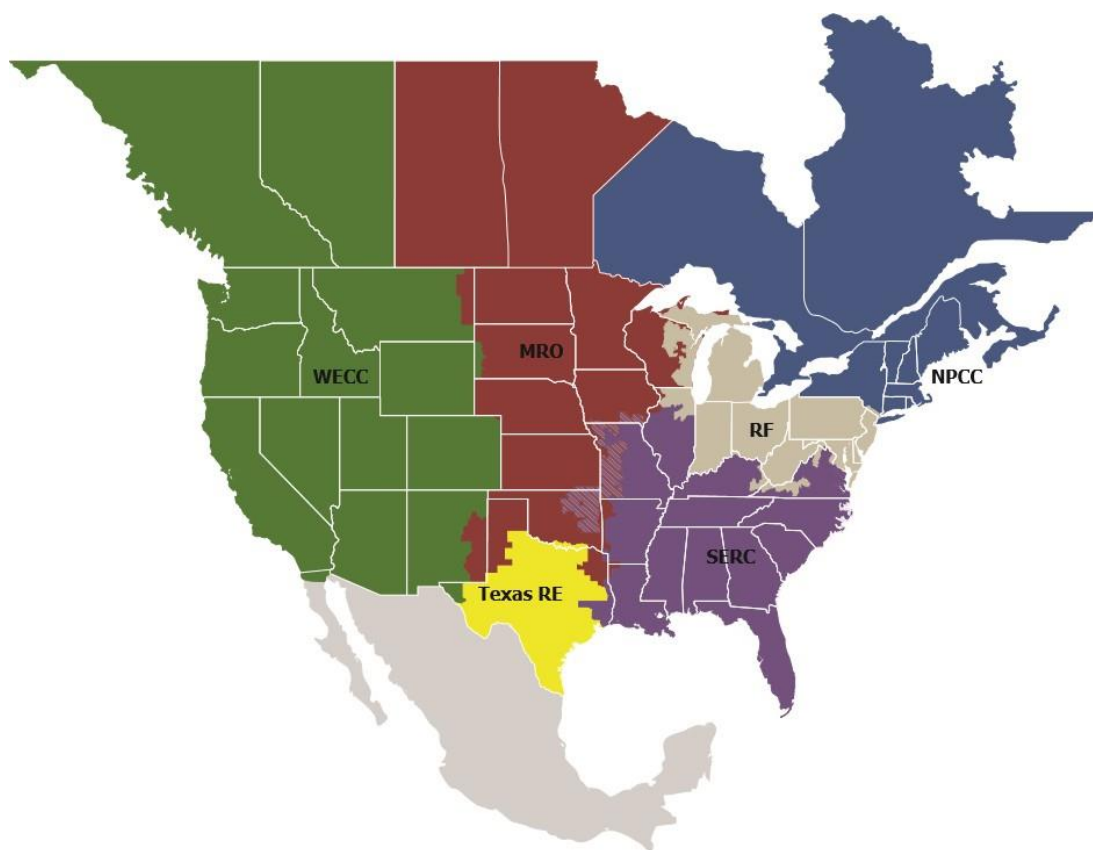
Préface

L'électricité est un élément essentiel du tissu de nos sociétés modernes, et l'organisme de fiabilité électrique (ERO) a pour mission de renforcer ce tissu. L'ERO, qui regroupe la North American Electric Reliability Corporation (NERC) et les six entités régionales, veille à maximiser la fiabilité et la sécurité du *système électrique interconnecté (BPS)* de l'Amérique du Nord. Nous travaillons en permanence à réduire de manière efficace et efficiente les risques pour la fiabilité et la sécurité du réseau électrique.

Fiabilité | Résilience | Sécurité

Parce que près de 400 millions de citoyens en Amérique du Nord comptent sur nous

Le *système électrique interconnecté* de l'Amérique du Nord est divisé en six territoires d'entités régionales, comme le montrent la carte et le tableau ci-dessous. Les zones combinant deux couleurs indiquent des chevauchements, car certains *responsables de l'approvisionnement* sont actifs dans une région alors que les *propriétaires d'installation de transport* et les *exploitants de réseau de transport* associés sont actifs dans une autre région.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst Corporation
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Ce document expose la justification technique de la *norme de fiabilité* CIP-004-7 proposée. Il vise à guider les parties prenantes ainsi que l'ERO dans la compréhension des enjeux technologiques et des exigences techniques de cette *norme de fiabilité*. Il présente aussi des précisions sur les intentions de l'équipe de rédaction (SDT) quant à ces exigences. Le présent document, *Justification technique de la norme de fiabilité CIP-004-7*, n'est pas une *norme de fiabilité* et son contenu ne doit donc pas être considéré comme obligatoire et exécutoire.

Le 24 juillet 2019, le Comité de normalisation de la North American Electric Reliability Corporation (NERC) a accepté une demande d'autorisation de norme (SAR) donnant suite à une initiative visant à renforcer la fiabilité du *BES* en offrant aux entités un meilleur éventail de choix, une flexibilité supérieure, une meilleure disponibilité et des options à meilleur coût pour la gestion de leurs *informations de système électronique BES*, au moyen d'un encadrement sécuritaire du recours à des systèmes de stockage et d'analyse de données modernes offerts par des tiers. En outre, le projet visait à clarifier les protections à prévoir dans le cadre de l'utilisation de solutions de tiers (par exemple, des services infonuagiques).

En réponse à cette SAR, la SDT du projet 2019-02 a modifié la *norme de fiabilité* CIP-004-7 de manière à obliger les entités responsables à mettre en place des mesures (énoncées dans l'exigence E6) pour autoriser, vérifier et révoquer les accès fournis aux *informations de système électronique BES* (BCSI).

Exigence E1

Remarques générales sur l'exigence E1

Aucune

Justification de l'exigence E1

Le programme de sensibilisation à la sécurité se veut un programme d'information, et non de formation. Il devrait rappeler les pratiques de sécurité afin de tenir le personnel au courant des pratiques recommandées en matière de sécurité physique et électronique pour protéger les *systèmes électroniques BES*. L'entité responsable n'a pas à fournir des documents qui attestent que chaque personne a reçu ou compris l'information, mais elle doit conserver en tout temps le matériel utilisé pour le programme : affiches, notes de service, présentations, etc.

Exigence E2

Remarques générales sur l'exigence E2

Aucune

Justification de l'exigence E2

La formation doit porter sur les politiques, les contrôles d'accès et les procédures établis pour les *systèmes électroniques BES* ; elle doit comporter au moins les éléments nécessaires en fonction des rôles et responsabilités de chacun, selon le tableau E2.

Le paragraphe 434 de l'ordonnance 706 de la FERC intègre à la formation un nouvel élément qui concerne les équipements et les logiciels de réseau ainsi que d'autres éléments d'interconnectabilité électronique nécessaires à l'exploitation et au contrôle des *systèmes électroniques BES*. La formation doit également porter sur les risques associés au branchement et à l'utilisation d'*actifs électroniques temporaires (TCA)* et de *supports de stockage amovibles* dans des *systèmes électroniques BES* ou à l'intérieur d'un *périmètre de sécurité électronique*. Comme l'indique le paragraphe 135 de l'ordonnance 791 de la FERC, des *TCA* et des *supports de stockage amovibles* ont été la cause de cas concrets de contamination de systèmes de commande industrielle de production d'électricité par des maliciels ; la formation à leur utilisation est donc essentielle pour la protection des *systèmes électroniques BES*. Il ne s'agit pas de donner une formation technique aux personnes responsables des équipements et des logiciels de réseau, mais plutôt d'informer les utilisateurs de systèmes sur les risques posés à la cybersécurité par l'interconnectabilité de ces systèmes. Selon leurs fonctions, rôles ou responsabilités, les utilisateurs doivent avoir une connaissance de base des systèmes auxquels ils peuvent accéder à partir d'autres systèmes et des incidences de leurs actions sur la cybersécurité.

Chaque entité responsable doit s'assurer que tous les membres du personnel auxquels un accès électronique autorisé ou un accès physique autorisé sans accompagnement est accordé à ses *systèmes électroniques BES*, ainsi que les contractuels et les fournisseurs de services, suivent une formation sur la cybersécurité avant d'obtenir cet accès autorisé, sauf dans des *circonstances CIP exceptionnelles*. Pour conserver leur accès autorisé, les personnes doivent suivre la formation au moins une fois tous les 15 mois.

Exigence E3

Remarques générales sur l'exigence E3

Aucune

Justification de l'exigence E3

Chaque entité responsable doit s'assurer qu'une évaluation des risques liés au personnel est menée pour tout le personnel auquel est accordé un accès électronique autorisé ou un accès physique autorisé sans accompagnement à ses *systèmes électroniques BES*, ainsi que les contractuels et les fournisseurs de services, avant que soit accordé cet accès, exception faite des circonstances exceptionnelles qui ont une incidence sur la fiabilité du *BES* ou la capacité d'intervention d'urgence, qui sont précisées au programme et approuvées par le cadre supérieur désigné ou son délégataire. Le contrôle de l'identité doit être réalisé en respectant les lois fédérales, d'État, provinciales et locales ainsi que les ententes syndicales en vigueur. Ce contrôle n'est nécessaire qu'avant le premier accès à accorder, mais peut être répété périodiquement durant la période d'emploi, selon le processus suivi par l'entité, à l'identique ou d'une autre façon.

Une vérification des antécédents judiciaires sur les sept années précédentes doit être effectuée en tenant compte des endroits où a résidé la personne pendant au moins six mois consécutifs. Cette vérification doit aussi être effectuée en respect des lois fédérales, d'État, provinciales et locales, et est sujette aux conventions collectives en vigueur. S'il est impossible de mener une vérification complète des antécédents judiciaires sur les sept années précédentes, la portion qui a pu être vérifiée doit être documentée ainsi que les motifs pour lesquels la vérification complète sur cette période n'a pu être faite. Il peut s'agir, par exemple, de personnes de moins de 25 ans dont les antécédents à titre de jeune contrevenant sont protégés en vertu de la loi, de personnes qui ont résidé à des endroits où il est impossible d'obtenir des vérifications d'antécédents judiciaires ou de personnes dont l'emploi est régi par une convention collective qui l'interdit. Dans de tels cas, l'entité responsable doit tenir compte du fait que les renseignements sont incomplets lorsqu'elle évalue le risque d'accorder un accès. Chaque personne ayant un accès doit avoir fait l'objet d'une évaluation des risques liés au personnel au cours des sept années précédentes. Une nouvelle vérification des antécédents judiciaires doit être menée dans le cadre de cette nouvelle évaluation des risques. Les personnes auxquelles on a accordé un accès en vertu d'une version antérieure des présentes normes doivent faire l'objet d'une nouvelle évaluation des risques liés au personnel dans les sept années suivant leur évaluation précédente. Dans la présente version de la norme, le processus de vérification des antécédents judiciaires sur les sept années précédentes a été clarifié de sorte qu'il ne soit pas nécessaire de mener une nouvelle évaluation des risques liés au personnel avant la date de mise en œuvre.

Exigence E4

Remarques générales sur l'exigence E4

Aucune

Justification de l'exigence E4

L'autorisation d'accès électronique et d'accès physique sans accompagnement doit être accordée selon le principe du besoin de savoir suivant la fonction de chacun. Les documents attestant l'autorisation doivent comporter une justification des besoins opérationnels invoqués.

Cette exigence prévoit des réexamens trimestriels ainsi que des réexamens au moins une fois tous les 15 mois civils. Les réexamens trimestriels servent à vérifier que l'accès aux *systèmes électroniques BES* n'a été accordé qu'aux utilisateurs autorisés. Cette exigence met l'accent sur l'intégrité du processus de fourniture d'accès plutôt que sur les comptes individuels de l'ensemble des *actifs électroniques BES*.

Le réexamen des droits d'accès effectué au moins une fois tous les 15 mois civils est plus détaillé afin de s'assurer que seuls les droits d'accès nécessaires à un utilisateur dans l'exercice de ses fonctions lui soient accordés (droit d'accès minimal).

Si les résultats des réexamens de comptes trimestriels ou des réexamens de comptes aux 15 mois révèlent qu'il s'est produit une erreur administrative ou de transcription faisant en sorte qu'un accès n'a pas été réellement fourni, la SDT juge que cette erreur ne constitue pas une non-conformité.

Dans le cas de *systèmes électroniques BES* pour lesquels aucun compte utilisateur n'est défini, les contrôles indiqués à l'exigence E4 ne s'appliquent pas. L'entité responsable doit cependant documenter ces configurations.

Exigence E5

Remarques générales sur l'exigence E5

Aucune

Justification de l'exigence E5

On entend par « révocation de l'accès électronique » d'une personne un processus dont le résultat final est l'impossibilité pour elle d'obtenir un accès électronique aux *systèmes électroniques BES* en utilisant les identifiants de connexion qui lui ont été attribués ou qu'elle connaît.

La révocation initiale prescrite à l'alinéa 5.1 de l'exigence E5 concerne aussi bien l'accès physique non accompagné que l'*accès distant interactif*. La révocation de ces deux accès doit empêcher tout accès de la personne après son départ. Si la personne détient toujours des comptes locaux pour l'accès à des *actifs électroniques BES* (c.-à-d. des comptes spécifiques à ces *actifs électroniques*), l'entité responsable dispose alors de 30 jours pour mener à bien le processus de révocation pour ces comptes. Toutefois, rien n'empêche l'entité responsable de révoquer tous les accès au moment du départ.

La révocation de l'accès aux comptes partagés est traitée séparément pour empêcher les situations où les mots de passe des équipements d'un poste ou d'une centrale changeraient constamment en raison du roulement du personnel.

L'alinéa 5.5 de l'exigence E5 précise que les mots de passe de comptes partagés doivent être changés dans les 30 jours civils suivant le départ ou lorsque l'entité responsable détermine qu'une personne n'a plus besoin d'avoir accès au compte en raison de sa réaffectation ou de sa mutation. Cette période de 30 jours est valable dans des conditions opérationnelles normales. Toutefois, certaines circonstances peuvent faire en sorte que ce ne soit pas possible. Il peut être nécessaire d'arrêter ou de redémarrer certains systèmes pour compléter le changement de mot de passe. En périodes de chaleur ou de froid extrême, plusieurs entités responsables pourraient interdire l'arrêt et le redémarrage de systèmes afin de maintenir la fiabilité du *BES*. Dans ce cas, l'entité responsable doit consigner ces circonstances et prévoir changer le mot de passe dans les 10 jours civils suivant la fin de celles-ci. Les documents consignant ces activités doivent être conservés afin de démontrer que l'entité responsable a suivi le plan qu'elle a établi.

Exigence E6

Remarques générales sur l'exigence E6

Aucune

Justification de l'exigence E6

L'exigence E6 demande aux entités responsables de mettre en œuvre un programme de gestion des accès aux *informations de système électronique BES* (BCSI) afin de faire en sorte que les accès fournis aux BCSI soient autorisés et vérifiés, et qu'ils soient révoqués sans délai. L'autorisation vise à ce que seules les personnes qui ont un véritable besoin soient autorisées à recevoir un accès aux BCSI. Une révocation sans délai de l'accès aux BCSI après le départ de la personne autorisée aide à prévenir toute divulgation ou utilisation inappropriée d'BCSI. Une vérification périodique sert à confirmer que tous les accès fournis sont bel et bien autorisés et qu'ils sont toujours nécessaires, et donne à l'entité responsable l'occasion de corriger toute erreur dans la fourniture des accès.

Le remplacement de l'expression « emplacement de stockage désigné » par l'expression « accès fourni » permet l'utilisation de solutions de tiers (par exemple, des services infonuagiques) pour les BCSI. Le concept d'emplacement de stockage désigné est jugé trop normatif et restrictif pour les entités qui souhaitent mettre en œuvre des droits et autorisations au niveau des fichiers (identifiants ou clés de chiffrement établis d'après un ensemble de règles et qui suivent le fichier et la personne autorisée), qui assurent un contrôle d'accès aux BCSI sans égard au lieu de stockage. Le concept d'accès fourni offre la souplesse voulue pour permettre aux entités d'utiliser d'autres technologies et approches au lieu (ou en plus) d'emplacements de stockage comme moyen de répondre aux exigences de gestion des accès pour les BCSI, en particulier celles qui sont stockées dans des solutions infonuagiques de tiers ou qui sont protégées au niveau de l'information ou du fichier, indépendamment de son emplacement de stockage.

Selon l'alinéa 6.1 de l'exigence E6, l'entité responsable doit autoriser les personnes auxquelles un accès à des BCSI devra être fourni. D'abord, l'entité responsable détermine qui a besoin d'obtenir et d'utiliser des BCSI pour effectuer les tâches liées spécifiquement à son travail. Ensuite, une personne habilitée à le faire par l'entité responsable autorise (accorde la permission ou l'approbation appropriée) la fourniture à ces personnes de l'accès aux BCSI. C'est seulement ensuite que l'entité responsable fournit l'accès aux BCSI selon l'autorisation accordée.

L'accès fourni doit être considéré comme le résultat d'actions visant spécifiquement à fournir à une personne le moyen d'accéder à des BCSI (clé physique, carte d'accès, compte d'utilisateur avec droits et privilèges associés, clé de chiffrement, etc.). Dans le contexte de cette exigence, on considère qu'un accès a été fourni à une personne si celle-ci a obtenu la capacité à la fois d'obtenir et d'utiliser les BCSI. Par exemple, si une personne peut obtenir des BCSI chiffrées, mais qu'elle ne dispose pas de la clé de chiffrement qui lui permettrait d'utiliser ces BCSI, on considère qu'il n'y a pas eu fourniture d'accès à ces BCSI.

Dans le cas des BCSI physiques, un accès physique est fourni à un emplacement de stockage physique désigné pour les BCSI et pour lequel un moyen d'accès peut être fourni, par exemple un classeur verrouillable. Dans le cas des BCSI sous forme électronique, un accès électronique est fourni à un système électronique ou à son contenu, ou à des fichiers individuels. La fourniture d'un accès à un emplacement physique où se trouve de l'équipement contenant des BCSI électroniques n'est pas considérée comme la fourniture d'un accès à ces BCSI. Considérons par

exemple le stockage d'BCSI chez un fournisseur de services infonuagiques : le personnel de ce fournisseur ayant un accès physique au centre de données n'est pas lui-même considéré comme s'étant fait fournir un accès aux BCSI électroniques stockées sur les serveurs du centre de données, car il faudrait qu'on lui ait fourni également un accès électronique aux serveurs ou au système. Dans des scénarios comme celui-ci, l'entité responsable doit mettre en place des mécanismes appropriés de protection de l'information pour aider à empêcher tout accès non autorisé aux BCSI dans le cadre de son programme de protection de l'information, conformément à la norme CIP-011-3. Les sous-alinéas de l'alinéa 6.1 de l'exigence E6 ont été rédigés de manière à renforcer ce concept et à clarifier les exigences de gestion des accès.

La vérification périodique prescrite à l'alinéa 6.2 de l'exigence E6 vise à confirmer que la fourniture d'accès aux BCSI est réservée aux seules personnes autorisées, et que l'accès fourni correspond à ce dont chaque personne a réellement besoin pour accomplir son travail. Par exemple, en procédant à la vérification, l'entité responsable pourrait constater que certaines personnes ont changé de poste ou d'emploi et n'ont plus besoin de l'accès qui leur a été fourni aux BCSI, et révoquerait alors cet accès.

À l'alinéa 6.3 de l'exigence E6, le retrait de la capacité d'une personne d'utiliser un accès fourni à des BCSI est considéré comme un processus dont le résultat est que l'accès électronique à des BCSI électroniques et l'accès physique à des BCSI physiques n'est plus désormais possible par le moyen qui avait été fourni à la personne pour obtenir et utiliser les BCSI dans ces circonstances. Ou bien le moyen qui a été spécifiquement fourni à la personne pour accéder aux BCSI (clé, compte d'utilisateur local ou de base de données et privilèges associés, etc.) est repris, supprimé, désactivé, révoqué, etc. (ce qu'on appelle parfois le « déprovisionnement »), ou bien un accès primaire est retiré de manière à empêcher la personne d'utiliser le moyen d'accès fourni. L'alinéa 6.3 de l'exigence E6 reconnaît que si le retrait d'un accès physique sans accompagnement et d'un accès *distant interactif*, comme le spécifie l'alinéa 5.1 de l'exigence E5, empêche désormais tout accès aux BCSI par la personne après son départ, cela revient à retirer à cette personne la capacité d'utiliser l'accès aux BCSI qui lui a été fourni. Une fois fourni, l'accès ne peut être révoqué ou retiré que dans la forme sous laquelle il a été fourni. Le but visé n'est pas d'obliger à récupérer les divers éléments d'BCSI (par exemple, des documents) qui pourraient être dans la possession de la personne (bien qu'il faille le faire dans la mesure du possible, mais la personne ne peut pas effacer de sa mémoire tout souvenir des BCSI dont elle a pris connaissance).

Dans les cas où aucun mécanisme particulier n'est disponible ou praticable pour fournir un accès à des BCSI, ces exigences ne s'appliquent pas. Ce serait le cas dans une situation où une personne reçoit directement, voit ou est susceptible de voir des BCSI, par exemple si la personne reçoit une feuille de papier pendant une réunion ou voit un tableau d'affichage dans une salle de réunion. De même, ces exigences ne s'appliquent pas à un accès électronique ou physique fourni qui n'est pas spécifiquement destiné à donner à la personne la capacité d'obtenir et d'utiliser des BCSI. Ainsi, il ne devrait vraisemblablement pas y avoir de fourniture particulière d'accès à des BCSI sur des postes de travail, des ordinateurs portatifs, des clés USB, des appareils portatifs, des bureaux, des véhicules, etc., en particulier si des BCSI n'y sont situées ou stockées que temporairement ou de façon fortuite. Un autre exemple est la fourniture d'un accès à un poste électrique dans le but de permettre à une personne d'effectuer des tâches liées à son travail, et non de lui donner accès aux BCSI qui peuvent s'y trouver. Il n'en demeure pas moins nécessaire que les BCSI dans ces emplacements et situations soient protégées contre les accès non autorisés, dans le cadre du programme de protection de l'information de l'entité responsable, conformément à la norme CIP-011-3.

L'utilisation de l'expression « accès fourni » aux BCSI est rétrocompatible avec le concept précédent d'« emplacement de stockage désigné » qu'elle remplace. En toute logique, les entités ont désigné spécifiquement des emplacements de stockage auxquels un accès peut être fourni, plutôt que tout emplacement où des BCSI pourraient se trouver. Les deux concepts visent à exclure les emplacements où des BCSI sont stockées temporairement, comme il est expliqué au paragraphe précédent. Le concept d'accès fourni, tout comme celui d'emplacement de stockage désigné, maintient la portée de l'exigence de telle sorte qu'elle s'applique à un objet fini et délimité, gérable et vérifiable en tant que tel ; il ne s'agit pas d'essayer de gérer l'accès à des éléments d'information individuels. Le retrait du terme « emplacements de stockage désignés » n'empêche aucunement une entité de définir des emplacements de stockage dans le cadre de son programme de gestion des accès en vue de l'autorisation, de la vérification et du retrait des accès aux BCSI.

Annexe 1 : Justification technique de la norme de fiabilité

CIP-004-6

Cette section reproduit les éléments de justification technique de la section Principes directeurs et fondements techniques de la norme CIP-004-6, à titre de référence historique. Par ailleurs, le contenu de cette même section qui donne des indications sur la conformité est repris dans un Guide d'application distinct pour la présente norme.

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

Le programme de sensibilisation à la sécurité se veut un programme d'information, et non de formation. Il devrait rappeler les pratiques de sécurité afin de tenir le personnel au courant des pratiques recommandées en matière de sécurité physique et électronique pour protéger les *systèmes électroniques BES*. L'entité responsable n'a pas à fournir des documents qui attestent que chaque personne a reçu ou compris l'information, mais elle doit conserver en tout temps le matériel utilisé pour le programme : affiches, notes de service, présentations, etc.

Exigence E2

La formation doit porter sur les politiques, les contrôles d'accès et les procédures établis pour les *systèmes électroniques BES* ; elle doit comporter au moins les éléments nécessaires en fonction des rôles et responsabilités de chacun, selon le tableau E2.

Le paragraphe 434 de l'ordonnance 706 de la FERC intègre à la formation un nouvel élément qui concerne les équipements et les logiciels de réseau ainsi que d'autres éléments d'interconnectabilité électronique nécessaires à l'exploitation et au contrôle des *systèmes électroniques BES*. La formation doit également porter sur les risques associés au branchement et à l'utilisation d'*actifs électroniques transitoires* et de *supports de stockage amovibles* dans des *systèmes électroniques BES* ou à l'intérieur d'un *périmètre de sécurité électronique*. Comme l'indique le paragraphe 135 de l'ordonnance 791 de la FERC, des *actifs électroniques transitoires*

et des *supports de stockage amovibles* ont été la cause de cas concrets de contamination de systèmes de commande industrielle de production d'électricité par des maliciels ; la formation à leur utilisation est donc essentielle pour la protection des *systèmes électroniques BES*. Il ne s'agit pas de donner une formation technique aux personnes responsables des équipements et des logiciels de réseau, mais plutôt d'informer les utilisateurs de systèmes sur les risques posés à la cybersécurité par l'interconnectabilité de ces systèmes. Selon leurs fonctions, rôles ou responsabilités, les utilisateurs doivent avoir une connaissance de base des systèmes auxquels ils peuvent accéder à partir d'autres systèmes et des incidences de leurs actions sur la cybersécurité.

Chaque entité responsable doit s'assurer que tous les membres du personnel auxquels un accès électronique autorisé ou un accès physique autorisé sans accompagnement est accordé à ses *systèmes électroniques BES*, ainsi que les contractuels et les fournisseurs de services, suivent une formation sur la cybersécurité avant d'obtenir cet accès autorisé, sauf dans des *circonstances CIP exceptionnelles*. Pour conserver leur accès autorisé, les personnes doivent suivre la formation au moins une fois tous les 15 mois.

Exigence E3

Chaque entité responsable doit s'assurer qu'une évaluation des risques liés au personnel est menée pour tout le personnel auquel est accordé un accès électronique autorisé ou un accès physique autorisé sans accompagnement à ses *systèmes électroniques BES*, ainsi que les contractuels et les fournisseurs de services, avant que soit accordé cet accès, exception faite des circonstances exceptionnelles qui ont une incidence sur la fiabilité du *BES* ou la capacité d'intervention d'urgence, qui sont précisées au programme et approuvées par le cadre supérieur désigné ou son délégataire.

Ce contrôle n'est nécessaire qu'avant le premier accès à accorder, mais peut être répété périodiquement durant la période d'emploi, selon le processus suivi par l'entité, à l'identique ou d'une autre façon.

Une vérification des antécédents judiciaires sur les sept années précédentes doit être effectuée en tenant compte des endroits où a résidé la personne pendant au moins six mois consécutifs. Cette vérification doit aussi être effectuée en respect des lois fédérales, d'État, provinciales et locales, et est sujette aux conventions collectives en vigueur. S'il est impossible de mener une vérification complète des antécédents judiciaires sur les sept années précédentes, la portion qui a pu être vérifiée doit être documentée ainsi que les motifs pour lesquels la vérification complète sur cette période n'a pu être faite.

Chaque personne ayant un accès doit avoir fait l'objet d'une évaluation des risques liés au personnel au cours des sept années précédentes. Une nouvelle vérification des antécédents judiciaires doit être menée dans le cadre de cette nouvelle évaluation des risques. Les personnes auxquelles on a accordé un accès en vertu d'une version antérieure des présentes normes doivent faire l'objet d'une nouvelle évaluation des risques liés au personnel dans les sept années suivant leur évaluation précédente. Le processus de vérification des antécédents judiciaires sur les sept années précédentes a été clarifié de sorte qu'il ne soit pas nécessaire de mener une nouvelle évaluation des risques liés au personnel avant la date de mise en œuvre.

Exigence E4

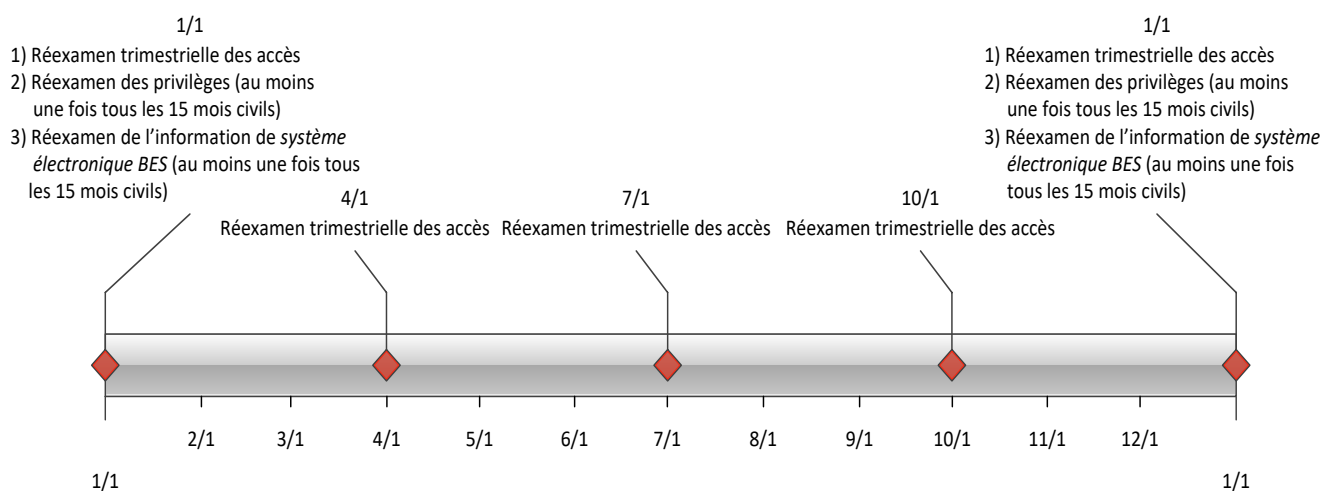
L'autorisation d'accès électronique et physique sans accompagnement et d'accès à l'information de *système électronique BES* doit être accordée selon le principe du besoin de savoir suivant la fonction de chacun. Les documents attestant l'autorisation doivent comporter une justification des besoins opérationnels invoqués. Pour assurer une séparation adéquate des tâches, l'autorisation

et la fourniture d'accès ne doivent pas être assumées par la même personne dans la mesure du possible.

Cette exigence prévoit des réexamens trimestriels ainsi que des réexamens au moins une fois tous les 15 mois civils. Les réexamens trimestriels servent à vérifier que l'accès aux *systèmes électroniques BES* n'a été accordé qu'aux utilisateurs autorisés. Cette exigence met l'accent sur l'intégrité du processus de fourniture d'accès plutôt que sur les comptes individuels de l'ensemble des *actifs électroniques BES*.

Le réexamen des droits d'accès effectué au moins une fois tous les 15 mois civils est plus détaillé afin de s'assurer que seuls les droits d'accès nécessaires à un utilisateur dans l'exercice de ses fonctions lui soient accordés (droit d'accès minimal).

Un calendrier type de tous les réexamens énoncés à l'exigence E4 est illustré ci-dessous.



Si les résultats des réexamens de comptes trimestriels ou des réexamens de comptes aux 15 mois révèlent qu'il s'est produit une erreur administrative ou de transcription faisant en sorte qu'un accès n'a pas été réellement fourni, la SDT juge que cette erreur ne constitue pas une non-conformité.

Dans le cas de *systèmes électroniques BES* pour lesquels aucun compte utilisateur n'est défini, les contrôles indiqués à l'exigence E4 ne s'appliquent pas. L'entité responsable doit cependant documenter ces configurations.

Exigence E5

L'exigence de révoquer les accès au moment du départ d'un employé (cessation d'emploi) prévoit des procédures démontrant que la révocation de l'accès se produit en même temps que le départ. On y admet que le moment du départ peut varier selon les circonstances.

On entend par « révocation de l'accès électronique » d'une personne un processus dont le résultat final est l'impossibilité pour elle d'obtenir un accès électronique aux *systèmes électroniques BES* en utilisant les identifiants de connexion qui lui ont été attribués ou qu'elle connaît.

La révocation initiale prescrite à l'exigence E5.1 concerne aussi bien l'accès physique non accompagné que l'*accès distant interactif*. La révocation de ces deux accès doit empêcher tout accès de la personne après son départ. Si la personne détient toujours des comptes locaux pour l'accès à des *actifs électroniques BES* (c.-à-d. des comptes spécifiques à ces *actifs électroniques*), l'entité responsable dispose alors de 30 jours pour mener à bien le processus de révocation pour ces comptes.

La révocation de l'accès aux comptes partagés est traitée séparément pour empêcher les situations où les mots de passe des équipements d'un poste ou d'une centrale changeraient constamment en raison du roulement du personnel.

L'exigence 5.5 précise que les mots de passe de comptes partagés doivent être changés dans les 30 jours civils suivant le départ ou lorsque l'entité responsable détermine qu'une personne n'a plus besoin d'avoir accès au compte en raison de sa réaffectation ou de sa mutation. Cette période de 30 jours est valable dans des conditions opérationnelles normales. Toutefois, certaines circonstances peuvent faire en sorte que ce ne soit pas possible. Il peut être nécessaire d'arrêter ou de redémarrer certains systèmes pour compléter le changement de mot de passe. En périodes de chaleur ou de froid extrême, plusieurs entités responsables pourraient interdire l'arrêt et le redémarrage de systèmes afin de maintenir la fiabilité du *BES*. Dans ce cas, l'entité responsable doit consigner ces circonstances et prévoir changer le mot de passe dans les 10 jours civils suivant la fin de celles-ci. Les documents consignant ces activités doivent être conservés afin de démontrer que l'entité responsable a suivi le plan qu'elle a établi.

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 :

Faire en sorte qu'une entité responsable dont des employés ont un accès électronique autorisé ou un accès physique autorisé sans accompagnement à des *actifs électroniques BES* prenne des mesures pour que les employés ayant de tels accès soient toujours au fait de ses pratiques de sécurité.

Justification de l'exigence E2 :

Faire en sorte que le programme de formation de l'entité responsable à l'intention du personnel ayant besoin d'un accès électronique autorisé ou d'un accès physique autorisé sans accompagnement à des *systèmes électroniques BES* traite des politiques, des contrôles d'accès et des procédures visant à protéger les *systèmes électroniques BES* et que ce personnel reçoive la formation appropriée avant de se voir accorder des accès.

Justification de l'exigence E3 :

Faire en sorte que les personnes qui ont besoin d'un accès électronique autorisé ou d'un accès physique autorisé sans accompagnement à des *systèmes électroniques BES* ont fait l'objet d'une évaluation des risques. Les personnes qui ont accès à ces systèmes doivent avoir fait l'objet d'une évaluation des risques liés au personnel au cours des sept dernières années, qu'il s'agisse d'une première autorisation d'accès ou du maintien de l'autorisation.

Justification de l'exigence E4 :

Faire en sorte que les personnes ayant accès à des *systèmes électroniques BES* et à des emplacements physiques et électroniques où l'entité responsable stocke de l'information de *système électronique BES* sont dûment autorisées à avoir accès à ces systèmes et emplacements. L'« autorisation » désigne l'octroi d'une permission par une ou des personnes habilitées par l'entité responsable à autoriser cet octroi ; ce pouvoir fait partie des délégations indiquées à la norme CIP-003-6. La « fourniture » désigne les mesures prises pour fournir un accès à une personne.

L'accès est constitué des accès physique, logique et distant à des *actifs électroniques* qui font partie du *système électronique BES* ou qui permettent l'accès au *système électronique BES*. Au moment d'accorder, de réexaminer ou de révoquer un accès, l'entité responsable doit tenir compte de l'*actif électronique* en particulier de même que des systèmes utilisés pour permettre cet accès (système de contrôle des accès physiques, système d'accès distant, services d'annuaire, etc.).

Les *circonstances CIP exceptionnelles* doivent être définies dans une politique de l'entité responsable conformément à la norme CIP-003-6 ; elles constituent une exception à l'exigence d'autorisation d'accès aux *systèmes électroniques BES* et à l'information de *système électronique BES*.

Les réexamens trimestriels prescrits à l'alinéa 4.5 servent à confirmer que l'accès aux *systèmes électroniques BES* n'a été accordé qu'aux utilisateurs autorisés. Pour ce faire, on compare la liste des personnes auxquelles on a réellement fourni un accès à un *système électronique BES* avec le registre des personnes autorisées à accéder à ce *système électronique BES*. Cette exigence met l'accent sur l'intégrité du processus de fourniture d'accès plutôt que sur les comptes individuels de l'ensemble des *actifs électroniques BES*.

Si les résultats des réexamens de comptes trimestriels ou annuels révèlent qu'il s'est produit une erreur administrative ou de transcription faisant en sorte que l'accès n'a pas été réellement fourni, la SDT juge que cette erreur ne constitue pas une non-conformité.

Dans le cas de *systèmes électroniques BES* pour lesquels aucun compte utilisateur n'est défini, les contrôles indiqués à l'exigence E4 ne s'appliquent pas. L'entité responsable devrait cependant documenter ces configurations.

Justification de l'exigence E5 :

La révocation rapide de l'accès électronique aux *systèmes électroniques BES* constitue un élément essentiel de tout système de gestion des accès. Lorsque l'accès d'une personne à un *système électronique BES* n'est plus nécessaire dans le cadre de ses fonctions, il doit être révoqué. Cela est particulièrement important dans les situations où des personnes sont licenciées ou réaffectées contre leur gré, puisqu'il y a un risque qu'elles réagissent de manière hostile ou destructrice.

En examinant la manière de répondre aux directives de l'ordonnance 706 de la FERC qui stipulent que l'accès doit être « immédiatement » révoqué en cas de départ involontaire, la SDT a choisi de ne pas préciser de délais en heures dans l'exigence (p. ex. « révoquer l'accès dans l'heure suivant le départ »). Le moment du départ d'une personne ne peut généralement pas être déterminé à l'heure près. Cependant, la plupart des organisations disposent d'un processus de cessation d'emploi en bonne et due forme, et la révocation de l'accès est plus expéditive si elle survient en même temps que les premières étapes de ce processus.

L'accès est constitué des accès physique, logique et distant à des *actifs électroniques* qui font partie du *système électronique BES* ou qui permettent l'accès au *système électronique BES*. Au moment d'accorder, de réexaminer ou de révoquer un accès, l'entité responsable doit tenir compte de l'*actif électronique* en particulier de même que des systèmes utilisés pour permettre cet accès (système de contrôle des accès physiques, système d'accès distant, services d'annuaire, etc.).